Linux Virtual Delivery Agent 2212

Contents

Linux Virtual Delivery Agent 2212 5

What's new 5

Fixed issues 7

Known issues 8

Third party notices 11

Deprecation 11

System requirements 12

Installation overview 17

Create domain-joined VDAs using easy install 17

Create non-domain-joined Linux VDAs 39

Create Linux VDAs using Machine Creation Services (MCS) 52

Create Linux VDAs using Citrix Provisioning 75

Create Linux VDAs in Citrix DaaS Standard for Azure 76

Install the Linux VDA manually 81

Install the Linux VDA on Amazon Linux 2, CentOS, RHEL, and Rocky Linux manually 81

Install the Linux VDA on SUSE manually 121

Install the Linux VDA on Ubuntu manually 150

Install the Linux VDA on Debian manually 184

Configure 214

Administration 214

Citrix Customer Experience Improvement Program (CEIP) 215

HDX Insight 219

Integration with the Citrix Telemetry Service 220

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux VDA self-update for Citrix DaaS Standard for Azure **224**

Linux VM and Linux session metrics **227**

Log collection **234**

Session shadowing **238**

The monitor service daemon **244**

Tools and utilities **247**

Others **252**

Citrix Workspace app for HTML5 support **252**

Create a Python3 virtual environment **253**

Integrate NIS with Active Directory **255**

IPv6 **261**

LDAPS **262**

Xauthority **266**

Authentication **269**

Authentication with Azure Active Directory **270**

Double-hop single sign-on authentication **274**

Federated Authentication Service **276**

Non-SSO authentication **286**

Smart cards **287**

Unauthenticated sessions by anonymous users **298**

File **301**

File copy and paste **301**

File transfer **302**

Graphics **306**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Automatic DPI scaling **307**

Client battery status display **308**

Graphics configuration and fine-tuning **312**

HDX screen sharing **324**

Non-virtualized GPUs **331**

Session watermark **334**

Thinwire progressive display **339**

Keyboard **341**

Client Input Method Editor (IME) **342**

Client IME user interface synchronization **342**

Dynamic keyboard layout synchronization **347**

Soft keyboard **351**

Support for multiple language inputs **354**

Multimedia **356**

Audio features **356**

Browser content redirection **357**

HDX webcam video compression **363**

Non-domain-joined Linux VDAs **368**

Policy support list **371**

Printing **381**

Printing best practices **381**

PDF printing **388**

Remote PC Access **389**

Session **401**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Adaptive transport **402**

Custom backgrounds and banner messages on session logon screens **405**

Custom desktop environments by session users **405**

Logon with a temp home directory **407**

Publish applications **408**

Rendezvous V1 **409**

Rendezvous V2 **413**

Secure user sessions using DTLS **416**

Secure user sessions using TLS **417**

Session reliability **420**

Session recording (experimental) **423**

USB device redirection **425**

Virtual Channel SDK (experimental) **433**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux Virtual Delivery Agent 2212

January 31, 2023

> **Important:**
>
> The product lifecycle strategy for Current Releases (CR) and Long Term Service Releases (LTSR) is described in Lifecycle Milestones.

The Linux Virtual Delivery Agent (VDA) enables access to the Linux virtual apps and desktops anywhere from any device where Citrix Workspace app is installed.

You can deliver virtual apps and desktops based on supported Linux distributions. Install the VDA software on your Linux virtual machines (VMs), configure the Delivery Controller, and then use Citrix Studio to make the apps and desktops available to users.

What's new

February 1, 2023

What's new in 2212

Version 2212 of the Linux VDA includes the following new features and enhancements:

Support for RHEL 9.0 and Rocky Linux 9.0

We have added RHEL 9.0 and Rocky Linux 9.0 as supported distributions. For more information, see System requirements.

USB device redirection enhancements

We have made the following enhancements for USB device redirection:

- We now use USB/IP as the new virtual host controller for USB device redirection. Because, in most cases, the USB/IP kernel module is released with Linux kernel version 3.17 and later, you don't have to build the kernel module by default.
- We have added support for USB 3.0 ports. You can now insert USB 3.0 devices into USB 3.0 ports on a client device.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- We have optimized bulk transfers and increased the transfer speed. The boost is more prominent for high latency environments.
- We have extended USB device redirection to more USB devices such as **TD-RDF5A Transcend USB device** and the composite USB device, **Yubico YubiKey OTP+FIDO+CCID**.

For more information, see USB device redirection.

Hardware acceleration for specific non-virtualized GPUs from NVIDIA

In the Linux VDA documentation, **non-virtualized GPUs** refers to:

- GPUs used in Remote PC Access scenarios
- GPUs passed through from a hypervisor

For HDX 3D Pro graphics to render with superior performance, we now enable hardware acceleration for specific non-virtualized GPUs from NVIDIA. For the specific non-virtualized GPUs, see the supported hardware section of the release notes for NVIDIA Linux Capture SDK.

For more information, see Non-virtualized GPUs.

Replacing pam_krb5 with SSSD for smart card and FAS authentication

Previously, to use smart card or Federated Authentication Service (FAS) authentication on RHEL 8 and Rocky Linux 8, you had to build the pam_krb5 module manually. Starting with this release, performing this manual step is no longer necessary for RHEL 8 and Rocky Linux 8 machines delivered in VDI mode. For more information, see Federated Authentication Service and Smart cards.

Extending easy install GUI to include MCS configuration

Previously, you could configure MCS variables only by editing the `/etc/xdl/mcs/mcs.conf` file. This release extends the easy install GUI to include MCS configuration so that you can also configure MCS variables by using the GUI. After you click **Deploy** on the GUI, the variables you set on the GUI override the variables you set in the `/etc/xdl/mcs/mcs.conf` file. For more information, see Step 3: Prepare a master image.

Support for recording Linux sessions (experimental)

As an experimental feature, you can now record and replay sessions hosted on a Linux VDA. For more information, see Session recording (experimental).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Database options now available (experimental)

As an experimental feature, you can now use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL by editing `/etc/xdl/db.conf` after installing the Linux VDA package. To do so, complete the following steps:

1. Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.
2. Edit `/etc/xdl/db.conf` to specify a database to use.
3. Run any of the following scripts based on your installation method:

- `/opt/Citrix/VDA/sbin/ctxinstall.sh` or `/opt/Citrix/VDA/bin/easyinstall` if you are using east install
- `/opt/Citrix/VDA/sbin/ctxsetup.sh` if you are installing the Linux VDA manually
- `/opt/Citrix/VDA/sbin/deploymcs.sh` if you are using MCS to create Linux VDAs

> **Note:**
>
> - We recommend you use SQLite for VDI mode only.
> - For manual installations, you must install SQLite and PostgreSQL manually before being able to switch between them. For easy install and MCS, you can switch between SQLite and PostgreSQL without having to install them manually.
> - You can also use `/etc/xdl/db.conf` to configure the port number for PostgreSQL.

For more information, see the installation articles.

What's new in earlier releases

For new features included in the releases that shipped after the 1912 LTSR through the 2210 CR, see What's new history.

Fixed issues

February 1, 2023

The following issues have been fixed since Linux Virtual Delivery Agent 2210:

- When the NSAP virtual channel is enabled, Linux VDAs might have performance issues causing them to become slow and unusable. [CVADHELP-19776]
- Linux VDAs might unregister when you restart the Cloud Connector or the Delivery Controller. [CVADHELP-21256]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Known issues

July 3, 2023

The following issues have been identified in this release:

- VDA registration might fail due to the following LDAP exception thrown in **/var/log/xdl/jproxy.log**:

  ```
  javax.naming.NamingException: LDAP response read timed out,
     timeout used: 10000 ms.
  <!--NeedCopy-->
  ```

  To work around the issue, do the following:

  - Change the LDAP timeout value. For example, change the LDAP timeout value to 60 s using the following command:

    ```
    ctxreg create -k "HKLM\Software\Citrix\GroupPolicy\Defaults"
       -t "REG_DWORD" -v "LDAPTimeout" -d "0x000EA60" --force
    <!--NeedCopy-->
    ```

  - Speed up LDAP queries by setting a search base. You can set a search base using the CTX_XDL_SEARCH_BASE variable in ctxsetup.sh or using the following command:

    ```
    ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent" -
       t "REG_SZ" -v "LDAPComputerSearchBase" -d "<specify a
       search base instead of the root of the domain to improve
       search performance>" --force
    <!--NeedCopy-->
    ```

  [CVADHELP-20895]

- Microsoft released cumulative updates KB5019966 and KB5019964 for Windows 10 in November 2022. The updates introduce failures in domain joining and registration. To work around the issue, see Knowledge center article CTX474888.

- With the **RC4_HMAC_MD5** encryption type allowed for Kerberos, the Linux VDA might fail to register with the Controller and the following error message appears:

  Error: Failure unspecified at GSS-API level (Mechanism level: Encryption type RC4 with HMAC is not supported/enabled)

  To address this issue, disable **RC4_HMAC_MD5** globally in your Active Directory domain (*or specifically on an OU*) or allow weak encryption types on the Linux VDA. After that, clear the cached Kerberos tickets on the Controller and Citrix Cloud Connector by using the **klist -li 0x3e4 purge** command and restart the Linux VDA.

  To disable **RC4_HMAC_MD5** globally in your Active Directory domain, complete the following steps:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Open the Group Policy Management Console.
2. Locate the target domain, and then select **Default Domain Policy**.
3. Right-click **Default Domain Policy** and select **Edit**. The Group Policy Management Editor opens.
4. Select **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**.
5. Double-click **Network security: Configure encryption types allowed for Kerberos**.
6. Clear the **DES_CBC_CRC**, **DES_CBC_MD5**, and **RC4_HMAC_MD5** check boxes and select **AES128_HMAC_SHA1**, **AES256_HMAC_SHA1**, and **Future encryption types**.

To allow weak encryption types on the Linux VDA, complete the following steps:

> **Note:**
>
> Weak encryption types make your deployment vulnerable to attacks.

1. Open the /etc/krb5.conf file on the Linux VDA.
2. Add the following setting under the **[libdefaults]** section:

   ```
   allow_weak_crypto= TRUE
   ```

- The Linux VDA does not support SecureICA for encryption. Enabling SecureICA on the Linux VDA causes session launch failure.
- In a GNOME desktop session, attempts to change the keyboard layout might fail. [CVADHELP-15639]
- Non-seamless published applications might exit shortly after launch. The issue occurs after a Mutter upgrade to a version later than mutter-3.28.3-4. To work around the issue, use mutter-3.28.3-4 or earlier. [LNXVDA-6967]
- An unexpected window appears during file download. The window does not affect the file download functionality and it disappears automatically after a while. [LNXVDA-5646]
- The default settings of PulseAudio cause the sound server program to exit after 20 seconds of inactivity. When PulseAudio exits, audio does not work. To work around this issue, set exit-idle-time=-1 in the /etc/pulse/daemon.conf file. [LNXVDA-5464]
- Sessions cannot be launched in Citrix Workspace app for Linux when SSL encryption is enabled and session reliability is disabled. [RFLNX-1557]
- Ubuntu graphics: In HDX 3D Pro, a black frame might appear around applications after resizing the Desktop Viewer, or sometimes, the background can appear black.
- Printers created by the Linux VDA printing redirection might not be removed after logging out of a session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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.
- In this release, only UTF-8 encoding is supported for non-English languages.
- Citrix Workspace app for Android CAPS LOCK state might be reversed during session roaming. The CAPS LOCK state can be lost when roaming an existing connection to Citrix Workspace app for Android. As a workaround, 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 you connect to the Linux VDA using Citrix Workspace app for Mac. Citrix Workspace app for Mac sends AltGr for both left and right Options/Alt keys by default. You can modify this behavior within the Citrix Workspace app settings but the results vary with different applications.
- Registration fails when the Linux VDA is rejoined to the domain. The rejoining generates a fresh set of Kerberos keys. But, the Broker might use a cached out-of-date VDA service ticket based on the previous set of Kerberos keys. When the VDA tries to connect to the Broker, the Broker might not be able to establish a return security context to the VDA. The usual symptom is that the VDA registration fails.

  This problem can eventually resolve itself when the VDA service ticket expires and is renewed. But because service tickets are long-lived, it can take a long time.

  As a workaround, clear the Broker's ticket cache. Restart the Broker or run the following command on the Broker from a command prompt as Administrator:

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

  This command purges all service tickets in the LSA cache held by the Network Service principal under which the Citrix Broker Service runs. It removes service tickets for other VDAs and potentially other services. However, it is harmless –these service tickets can be reacquired from the KDC when needed again.
- Audio plug-n-play is not supported. You can connect an audio capture device to the client machine before starting to record audio in the ICA session. If a capture device is attached after the audio recording application has started, the application might become unresponsive and you must restart it. If a capture device is unplugged while recording, a similar issue might occur.
- Citrix Workspace app for Windows might experience audio distortion during audio recording.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Third party notices

January 23, 2023

Linux Virtual Delivery Agent Version 2212 (PDF Download)

This release of the Linux VDA can include third party software licensed under the terms defined in the document.

Deprecation

March 7, 2023

The announcements in this article give you advanced notice of platforms, Citrix products, and features that are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.
For details about product lifecycle support, see the Product Lifecycle Support Policy article.

Deprecations and removals

The following table shows the platforms, Citrix products, and features that are deprecated or removed.
Deprecated items are not removed immediately. Citrix continues to support them in this release but they will be removed in a future Current Release.
Removed items are either removed, or are no longer supported, in the Linux VDA.

Item	Deprecation announced in	Removed in
Support for Ubuntu 18.04	2212	2305
Support for SUSE 15.3	2210	2301
Support for Debian 10.9	2206	2210
Support for SUSE 15.2	2206	2209
Support for RHEL 8.2	2206	2209
Support for RHEL 8.1, RHEL 8.3	2203	2206
Support for RHEL 7.8, CentOS 7.8	2203	2204

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Item	Deprecation announced in	Removed in
Support for CentOS 8.x	2110	2201
Support for SUSE 12.5	2109	2204
Support for Ubuntu 16.04	2109	2203
Support for RHEL 7.7, CentOS 7.7	2006	2009
Support for SUSE 12.3	2006	2006
Support for RHEL 6.10, CentOS 6.10	2003	2003
Support for RHEL 6.9, CentOS 6.9	1909	1909
Support for RHEL 7.5, CentOS 7.5	1903	1903
Support for RHEL 7.4, CentOS 7.4	1811	1811
Support for RHEL 6.8, CentOS 6.8	1811	1811
Support for RHEL 7.3, CentOS 7.3	7.18	7.18
Support for RHEL 6.6, CentOS 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

System requirements

January 23, 2023

The Current Release of the Linux VDA is aligned with Citrix Virtual Apps and Desktops. It is also backward compatible with earlier versions of Citrix Virtual Apps and Desktops that haven't yet reached the end of their lifecycle. For information about the Citrix product lifecycle, and to find out when Citrix stops supporting specific versions of products, see the Citrix Product Lifecycle Matrix.

The configuration process for Linux VDAs differs slightly from Windows VDAs. Any Delivery Controller farm is able to broker both Windows and Linux desktops.

System requirements for components not covered here (such as Citrix Workspace app) are described in their respective documentation sets.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For information about using a Current Release (CR) in a Long Term Service (LTSR) environment and other FAQs, see Knowledge Center article.

Linux distributions

The Linux VDA supports the following Linux distributions:

> **Important:**
>
> When the support from your OS vendor expires, Citrix might be limited in its ability to remediate problems.
> For deprecated or removed platforms, see Deprecation.

- Amazon Linux
  - Amazon Linux 2
- CentOS Linux
  - CentOS 7.9
- Debian Linux
  - Debian 11.3
- Red Hat Enterprise Linux
  - Workstation 9.0
  - Workstation 8.6
  - Workstation 8.4
  - Workstation 7.9
  - Server 9.0
  - Server 8.6
  - Server 8.4
  - Server 7.9
- Rocky Linux 9.0
- Rocky Linux 8.6
- SUSE Linux Enterprise:
  - Server 15 Service Pack 3
- Ubuntu Linux
  - Ubuntu Desktop 22.04
  - Ubuntu Server 22.04
  - Ubuntu Desktop 20.04

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Ubuntu Server 20.04
- Ubuntu Desktop 18.04
- Ubuntu Server 18.04
- Ubuntu Live Server 18.04

> **Note:**
>
> CentOS project shifts focus to CentOS Stream. CentOS Linux 8, as a rebuild of RHEL 8, ends at the end of 2021. CentOS Stream continues after that date, serving as the upstream (development) branch of Red Hat Enterprise Linux. For more information, see https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux.

For a matrix of the Linux distributions and the Xorg versions that this version of the Linux VDA supports, see the following table. For more information, see XorgModuleABIVersions.

Linux distribution	Xorg version	Supported desktop
Amazon Linux 2	1.20	MATE, GNOME, GNOME Classic
Debian 11.3	1.20	MATE, GNOME, GNOME Classic, KDE
RHEL 9.0, Rocky Linux 9.0	1.20	GNOME
RHEL 8.6, RHEL 8.4	1.20	MATE, GNOME, GNOME Classic
RHEL 7.9, CentOS 7.9	1.20	MATE, GNOME, GNOME Classic, KDE
Rocky Linux 8.6	1.20	MATE, GNOME, GNOME Classic, KDE
SUSE 15.3	1.20	MATE, GNOME, GNOME Classic
Ubuntu 22.04	1.21	MATE, GNOME, GNOME Classic, KDE
Ubuntu 20.04	1.20	MATE, GNOME, GNOME Classic, KDE
Ubuntu 18.04	1.19	MATE, GNOME, GNOME Classic, KDE

> **Tip:**
>
> Do not use `HWE kernel` or `HWE Xorg` on Ubuntu.
>
> At least one desktop must be installed. You can specify through the ctxinstall.sh or ctxsetup.sh script the GNOME or MATE desktop environment to use in sessions.
> Your user name format must comply with the `systemd` syntax rules for your current display

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> manager. For more information about the `systemd` user name syntax, see User/Group Name Syntax.

Supported host platforms and virtualization environments

- Bare metal servers
- Amazon Web Services (AWS)
- Citrix Hypervisor
- Google Cloud Platform (GCP)
- Kernel-based Virtual Machine (KVM)
- Microsoft Azure
- Microsoft Hyper-V
- VMware vSphere Hypervisor
- Nutanix AHV

> **Note:**
>
> In all cases, the supported processor architecture is x86-64.
>
> From Citrix Virtual Apps and Desktops 7 2003 through 2112, hosting the Linux VDA on Microsoft Azure, AWS, and GCP was supported only for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Starting with the 2203 release, you can host the Linux VDA on these public clouds for both Citrix DaaS and Citrix Virtual Apps and Desktops. To add these public cloud host connections to your Citrix Virtual Apps and Desktops deployment, you need **Hybrid Rights License**. For information about **Hybrid Rights License**, see Transition and Trade-Up (TTU) with Hybrid Rights.

Active Directory integration packages

The Linux VDA supports the following Active Directory integration packages and products:

	Winbind	SSSD	Centrify	PBIS	Quest
Amazon Linux 2	Yes	Yes	Yes	Yes	No
Debian 11.3	Yes	Yes	Yes	Yes	No
RHEL 9.0	Yes	Yes	No	No	No
RHEL 8.6, RHEL 8.4	Yes	Yes	Yes	Yes	No
RHEL 7.9, CentOS 7.9	Yes	Yes	Yes	Yes	Yes (Quest v4.1 and later)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	Winbind	SSSD	Centrify	PBIS	Quest
Rocky Linux 9.0	Yes	Yes	No	No	No
Rocky Linux 8.6	Yes	Yes	No	No	No
SUSE 15.3	Yes	Yes	Yes	Yes	No
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Yes	Yes	Yes	Yes	Yes (Quest v4.1 and later)

HDX 3D Pro

HDX 3D Pro of Citrix Virtual Apps and Desktops lets you deliver desktops and applications that perform best using a Graphics Processing Unit (GPU) for hardware acceleration.

Hypervisors

For the Linux VDA, HDX 3D Pro is compatible with the following hypervisors:

- Citrix Hypervisor
- VMware vSphere Hypervisor
- Nutanix AHV
- Microsoft Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

> **Note:**
>
> The hypervisors are compatible with certain Linux distributions.
> To use HDX 3D Pro for Amazon Linux 2, we recommend you install NVIDIA driver 470.

GPUs

To learn which NVIDIA GPU cards your Linux distribution supports, go to the NVIDIA product support matrix and check the **Hypervisor or Bare-Metal OS**, **Software Product Deployment**, **Hardware Supported**, and **Guest OS Support** columns.

Ensure that you install the latest vGPU driver for your GPU card. Currently, the Linux VDA supports up to vGPU 14. For more information, see NVIDIA Virtual GPU Software Supported GPUs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Installation overview

January 23, 2023

This section guides you through the following procedures:

- Create domain-joined VDAs using easy install
- Create non-domain-joined Linux VDAs using MCS
- Create Linux VDAs using MCS
- Create Linux VDAs using Citrix Provisioning
- Create Linux VDAs in Citrix DaaS Standard for Azure
- Install the Linux VDA manually
  - Install the Linux VDA on Amazon Linux 2, CentOS, RHEL, and Rocky Linux manually
  - Install the Linux VDA on SUSE manually
  - Install the Linux VDA on Ubuntu manually
  - Install the Linux VDA on Debian manually

Create domain-joined VDAs using easy install

March 7, 2023

> **Important:**
>
> - For fresh installations, we recommend you refer to this article for a quick installation. This article steps through how to install and configure the Linux VDA by using easy install. Easy install saves time and labor and is less error-prone than manual installation. It helps you set up a running environment of the Linux VDA by installing the necessary packages and customizing the configuration files automatically.
> - To create non-domain joined VDAs, you must use Machine Creation Services (MCS). For more information, see Create non-domain-joined Linux VDAs.
> - To learn about features available for non-domain-joined VDAs, go to Non-domain-joined VDAs.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 1: Prepare configuration information and the Linux machine

Collect the following configuration information needed for easy install:

- Host name - Host name of the machine on which the Linux VDA is to be installed
- IP address of Domain Name Server
- IP address or string name of NTP Server
- Domain name - The NetBIOS name of the domain
- Realm name - The Kerberos realm name
- Fully Qualified Domain Name (FQDN) of the domain

> **Important:**
>
> - To install the Linux VDA, verify that the repositories are added correctly on the Linux machine.
> - To launch a session, verify that the X Window system and desktop environments are installed.

Considerations

- The workgroup name, by default, is the domain name. To customize the workgroup in your environment, do the following:

  a. Create the /tmp/ctxinstall.conf file on the Linux VDA machine.
  b. Add the workgroup=<your workgroup> line to the file and save your changes.

- Centrify does not support pure IPv6 DNS configuration. At least one DNS server using IPv4 is required in /etc/resolv.conf for `adclient` to find AD services properly.

  Log:

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

  This issue is unique to Centrify and its configuration. To resolve this issue, do the following:

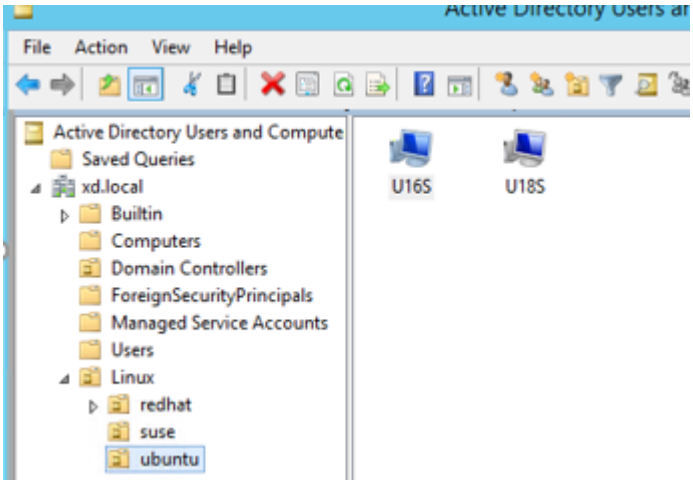
  a. Open **Administrative Tools** on the domain controller.
  b. Select **Active Directory Sites and Services**.
  c. Add a proper subnet address for **Subnets**.

- To join your VDA to a specific OU, do the following:

  1. Ensure that the specific OU exists on the domain controller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For an example OU, see the following screen capture



2. Create the /tmp/ctxinstall.conf file on the VDA.
3. Add the ou=<your ou> line to the /tmp/ctxinstall.conf file.

   OU values vary with different AD methods. The following table reflects the example OU names in the preceding screen capture. You can use any other OU names in your organization.

OS	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	`ou="Linux/amazon"`	`ou="Linux/amazon"`	`ou="XD.LOCAL/Linux/amazon"`	`ou="Linux/amazon"`
Debian	`ou="Linux/debian"`	`ou="Linux/debian"`	`ou="XD.LOCAL/Linux/debian"`	`ou="Linux/debian"`
RHEL 9.0, Rocky Linux 9.0	`ou="OU=redhat,OU=Linux"`	`ou="OU=redhat,OU=Linux"`	N/A	N/A
RHEL 8, Rocky Linux 8	`ou="OU=redhat,OU=Linux"`	`ou="OU=redhat,OU=Linux"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`
RHEL 7	`ou="Linux/redhat"`	`ou="Linux/redhat"`	`ou="XD.LOCAL/Linux/redhat"`	`ou="Linux/redhat"`
SUSE	`ou="Linux/suse"`	`ou="Linux/suse"`	`ou="XD.LOCAL/Linux/suse"`	`ou="Linux/suse"`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

OS	Winbind	SSSD	Centrify	PBIS
Ubuntu	`ou="Linux/ubuntu"`	`ou="Linux/ubuntu"`	`ou="XD.LOCAL/Linux/ubuntu"`	`ou="Linux/ubuntu"`

- Easy install supports pure IPv6 starting from the Linux VDA 7.16. The following preconditions and limitations apply:
  - Your Linux repository must be configured to ensure that your machine can download the required packages over pure IPv6 networks.
  - Centrify is not supported on pure IPv6 networks.

  > **Note:**
  >
  > If your network is pure IPv6 and all your input is in proper IPv6 format, the VDA registers with the Delivery Controller through IPv6. If your network has a hybrid IPv4 and IPv6 configuration, the type of the first DNS IP address determines whether IPv4 or IPv6 is used for registration.

- If you choose Centrify as the method to join a domain, the ctxinstall.sh script requires the Centrify package. There are two ways for ctxinstall.sh to get the Centrify package:
  - Easy install helps download the Centrify package from the Internet automatically. The following are the URLs for each distribution:

    Amazon Linux 2/RHEL: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz

    CentOS: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-rhel6-x86_64.tgz

    SUSE: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-suse12-x86_64.tgz

    Ubuntu/Debian: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-deb9-x86_64.tgz
  - Fetch the Centrify package from a local directory. To designate the directory of the Centrify package, do the following:

    a. Create the /tmp/ctxinstall.conf file on the Linux VDA server if it does not exist.
    b. Add the “centrifypkgpath=<path name>”line to the file.

    For example:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

- If you choose PBIS as the method to join a domain, the ctxinstall.sh script requires the PBIS package. There are two ways for ctxinstall.sh to get the PBIS package:
  - Easy install helps download the PBIS package from the Internet automatically. For example, the following are the URLs for each distribution:

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

    Debian, Ubuntu: `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh`
  - Fetch a specific version of the PBIS package from the Internet. To do so, change the "pbisDownloadRelease"and "pbisDownloadExpectedSHA256"lines in the /opt/Citrix/VDA/sbin/ctxinstall.sh file.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For an example, see the following screen capture:

Step 2: Prepare the hypervisor

Some changes are required when running the Linux VDA as a virtual machine on a supported hypervisor. Make the following changes based on 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 Hypervisor

When the Citrix Hypervisor Time Sync feature is enabled, within each paravirtualized Linux VM you experience issues with NTP and Citrix Hypervisor. Both try to manage the system clock. To avoid the clock becoming out of sync with other servers, make sure that the system clock within each Linux guest is synchronized with the NTP. This case requires disabling host time synchronization. No changes are required in HVM mode.

If you are running a paravirtualized Linux kernel with Citrix VM Tools installed, you can check whether the Citrix Hypervisor Time Sync feature is present and enabled from within the Linux VM:

```
su -

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

This command returns 0 or 1:

- 0 - The time sync feature is enabled, and must 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
<!--NeedCopy-->
```

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

```
xen.independent_wallclock = 1
```

To verify these changes, restart the system:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
su -

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

This command returns the value 1.

Fix time synchronization on Microsoft Hyper-V

The Linux VMs with Hyper-V Linux Integration Services installed can apply the Hyper-V time synchronization feature to use the time of the host operating system. To ensure that the system clock remains accurate, you must enable this feature alongside the 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 that **Time synchronization** is selected.

> **Note:**
>
> This approach is different from VMware and Citrix Hypervisor, 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

When the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you experience issues with the NTP and the hypervisor. Both try to synchronize the system clock. To avoid the clock becoming out of sync with other servers, ensure that the system clock within each Linux guest is synchronized with the NTP. This case 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 3: Install .NET Runtime 6.0

Before installing the Linux VDA, install .NET Runtime 6.0 according to the instructions at https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

After installing .NET Runtime 6.0, run the **which dotnet** command to find your runtime path.

Based on the command output, set the .NET runtime binary path. For example, if the command output is /aa/bb/dotnet, use /aa/bb as the .NET binary path.

Step 4: Download the Linux VDA package

1. Go to the Citrix Virtual Apps and Desktops download page.
2. Expand the appropriate version of Citrix Virtual Apps and Desktops.
3. Click **Components** to download the Linux VDA package that matches your Linux distribution and the GPG public key that you can use to verify the integrity of the Linux VDA package.

   To verify the integrity of the Linux VDA package by using the public key:

   - For an RPM package, import the public key into the RPM database and run the following commands:

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

   - For a DEB package, import the public key into the DEB database and run the following commands:

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

Step 5: Install the Linux VDA package

To set up the environment for the Linux VDA, run the following commands.

For Amazon Linux 2, CentOS, RHEL, and Rocky Linux distributions:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> For RHEL and CentOS, install the EPEL repository before you can install the Linux VDA successfully. For information on how to install EPEL, see the instructions at https://docs.fedoraproject.org/en-US/epel/.

For Ubuntu/Debian distributions:

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

> **Note:**
>
> - To install the necessary dependencies for a Debian 11.3 distribution, add the `deb http://deb.debian.org/debian/ bullseye main` line to the /etc/apt/sources.list file.
> - For Ubuntu 20.04 on GCP, disable RDNS. To do so, add the **rdns = false** line under **[libdefaults]** in /etc/krb5.conf.

For SUSE distributions:

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

Step 6: Install NVIDIA GRID drivers

Enabling HDX 3D Pro requires you to install the NVIDIA GRID drivers on your hypervisor and on the VDA machines.

To install and configure the NVIDIA GRID Virtual GPU Manager (the host driver) on the specific hypervisors, see the following guides:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

To install and configure the NVIDIA GRID guest VM drivers, perform the following general steps:

1. Ensure that the guest VM is shut down.
2. In the hypervisor control panel, allocate a GPU to the VM.
3. Start the VM.
4. Install the guest VM driver on the VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 7: Specify a database to use

As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL by editing `/etc/xdl/db.conf` after installing the Linux VDA package.

To do so, edit `etc/xdl/db.conf` before running `sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` or `/opt/Citrix/VDA/bin/easyinstall`.

> **Note:**
>
> - We recommend you use SQLite for VDI mode only.
> - For easy install and MCS, you can switch between SQLite and PostgreSQL without having to install them manually. Unless otherwise specified through `/etc/xdl/db.conf`, the Linux VDA uses PostgreSQL by default.
> - You can also use `/etc/xdl/db.conf` to configure the port number for PostgreSQL.

Step 8: Set up the runtime environment to complete the installation

After installing the Linux VDA package, configure the running environment by using the ctxinstall.sh script. You can run the script in interactive mode or silent mode.

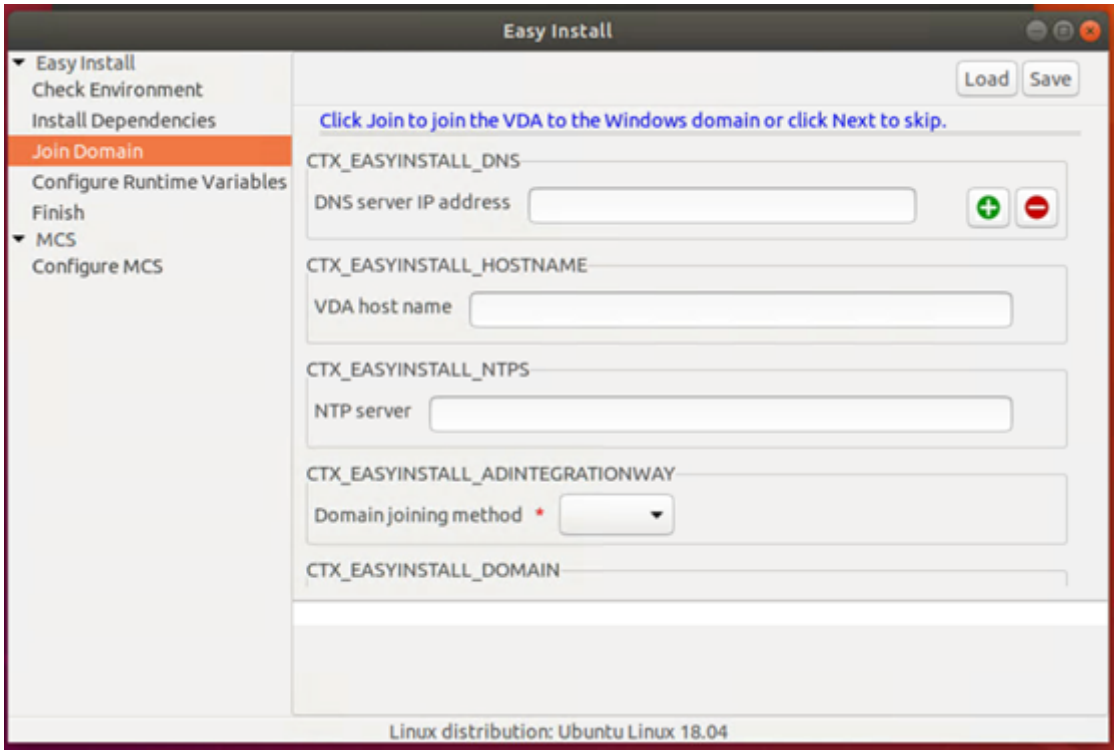
> **Note:**
>
> Before setting up the runtime environment, ensure that the `en_US.UTF-8` locale is installed in your OS. If the locale is not available in your OS, run the `sudo locale-gen en_US.UTF-8` command. For Debian, edit the `/etc/locale.gen` file by uncommenting the `# en_US.UTF-8 UTF-8` line and then run the `sudo locale-gen` command.

Interactive mode:

There are two ways to use easy install in interactive mode:

- Run the `sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` command and type the relevant parameter at each prompt in the command line interface.
- Run the `/opt/Citrix/VDA/bin/easyinstall` command in the desktop environment of your VDA and then follow the instructions on the easy install GUI.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The easy install GUI guides you through the following operations:

- Check the system environment
- Install dependencies
- Join the VDA to a specified domain
- Configure the runtime environment

> **Tip:**
>
> Click **Save** to save variable settings to a local file under the path you specify. Click **Load** to load variable settings from a file that you specify. For information on configuring MCS variables, see Step 3: Prepare a master image.

Silent mode:

To use easy install in silent mode, set the following environment variables before running ctxinstall.sh.

- **CTX_EASYINSTALL_HOSTNAME=host-name** –Denotes the host name of the Linux VDA server.
- **CTX_EASYINSTALL_DNS=ip-address-of-dns** –IP address of DNS.
- **CTX_EASYINSTALL_NTPS=address-of-ntps** –IP address or string name of the NTP server.
- **CTX_EASYINSTALL_DOMAIN=domain-name** –The NetBIOS name of the domain.
- **CTX_EASYINSTALL_REALM=realm-name** –The Kerberos realm name.
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis** –Denotes the Active Directory integration method.
- **CTX_EASYINSTALL_USERNAME=domain-user-name** –Denotes the name of the domain user; used to join the domain.
- **CTX_EASYINSTALL_PASSWORD=password** –Specifies the password of the domain user; used to join the domain.

The ctxsetup.sh script uses the following variables:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** –The Linux VDA supports specifying a Delivery Controller name using a DNS CNAME record.
- **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 must be specified.
- **CTX_XDL_VDA_PORT=port-number** –The Linux VDA communicates with Delivery Controllers through a TCP/IP port.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –The Linux Virtual Desktop services are started after machine startup.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –The Linux VDA services require incoming network connections to be allowed through the system firewall. You can open the required ports (by default ports 80 and 1494) automatically in the system firewall for the Linux Virtual Desktop.
- **CTX_XDL_HDX_3D_PRO=Y | N** –The Linux VDA supports HDX 3D Pro, a set of GPU acceleration technologies designed to optimize the virtualization of rich graphics applications. If HDX 3D Pro is selected, the VDA is configured for VDI desktops (single-session) mode - (that is, 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 the value to Y.
- **CTX_XDL_SITE_NAME=dns-name** –The Linux VDA discovers LDAP servers through DNS. To limit the DNS search results to a local Site, specify a DNS Site name. If unnecessary, set to **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –The Linux VDA queries DNS to discover LDAP servers. If DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP FQDNs with LDAP ports. For example, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. If you specify the LDAP port number as 389, the Linux VDA queries each LDAP server in the specified domain in polling mode. If there are x number of policies and y number of LDAP servers, the Linux VDA performs the total of X multiplied by Y queries. If the polling time exceeds the threshold, session logons might fail. To enable the faster LDAP

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

queries, enable **Global Catalog** on a domain controller and specify the relevant LDAP port number as 3268. This variable is set to **<none>** by default.

- **CTX_XDL_SEARCH_BASE=search-base-set** –The Linux VDA queries LDAP through a search base set to the root of the Active Directory Domain (for example, DC=mycompany,DC=com). To improve search performance, you can specify a search base (for example, OU=VDI,DC=mycompany,DC=com). If unnecessary, set to **<none>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'**–The Federated Authentication Service (FAS) servers are configured through AD Group Policy. The Linux VDA does not support AD Group Policy, but you can provide a semicolon-separated list of FAS servers instead. The sequence must be the same as configured in AD Group Policy. If any server address is removed, fill its blank with the **<none>** text string and do not modify the order of server addresses. To communicate with FAS servers properly, make sure you append a port number consistent with that specified on the FAS servers, for example, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** –The path to install .NET Runtime 6.0 for supporting the new broker agent service (`ctxvda`). The default path is /usr/bin.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate** –Specifies the GNOME, GNOME Classic, or MATE desktop environment to use in sessions. If you leave the variable unspecified, the desktop currently installed on the VDA is used. However, if the currently installed desktop is MATE, you must set the variable value to **mate**.

  You can also change the desktop environment for a target session user by completing the following steps:

  1. Create an `.xsession` or `.Xclients` file under the **$HOME/<username>** directory on the VDA. If you are using Amazon Linux 2, create an `.Xclients` file. If you are using other distributions, create an `.xsession` file.
  2. Edit the `.xsession` or `.Xclients` file to specify a desktop environment based on distributions.

     - **For MATE desktop**

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

     - **For GNOME Classic desktop**

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
3  export GNOME_SHELL_SESSION_MODE=classic
4  exec gnome-session --session=gnome-classic
5  fi
```

- **For GNOME desktop**

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

3. Share the 700 file permission with the target session user.

Starting with Version 2209, session users can customize their desktop environments.To enable this feature, you must install switchable desktop environments on the VDA in advance. For more information, see Custom desktop environments by session users.

- **CTX_XDL_START_SERVICE=Y | N** –Whether or not the Linux VDA services are started when the configuration is complete.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** –The socket port for listening for Citrix Scout. The default port is 7503.
- **CTX_XDL_TELEMETRY_PORT** –The port for communicating with Citrix Scout. The default port is 7502.

If any parameters are not set, the installation rolls back to interactive mode, with a prompt for user input. When all parameters are already set through the environment variables, the ctxinstall.sh script still prompts for user input for the path to install .NET Runtime 6.0.

In silent mode, you must run the following commands to set environment variables and then run the ctxinstall.sh script.

```
1  export CTX_EASYINSTALL_HOSTNAME=host-name
2
3  export CTX_EASYINSTALL_DNS=ip-address-of-dns
4
5  export CTX_EASYINSTALL_NTPS=address-of-ntps
6
7  export CTX_EASYINSTALL_DOMAIN=domain-name
8
9  export CTX_EASYINSTALL_REALM=realm-name
10
11 export CTX_EASYINSTALL_FQDN=ad-fqdn-name
12
13 export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify |
      pbis
14
15 export CTX_EASYINSTALL_USERNAME=domain-user-name
16
17 export CTX_EASYINSTALL_PASSWORD=password
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
18
19 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
20
21 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
22
23 export CTX_XDL_VDA_PORT=port-number
24
25 export CTX_XDL_REGISTER_SERVICE=Y | N
26
27 export CTX_XDL_ADD_FIREWALL_RULES=Y | N
28
29 export CTX_XDL_HDX_3D_PRO=Y | N
30
31 export CTX_XDL_VDI_MODE=Y | N
32
33 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
34
35 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
36
37 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
38
39 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
40
41 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
42
43 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
   none>'
44
45 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
46
47 export CTX_XDL_TELEMETRY_PORT=port-number
48
49 export CTX_XDL_START_SERVICE=Y | N
50
51 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
52 <!--NeedCopy-->
```

When running the sudo command, type the -E option to pass the existing environment variables to the new shell it creates. We recommend that you create a shell script file from the preceding commands with **#!/bin/bash** as the first line.

Alternatively, you can specify all parameters by using a single command:

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Step 9: Run XDPing

Run `sudo /opt/Citrix/VDA/bin/xdping` to check for common configuration issues with a Linux VDA environment. For more information, see XDPing.

Step 10: Run the Linux VDA

Start the Linux VDA:

To start the Linux VDA services:

```
sudo /sbin/service ctxhdx start

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

Stop the Linux VDA:

To stop the Linux VDA services:

```
sudo /sbin/service ctxvda stop

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

> **Note:**
>
> Before you stop the `ctxvda` and `ctxhdx` services, run the `service ctxmonitorservice stop` command to stop the monitor service daemon. Otherwise, the monitor service daemon restarts the services you stopped.

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
<!--NeedCopy-->
```

Check the status of the Linux VDA:

To check the running status of the Linux VDA services:

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

Step 11: Create machine catalogs

The process for creating machine catalogs and adding Linux VDA machines is 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:
  - The **Multi-session OS** option for a hosted shared desktops delivery model.
  - The **Single-session OS** option for a VDI dedicated desktop delivery model.
- 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 deliv-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ery model. Selecting the **Windows Desktop OS** or **Desktop OS** option implies a single user per machine delivery model.
>
> **Tip:**
>
> If you remove and rejoin a machine to the Active Directory domain, you must remove and add the machine to the machine catalog again.

Step 12: Create delivery groups

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:

- Ensure that the AD users and groups that 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.

For information about how to create machine catalogs and delivery groups, see Citrix Virtual Apps and Desktops 7 2212.

Troubleshooting

Use the information in this section to troubleshoot issues that can arise from using the easy install feature.

Joining a domain by using SSSD fails

An error might occur when you attempt to join a domain, with the output similar to the following (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'over rpc: The
network name cannot be found
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

/var/log/xdl/vda.log:

```
2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service
    successfully obtained the following list of 1 delivery controller(s)
     with which to register: 'CTXDDC.citrixlab.local (10.158.139.214)'.
2016-11-04 02:11:52.362 [ERROR] - RegistrationManager.
    AttemptRegistrationWithSingleDdc: Failed to register with http://
    CTXDDC.citrixlab.local:80/Citrix/CdsController/IRegistrar. Error:
    General security error (An error occurred in trying to obtain a TGT:
     Client not found in Kerberos database (6))
2016-11-04 02:11:52.362 [ERROR] - The Citrix Desktop Service cannot
    connect to the delivery controller 'http://CTXDDC.citrixlab.local
    :80/Citrix/CdsController/IRegistrar' (IP Address '10.158.139.214')
Check the following:- The system clock is in sync between this machine
    and the delivery controller.
-  The Active Directory provider (e.g. winbind daemon) service is
    running and correctly configured.
-  Kerberos is correctly configured on this machine.
If the problem persists, please refer to Citrix Knowledge Base article
    CTX117248 for further information.
Error Details:
Exception 'General security error (An error occurred in trying to
    obtain a TGT: Client not found in Kerberos database (6))' of type '
    class javax.xml.ws.soap.SOAPFaultException'.
2016-11-04 02:11:52.362 [INFO ] - RegistrationManager.
    AttemptRegistrationWithSingleDdc: The current time for this VDA is
    Fri Nov 04 02:11:52 EDT 2016.
Ensure that the system clock is in sync between this machine and the
    delivery controller.
Verify the NTP daemon is running on this machine and is correctly
    configured.
2016-11-04 02:11:52.364 [ERROR] - Could not register with any
    controllers. Waiting to try again in 120000 ms. Multi-forest - false
2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
    register with any controllers in the last 470 minutes.
<!--NeedCopy-->
```

/var/log/messages:

```
Nov 4 02:15:27 RH-WS-68 [sssd[ldap_child[14867]]]: Failed to initialize
 credentials using keytab [MEMORY:/etc/krb5.keytab]: Client 'RH-WS-68
$@CITRIXLAB.LOCAL'not found in Kerberos database. Unable to create
 GSSAPI-encrypted LDAP connection.Nov 4 02:15:27 RH-WS-68 [sssd[
ldap_child[14867]]]: Client 'RH-WS-68$@CITRIXLAB.LOCAL'not found
in Kerberos database
```

To resolve this issue:

1. Run the `rm -f /etc/krb5.keytab` command.
2. Run the `net ads leave $REALM -U $domain-administrator` command.
3. Remove the machine catalog and delivery group on the Delivery Controller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Run /opt/Citrix/VDA/sbin/ctxinstall.sh.
5. Create the machine catalog and delivery group on the Delivery Controller.

Ubuntu desktop sessions show a gray screen

This issue occurs when you launch a session that is then blocked in a blank desktop. In addition, the console of the machine also shows a gray screen when you log on by using a local user account.

To resolve this issue:

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

Attempts to launch Ubuntu desktop sessions fail due to a missing home directory

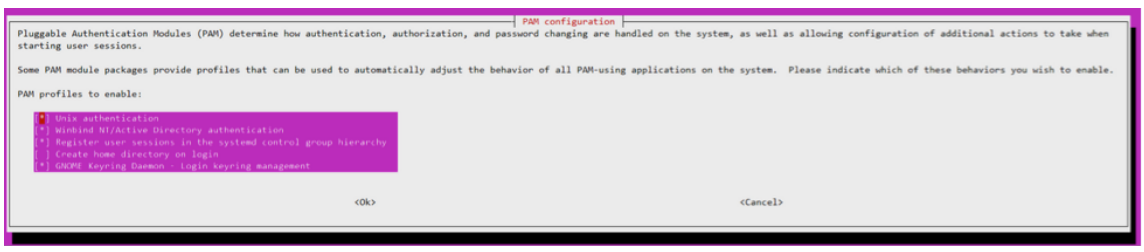
/var/log/xdl/hdx.log:

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

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

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

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

> **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, type **pam-auth-update**.
2. In the resulting dialog, verify that **Create home directory login** is selected.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Session does not launch or ends quickly with dbus 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)#012aborting...

Oct 27 04:17:18 CentOS7 gnome-session: gnome-session[19146]: ERROR:
    Failed to connect to system bus: Exhausted all available
    authentication mechanisms (tried: EXTERNAL, DBUS_COOKIE_SHA1,
    ANONYMOUS) (available: EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS)

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

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

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

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

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

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] bluez5-
    util.c: Failed to get D-Bus connection: Did not receive a reply.
    Possible causes include: the remote application did not send a reply
    , the message bus security policy blocked the reply, the reply
    timeout expired, or the network connection was broken.

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] hashmap
    .c: Assertion 'h' failed at pulsecore/hashmap.c:116, function
    pa_hashmap_free(). Aborting.

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] core-
    util.c: Failed to connect to system bus: Did not receive a reply.
    Possible causes include: the remote application did not send a reply
    , the message bus security policy blocked the reply, the reply
    timeout expired, or the network connection was broken.

Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
    times: [ [pulseaudio] core-util.c: Failed to connect to system bus:
    Did not receive a reply. Possible causes include: the remote
    application did not send a reply, the message bus security policy
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
      blocked the reply, the reply timeout expired, or the network
      connection was broken.]
10
11 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
      Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-ctxgfx
      [24693]: Exiting normally
12 <!--NeedCopy-->
```

Some groups or modules do not take effect until a restart. If the **dbus** error messages appear in the log, we recommend that you restart the system and retry.

SELinux prevents SSHD from accessing the home directory

The user can launch a session but cannot log on.

/var/log/ctxinstall.log:

```
1  Jan 25 23:30:31 yz-rhel72-1 setroubleshoot[3945]: SELinux is preventing
       /usr/sbin/sshd from setattr access on the directory /root. For
      complete SELinux messages. run sealert -l 32f52c1f-8ff9-4566-a698
      -963a79f16b81
2
3  Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/
      sbin/sshd from setattr access on the directory /root.
4
5  *****  Plugin catchall_boolean (89.3 confidence) suggests
      ******************
6
7  If you want to allow polyinstantiation to enabled
8
9     Then you must tell SELinux about this by enabling the '
      polyinstantiation_enabled' boolean.
10
11 You can read 'None' man page for more details.
12
13     Do
14
15        setsebool -P polyinstantiation_enabled 1
16
17 *****  Plugin catchall (11.6 confidence) suggests
      **************************
18
19 If you believe that sshd should be allowed setattr access on the root
      directory by default.
20
21 Then you should report this as a bug.
22
23 You can generate a local policy module to allow this access.
24
25       Do
26
27        allow this access for now by executing:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
28
29          # grep sshd /var/log/audit/audit.log | audit2allow -M mypol
30
31  # semodule -i mypol.pp
32  <!--NeedCopy-->
```

To resolve this issue:

1. Disable SELinux by making the following change to /etc/selinux/config.

   SELINUX=disabled

2. Restart the VDA.

Create non-domain-joined Linux VDAs

January 23, 2023

This article walks you through using Machine Creation Services (MCS) to create non-domain-joined Linux VDAs in Citrix DaaS.

> **Important:**
>
> - Non-domain-joined VDAs are supported for Citrix DaaS.
>   - Your control plane must be deployed over Citrix DaaS.
>   - You can deploy non-domain-joined VDAs in a public cloud or on-premises data center. Non-domain-joined VDAs are managed by the control plane in Citrix DaaS.
>   - You can configure Rendezvous V2 to bypass Citrix Cloud Connectors. Otherwise, you must install Cloud Connectors to connect VDAs with your control plane.
> - To create non-domain-joined VDAs, you must use MCS.
>   - Bare metal servers are not supported by MCS.
> - The following features are available for non-domain-joined Linux VDAs:
>   - Create local users with specified attributes on non-domain-joined VDAs
>   - Non-SSO authentication
>   - Authentication with Azure Active Directory
>   - Rendezvous V2

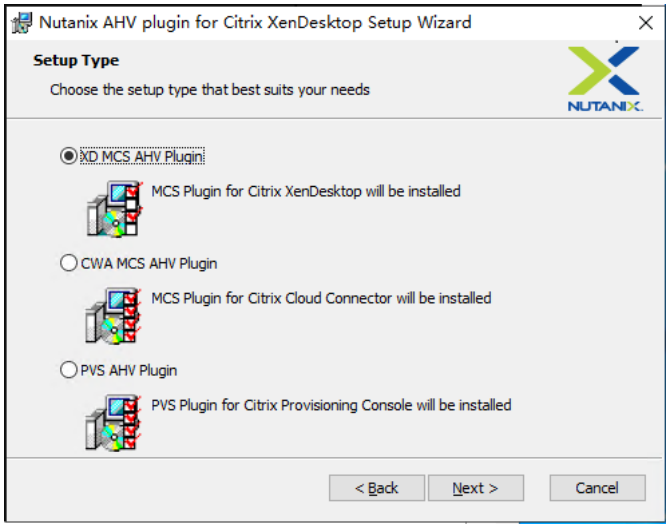
(For Nutanix only) Step 1: Install and register the Nutanix AHV plug-in

Obtain the Nutanix AHV plug-in package from Nutanix. Install and register the plug-in in your Citrix Virtual Apps and Desktops environment. For more information, see the Nutanix Acropolis MCS plug-in installation guide, available at the Nutanix Support Portal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 1a: Install and register the Nutanix AHV plug-in for on-premises Delivery Controllers

After you install Citrix Virtual Apps and Desktops, select and install the **XD MCS AHV Plugin** on your Delivery Controllers.



Step 1b: Install and register the Nutanix AHV plug-in for cloud Delivery Controllers

Select and install the **CWA MCS AHV Plugin** for Citrix Cloud Connectors. Install the plug-in on all Citrix Cloud Connectors that are registered with the Citrix Cloud tenant. You must register Citrix Cloud Connectors even when they serve a resource location without the AHV.

Step 1c: Complete the following steps after installing the plug-in

- Verify that a Nutanix Acropolis folder has been created in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`.
- Run the `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"` command.
- Restart the Citrix Host, Citrix Broker, and Citrix Machine Creation Services on your on-premises Delivery Controllers or restart the Citrix RemoteHCLServer Service on Citrix Cloud Connectors.

  > **Tip:**
  >
  > We recommend that you stop and then restart the Citrix Host, Citrix Broker, and Machine Creation Services when you install or update the Nutanix AHV plug-in.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

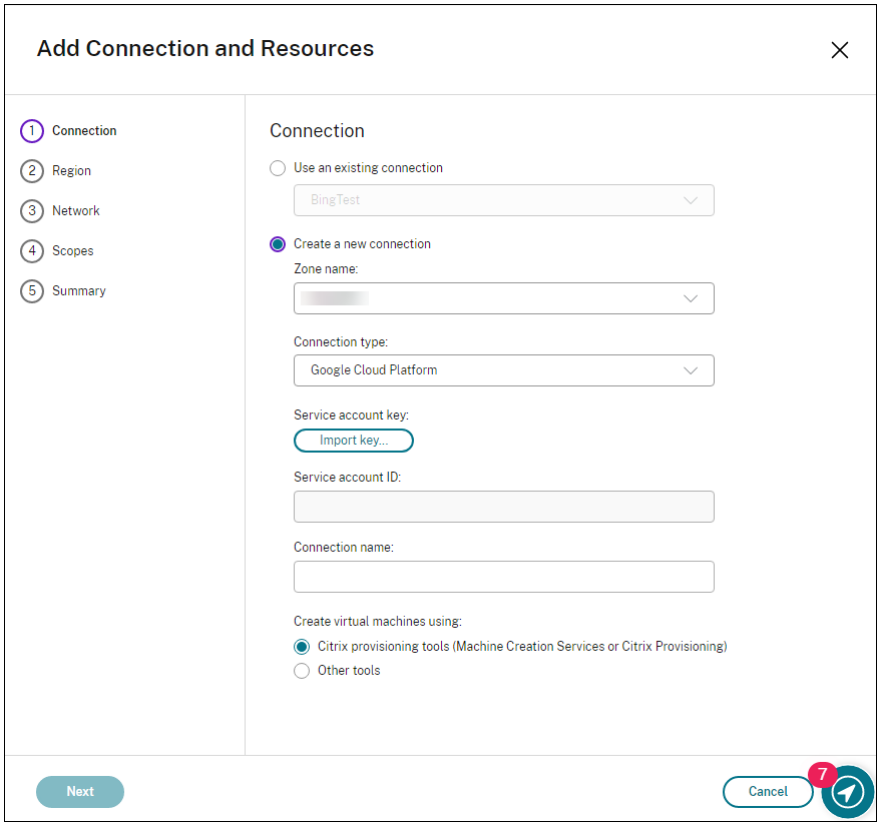
Step 2: Create a host connection

Hosts are hypervisors or cloud services that are in use in your resource locations. This step lets you specify information that DaaS uses to communicate with VMs on a host. Detailed information includes the resource location, host type, access credentials, storage method to use, and which networks the VMs on the host can use.

> **Important:**
>
> The host resources (storage and network) in your resource location must be available before you create a connection.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. From **Manage > Full Configuration**, select **Hosting** in the left pane.
4. Select **Add Connections and Resources** in the action bar.
5. The wizard guides you through the following pages. Specific page content depends on the selected connection type. After completing each page, select **Next** until you reach the **Summary** page.

Step 2a: Connection



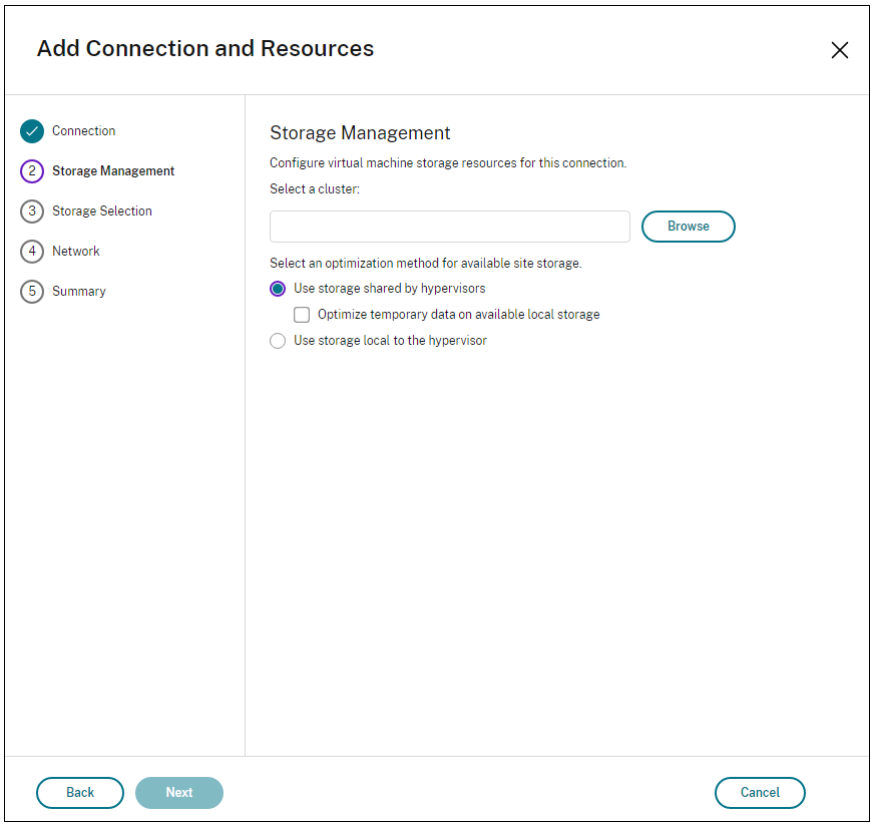
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

On the **Connection** page:

- To create a new connection, select **Create a new Connection**. To create a connection based on the same host configuration as an existing connection, select **Use an existing Connection** and then choose the relevant connection.
- Select a zone in the **Zone name** field. The options are all resource locations you configured.
- Select a hypervisor or cloud service in the **Connection type** field. The options are hypervisors and cloud services that have their plug-ins installed properly in the zone.
  Alternatively, you can use the PowerShell command `Get-HypHypervisorPlugin -ZoneUid` to get the list of hypervisor plug-ins available with the selected zone.
- Enter a connection name. This name appears in the **Manage** display.
- Choose the tool to create virtual machines: Machine Creation Services or Citrix Provisioning.

Information on the **Connection** page differs depending on the host (connection type) you're using. For example, when using Azure Resource Manager, you can use an existing service principal or create a new one.

Step 2b: Storage management



For information about storage management types and methods, see Host storage.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

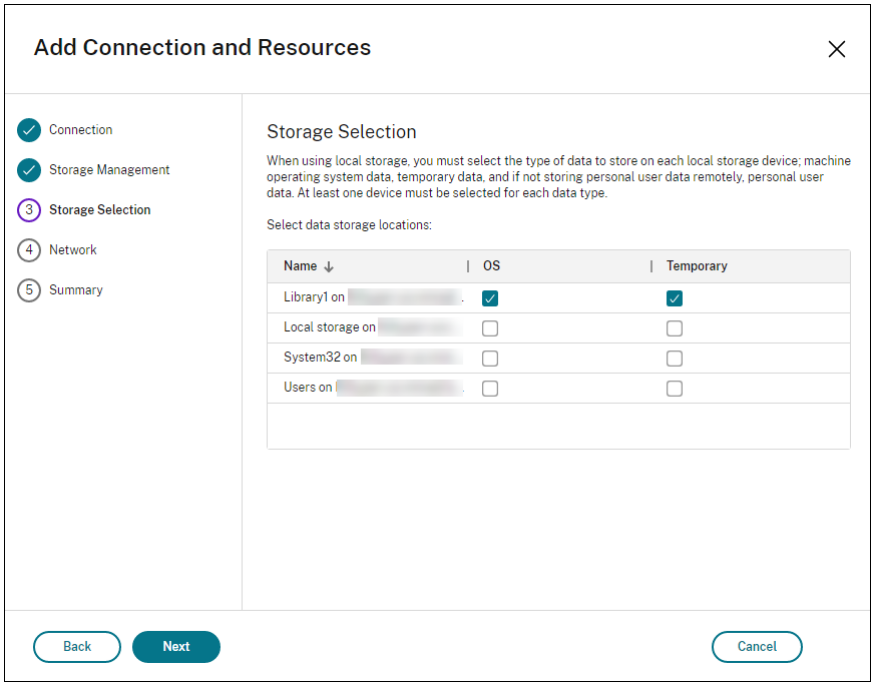
If you are configuring a connection to a Hyper-V or VMware host, browse to and then select a cluster name. Other connection types do not request a cluster name.

Select a storage management method: storage shared by hypervisors or storage local to the hypervisor.

- If you choose storage shared by hypervisors, indicate if you want to keep temporary data on available local storage. (You can specify nondefault temporary storage sizes in the machine catalogs that use this connection.) **Exception:** When using Clustered Storage Volumes (CSV), Microsoft System Center Virtual Machine Manager does not allow temporary data cache disks to be created on local storage. Attempts to configure that storage management setup in the **Manage** console fails.

If you use shared storage in a Citrix Hypervisor pool, indicate if you want to use IntelliCache to reduce the load on the shared storage device. See Citrix Hypervisor virtualization environments.

Step 2c: Storage selection



For more information about storage selection, see Host storage.

Select at least one host storage device for each available data type. The storage management method that you selected on the previous page affects which data types are available for selection on this page. You must select at least one storage device for each supported data type before you can proceed to the next page in the wizard.

The lower portion of the **Storage Selection** page contains more configuration options if you chose

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

storage shared by hypervisors and enabled **Optimize temporary data on available local storage**. You can select which local storage devices (in the same hypervisor pool) to use for temporary data.

The number of currently selected storage devices is shown (in the graphic, "1 storage device selected"). When you hover over that entry, the selected device names appear (unless no devices are configured).

1. Select **Select** to change the storage devices to use.
2. In the **Select Storage** dialog box, select or clear the storage device check boxes, and then select **OK**.

Step 2d: Region

(Appears only for some host types.) The region selection indicates where VMs will be deployed. Ideally, choose a region close to where users access their applications.

Step 2e: Network

Enter a name for the resources. This name appears in the **Manage** console to identify the storage and network combination associated with the connection.
Select one or more networks that the VMs use.

Some connection types (such as Azure Resource Manager) also list subnets that VMs use. Select one or more subnets.

Step 2f: Summary

Review your selections; if you want to make changes, use return to previous wizard pages. When you complete your review, select **Finish**.

Remember: If you store temporary data locally, you can configure nondefault values for temporary data storage when you create the catalog containing machines that use this connection.

> **Note:**
>
> A scope is not shown for Full access administrators. For more information, see Administrators, roles, and scopes.

For more information, see Create and manage connections.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 3: Prepare a master image

> **Tip:**
>
> You can use a single image for creating both domain-joined and non-domain-joined VDAs.

(For Citrix Hypervisor only) Step 3a: Install Citrix VM Tools

Install Citrix VM Tools on the template VM for each VM to use the xe CLI or XenCenter. VM performance can be slow unless you install the tools. Without the tools, you can't do any of the following:

- Cleanly shut down, restart, or suspend a VM.
- View the VM performance data in XenCenter.
- Migrate a running VM (through XenMotion).
- Create snapshots or snapshots with memory (checkpoints), and revert to snapshots.
- Adjust the number of vCPUs on a running Linux VM.

1. Run the following command to mount Citrix VM Tools named guest-tools.iso.

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

2. Run the following command to install the xe-guest-utilities package based on your Linux distribution.

   For RHEL/CentOS/Rocky Linux:

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

   For Ubuntu/Debian:

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

   For SUSE:

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

3. Check the virtualization state of the template VM on the **General** tab in XenCenter. If Citrix VM Tools are installed correctly, the virtualization state is **Optimized**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

(For Azure, AWS, and GCP) Step 3b: Configure cloud-init for Ubuntu 18.04

1. To ensure that a VDA host name persists when a VM is restarted or stopped, run the following command:

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

   Verify that the following lines are present under the **system_info** section in the /etc/cloud/-cloud.cfg file:

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

2. To use SSH for remotely accessing MCS-created VMs on AWS, enable password authentication because no key name is attached to those VMs. Do the following as needed.

   - Edit the `cloud-init` configuration file, /etc/cloud/cloud.cfg. Ensure that the **ssh_pwauth: true** line is present. Remove or comment the **set-password** line and the following lines if they exist.

```
users:
- default
<!--NeedCopy-->
```

   - If you plan to use the default user `ec2-user` or `ubuntu` created by `cloud-init`, you can change the user password by using the `passwd` command. Keep the new password in mind for later use to log in to the MCS-created VMs.
   - Edit the `/etc/ssh/sshd_config` file to ensure that the following line is present:

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

     Save the file and run the `sudo service sshd restart` command.

Step 3c: Install the Linux VDA package on the template VM

> **Note:**
>
> To use a currently running VDA as the template VM, skip this step.
>
> Before installing the Linux VDA package on the template VM, install .NET Runtime 6.0.

Based on your Linux distribution, run the following command to set up the environment for the Linux VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For RHEL/CentOS/Rocky Linux:

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

> **Note:**
>
> For RHEL and CentOS, install the EPEL repository before you can install the Linux VDA and run `deploymcs.sh` successfully. For information on how to install EPEL, see the instructions at https://docs.fedoraproject.org/en-US/epel/.

For Ubuntu/Debian:

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

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

For SUSE:

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

Step 3d: Enable repositories to install the tdb-tools package (for RHEL 7 only)

For RHEL 7 server:

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

For RHEL 7 workstation:

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

Step 3e: (On SUSE) Manually install ntfs-3g

On the SUSE platform, no repository provides ntfs-3g. Download the source code, compile, and install ntfs-3g manually:

1. Install the GNU Compiler Collection (GCC) compiler system and the make package:

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

2. Download the ntfs-3g package.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Decompress the ntfs-3g package:

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

4. Enter the path to the ntfs-3g package:

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

5. Install ntfs-3g:

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

Step 3f: Specify a database to use

As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL after installing the Linux VDA package. To do so, complete the following steps:

1. Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.
2. Edit `/etc/xdl/db.conf` before running `deploymcs.sh`.

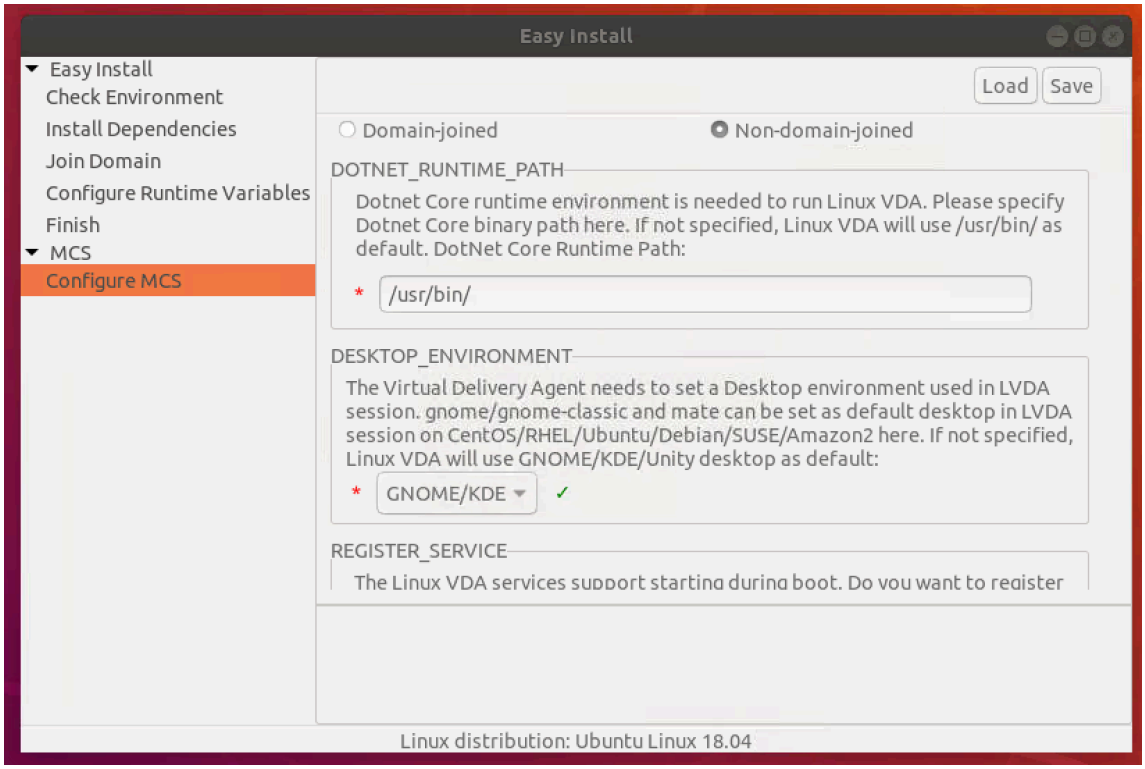
> **Note:**
>
> - We recommend you use SQLite for VDI mode only.
> - For easy install and MCS, you can switch between SQLite and PostgreSQL without having to install them manually. Unless otherwise specified through `/etc/xdl/db.conf`, the Linux VDA uses PostgreSQL by default.
> - You can also use `/etc/xdl/db.conf` to configure the port number for PostgreSQL.

Step 3g: Configure MCS variables

There are two ways to configure MCS variables:

- Edit the `/etc/xdl/mcs/mcs.conf` file.
- Use the easy install GUI. To open the easy install GUI, run the `/opt/Citrix/VDA/bin/easyinstall` command in the desktop environment of your Linux VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Tip:**
>
> Click **Save** to save variable settings to a local file under the path you specify. Click **Load** to load variable settings from a file that you specify.

The following are MCS variables that you can configure for non-domain-joined scenarios. You can use the default variable values or customize the variables as required (optional):

```
DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
DESKTOP_ENVIRONMENT= **gnome | mate \**
REGISTER_SERVICE=**Y | N**
ADD_FIREWALL_RULES=**Y | N**
VDI_MODE=**Y | N**
START_SERVICE=**Y | N**
```

Step 3h: Write or update registry values for MCS (optional)

On the template machine, add command lines to the `/etc/xdl/mcs/mcs_local_setting.reg` file for writing or updating registry values as required. This action prevents the loss of data and settings every time an MCS-provisioned machine restarts.

Each line in the `/etc/xdl/mcs/mcs_local_setting.reg` file is a command for setting or updating a registry value.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

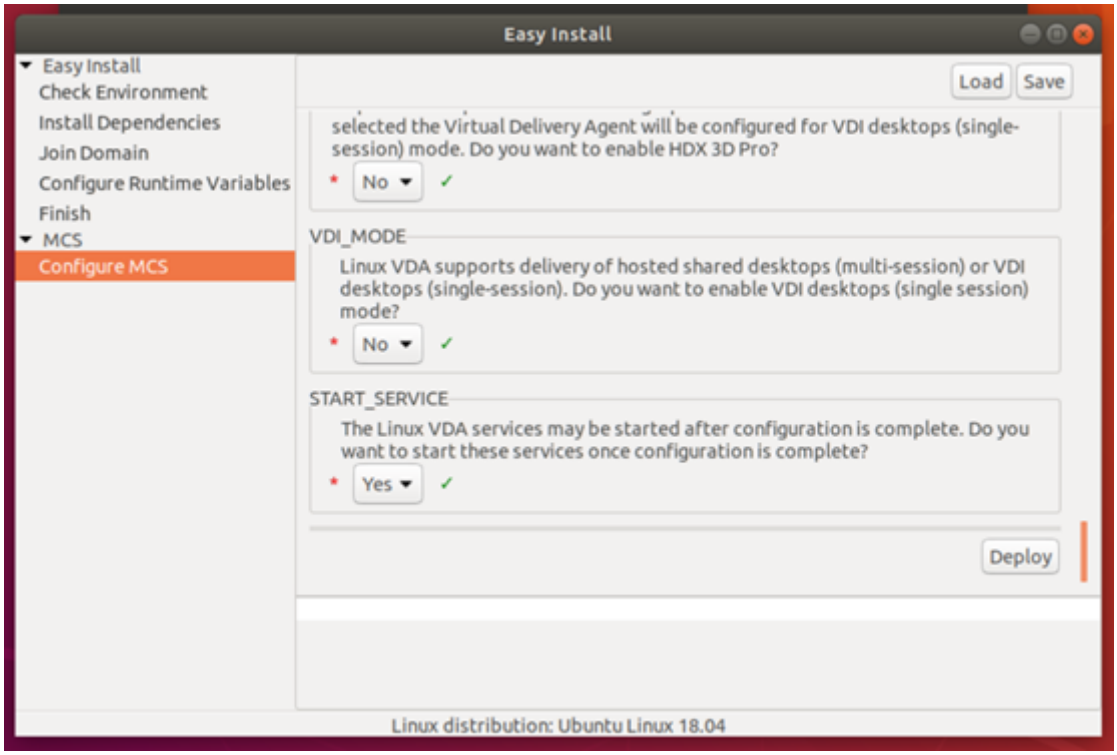
For example, you can add the following command lines to the /etc/xdl/mcs/mcs_local_setting.reg file to write or update a registry value respectively:

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

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

Step 3i: Create a master image

1. If you configure MCS variables by editing /etc/xdl/mcs/mcs.conf, run /opt/Citrix/VDA/sbin/deploymcs.sh. If you configure MCS variables by using the GUI, click **Deploy**.



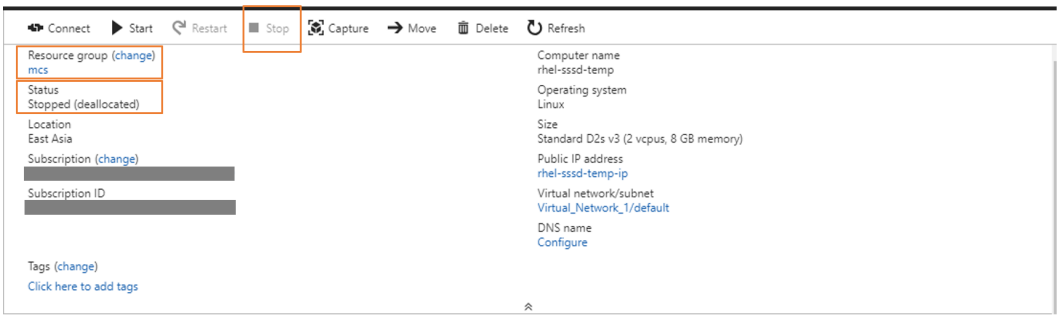
   After you click **Deploy** on the GUI, the variables you set on the GUI override the variables you set in the /etc/xdl/mcs/mcs.conf file.

2. Create and name a snapshot of your master image based on the public cloud you use.

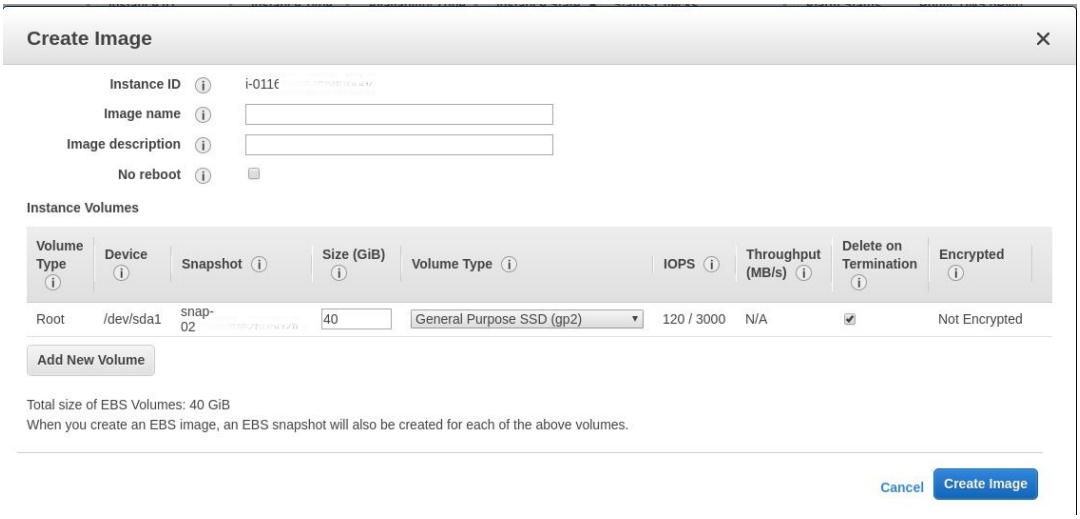
   - **(For Citrix Hypervisor, GCP, and VMware vSphere)** Install applications on the template VM and shut down the template VM. Create and name a snapshot of your master image.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **(For Azure)** Install applications on the template VM and shut down the template VM from the Azure portal. Ensure that the power status of the template VM is **Stopped (deallocated)**. Remember the name of the resource group here. You need the name to locate your master image on Azure.



- **(For AWS)** Install applications on the template VM and shut down the template VM from the AWS EC2 portal. Ensure that the instance state of the template VM is **Stopped**. Right-click the template VM and select **Image > Create Image**. Type information and make settings as needed. Click **Create Image**.



- **(For Nutanix)** On Nutanix AHV, shut down the template VM. Create and name a snapshot of your master image.

> **Note:**
>
> You must prefix Acropolis snapshot names with XD_ for use in Citrix Virtual Apps and Desktops. Use the Acropolis console to rename your snapshots when needed. After you rename a snapshot, restart the **Create Catalog** wizard to obtain a refreshed list.

Step 4: Create a machine catalog

1. Sign in to Citrix Cloud.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. In the upper left menu, select **My Services > DaaS**.
3. From **Manage > Full Configuration**, select **Machine Catalogs**.
4. The wizard guides you to create a machine catalog.

   On the **Container** page that is unique to Nutanix, select the container that you specified for the template VM earlier.

   On the **Master Image** page, select the image snapshot.

   On the **Virtual Machines** page, check for the number of virtual CPUs and the number of cores per vCPU. Select MCS as the machine deployment method and select **Non-domain-joined** as the identity for machines to be created in the catalog.

   Do other configuration tasks as needed. For more information, see Create machine catalogs.

> **Note:**
>
> If your machine catalog creation process on the Delivery Controller takes a significant amount of time, go to Nutanix Prism and power on the machine prefixed with **Preparation** manually. This approach helps to continue the creation process.

Step 5: Create a delivery group

A delivery group is a collection of machines selected from one or more machine catalogs. It specifies which users can use those machines, and the applications and desktops available to those users. For more information, see Create delivery groups.

Create Linux VDAs using Machine Creation Services (MCS)

November 30, 2023

You can create domain-joined and non-domain-joined VDAs using MCS.

> **Important:**
>
> The following are important changes starting with the 2212 release:
>
> - This **AD_INTEGRATION** variable in the /etc/xdl/mcs/mcs.conf file or on the easy install GUI does not have a default value any longer. You must set a value as needed. For more information, see the Step 3h: Configure MCS variables section in this article.
> - The valid value of the **UPDATE_MACHINE_PW** entry in /etc/xdl/mcs/mcs.conf is no longer **enabled** or **disabled**, but **Y** or **N**. For more information, see the Automate machine account

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> password updates section in this article.

Supported distributions

	Winbind	SSSD	Centrify	PBIS
Debian 11.3	Yes	Yes	No	Yes
RHEL 9.0	Yes	No	No	No
RHEL 8.6, RHEL 8.4	Yes	No	Yes	Yes
Rocky Linux 9.0	Yes	No	No	No
Rocky Linux 8.6	Yes	No	No	No
RHEL 7.9, CentOS 7.9	Yes	Yes	Yes	Yes
SUSE 15.3	Yes	Yes	No	Yes
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Yes	Yes	No	Yes

Supported hypervisors

- AWS
- Citrix Hypervisor
- GCP
- Microsoft Azure
- Nutanix AHV
- VMware vSphere

Unexpected results can occur if you try to prepare a master image on hypervisors other than the supported ones.

Use MCS to create Linux VMs

Considerations

- From Citrix Virtual Apps and Desktops 7 2003 through Citrix Virtual Apps and Desktops 7 2112, hosting the Linux VDA on Microsoft Azure, AWS, and GCP was supported only for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Starting with the 2203 release, you can host the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Linux VDA on these public clouds for both Citrix DaaS and Citrix Virtual Apps and Desktops. To add these public cloud host connections to your Citrix Virtual Apps and Desktops deployment, you need **Hybrid Rights License**. For information about **Hybrid Rights License**, see Transition and Trade-Up (TTU) with Hybrid Rights.

- Bare metal servers are not supported for use with MCS to create virtual machines.
- Citrix uses the following Centrify versions for initial feature validation on the relevant Linux distributions:

Linux distribution	Centrify version
RHEL 7/8	5.8.0
SUSE	5.7.1
Debian, Ubuntu	5.6.1

Using other versions of Centrify might cause errors. Do not use Centrify to join a template machine to a domain.

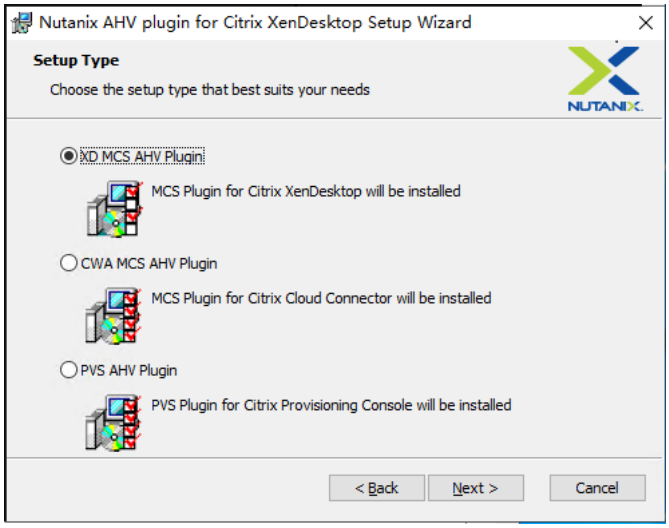
- If you are using PBIS or Centrify for joining MCS-created machines to Windows domains, complete the following tasks:
  - On the template machine, configure the PBIS or Centrify package download path in the `/etc/xdl/mcs/mcs.conf` file or install the PBIS or Centrify package directly.
  - Before you run `/opt/Citrix/VDA/sbin/deploymcs.sh`, create an Organizational Unit (OU) that has write and password reset permissions to all its subordinate, MCS-created machines.
  - Before you restart MCS-created machines after `/opt/Citrix/VDA/sbin/deploymcs.sh` finishes running, run `klist -li 0x3e4 purge` on your Delivery Controller or on your Citrix Cloud Connector based on your deployment.

(For Nutanix only) Step 1: Install and register the Nutanix AHV plug-in

Obtain the Nutanix AHV plug-in package from Nutanix. Install and register the plug-in in your Citrix Virtual Apps and Desktops environment. For more information, see the Nutanix Acropolis MCS plug-in installation guide, available at the Nutanix Support Portal.

Step 1a: Install and register the Nutanix AHV plug-in for on-premises Delivery Controllers After you install Citrix Virtual Apps and Desktops, select and install the **XD MCS AHV Plugin** on your Delivery Controllers.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Step 1b: Install and register the Nutanix AHV plug-in for cloud Delivery Controllers Select and install the **CWA MCS AHV Plugin** for Citrix Cloud Connectors. Install the plug-in on all Citrix Cloud Connectors that are registered with the Citrix Cloud tenant. You must register Citrix Cloud Connectors even when they serve a resource location without the AHV.

Step 1c: Complete the following steps after installing the plug-in

- Verify that a Nutanix Acropolis folder has been created in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`.
- Run the `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"` command.
- Restart the Citrix Host, Citrix Broker, and Citrix Machine Creation Services on your on-premises Delivery Controllers or restart the Citrix RemoteHCLServer Service on Citrix Cloud Connectors.

  > **Tip:**
  >
  > We recommend that you stop and then restart the Citrix Host, Citrix Broker, and Machine Creation Services when you install or update the Nutanix AHV plug-in.

Step 2: Create a host connection

This section walks you through creating a host connection to Azure, AWS, GCP, Nutanix AHV, and VMware vSphere:

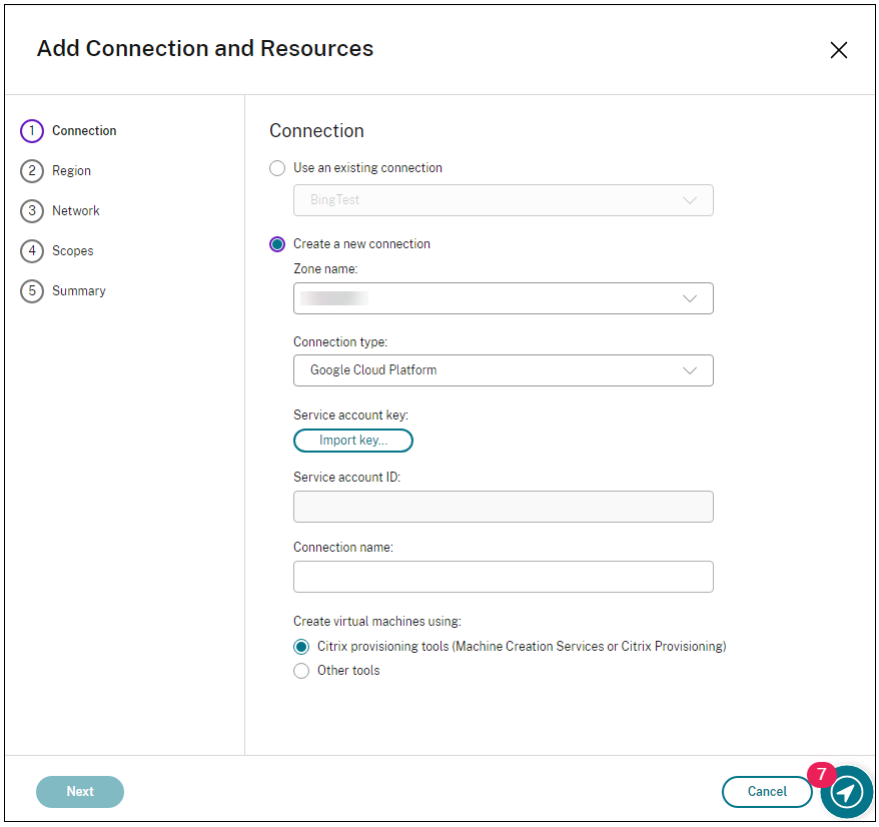
- Create a host connection to Azure in Citrix Studio

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Create a host connection to AWS in Citrix Studio
- Create a host connection to GCP in Citrix Studio
- Create a host connection to Nutanix in Citrix Studio
- Create a host connection to VMware in Citrix Studio

Create a host connection to Azure in Citrix Studio

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.
3. From **Manage > Full Configuration**, select **Hosting** in the left pane.
4. Select **Add Connection and Resources** in the action bar.

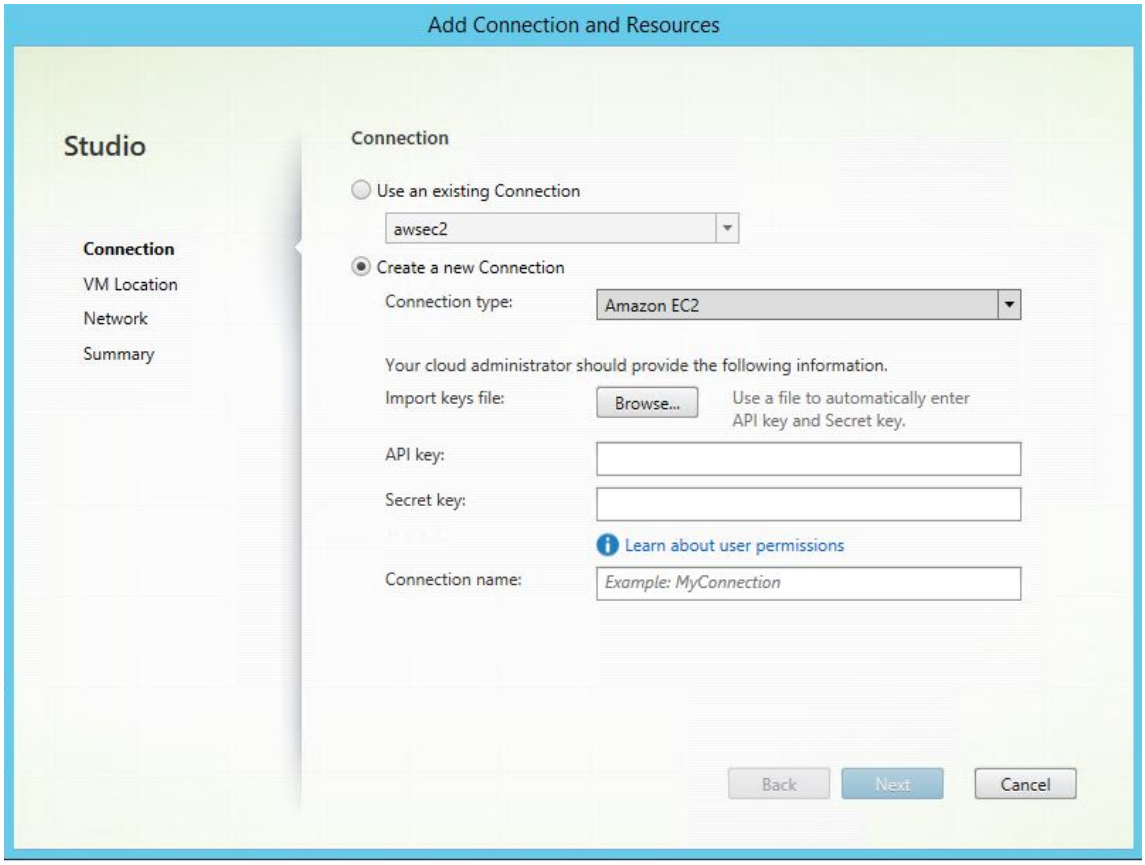


5. Select Microsoft Azure as the connection type.
6. The wizard guides you through pages. Specific page content depends on the selected connection type. After completing each page, select **Next** until you reach the **Summary** page. For more information, see Step 2: Create a host connection in the Create non-domain-joined Linux VDAs article.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

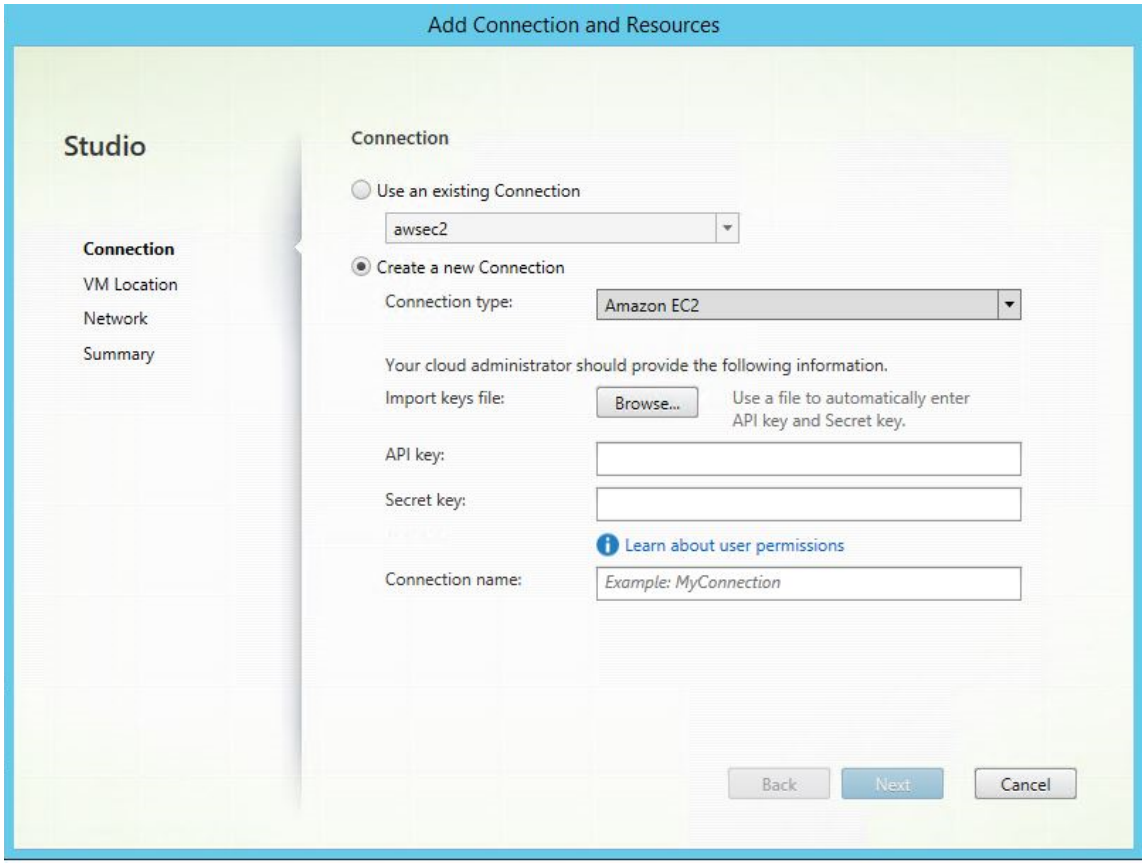
Create a host connection to AWS in Citrix Studio

1. In Citrix Studio, choose **Configuration** > **Hosting** > **Add Connection and Resources**.
2. Choose **Amazon EC2** as the connection type.



3. Type the API key and secret key of your AWS account and type your connection name.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The **API key** is your access key ID and the **Secret key** is your secret access key. They are considered as an access key pair. If you lose your secret access key, you can delete the access key and create another one. To create an access key, do the following:

a) Sign in to the AWS services.
b) Navigate to the Identity and Access Management (IAM) console.
c) On the left navigation pane, choose **Users**.
d) Select the target user and scroll down to select the **Security credentials** tab.
e) Scroll down and click **Create access key**. A new window appears.
f) Click **Download .csv file** and save the access key to a secure location.

4. The wizard guides you through pages. Specific page content depends on the selected connection type. After completing each page, select **Next** until you reach the **Summary** page.

Create a host connection to GCP in Citrix Studio Set up your GCP environment according to Google Cloud Platform virtualization environments and then complete the following steps to create a host connection to GCP.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > DaaS**.

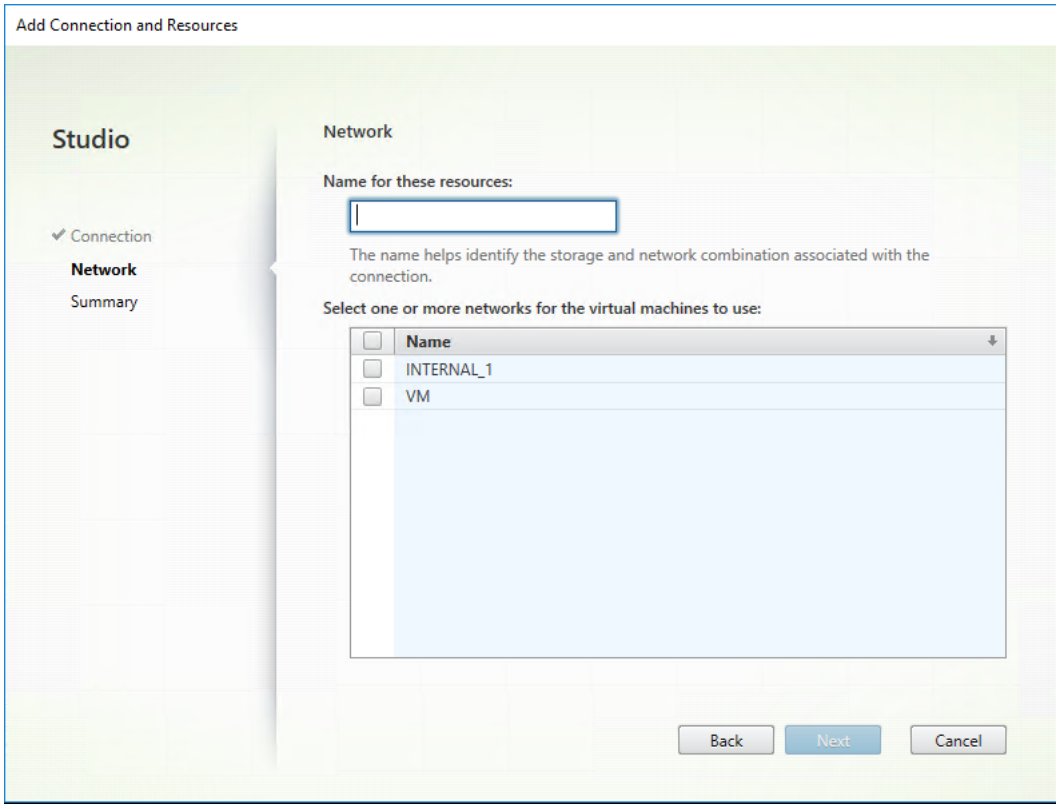
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. From **Manage > Full Configuration**, select **Hosting** in the left pane.
4. Select **Add Connection and Resources** in the action bar.
5. Select **Google Cloud Platform** as the connection type.
6. Import the service account key of your GCP account and type your connection name.
7. The wizard guides you through pages. Specific page content depends on the selected connection type. After completing each page, select **Next** until you reach the **Summary** page. For more information, see Step 2: Create a host connection in the Create non-domain-joined Linux VDAs article.

Create a host connection to Nutanix in Citrix Studio

1. For on-premises Delivery Controllers, choose **Configuration > Hosting > Add Connection and Resources** in the on-premises Citrix Studio. For cloud Delivery Controllers, choose **Manage > Hosting > Add Connection and Resources** in the web-based Studio console on Citrix Cloud to create a connection to the Nutanix hypervisor.
2. In the **Add Connection and Resources** wizard, select Nutanix AHV as the connection type on the **Connection** page, and then specify the hypervisor address, credentials, and your connection name. On the **Network** page, select a network for the unit.

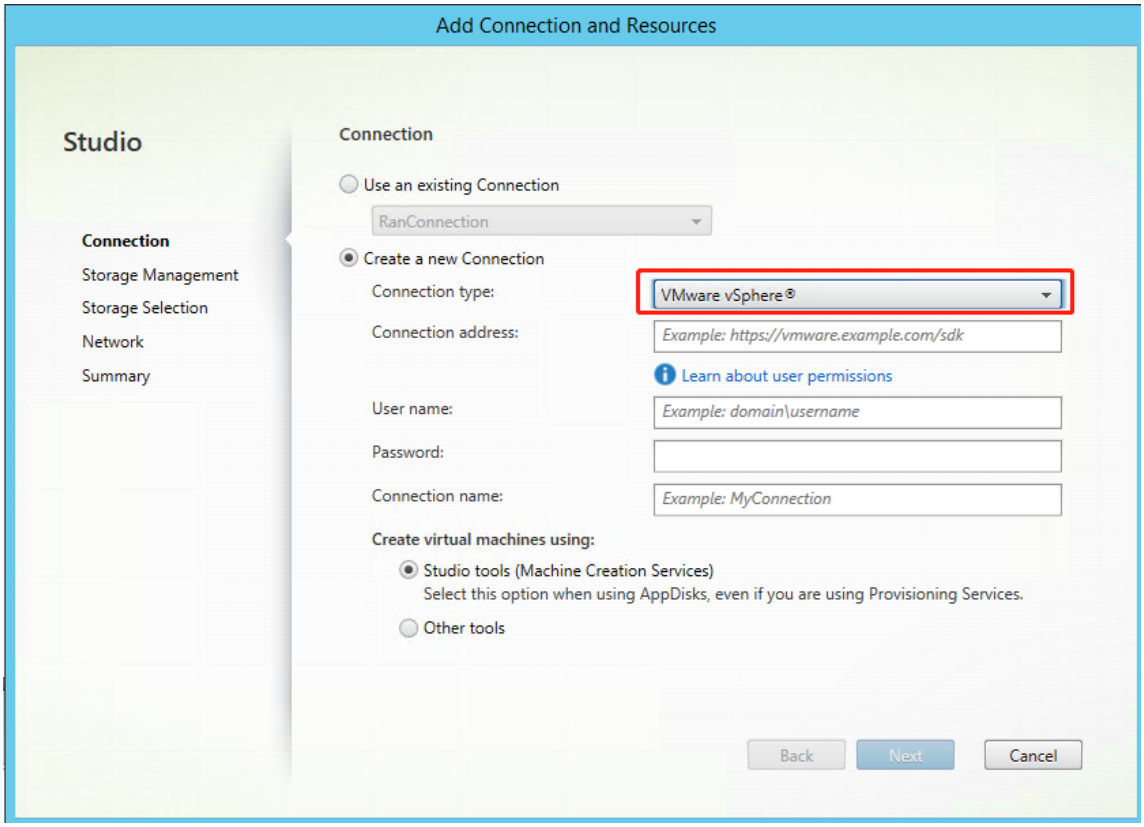
   For example, in the on-premises Citrix Studio:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

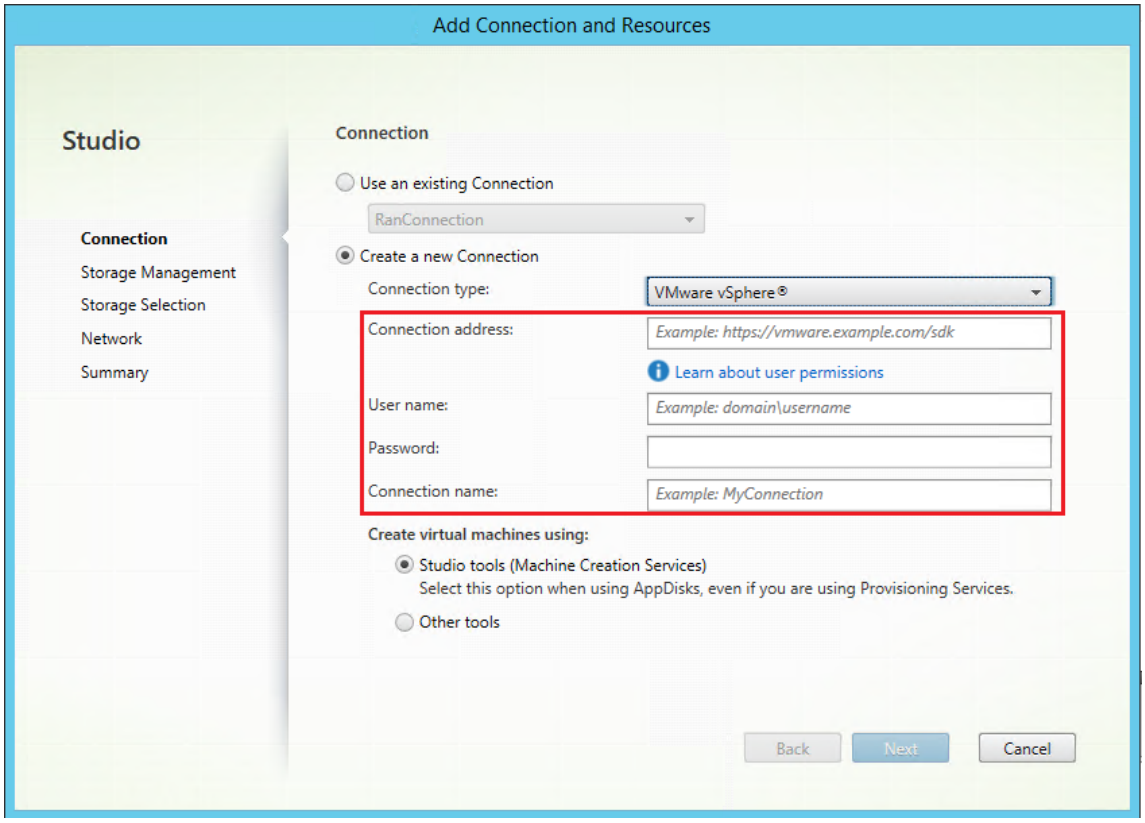
Create a host connection to VMware in Citrix Studio

1. Install vCenter Server in the vSphere environment. For more information, see VMware vSphere.
2. In Citrix Studio, choose **Configuration > Hosting > Add Connection and Resources**.
3. Choose VMware vSphere as the connection type.



4. Type the connection address (the vCenter Server URL) of your VMware account, your user name and password, and your connection name.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Step 3: Prepare a master image

(For Citrix Hypervisor only) Step 3a: Install Citrix VM Tools Install Citrix VM Tools on the template VM for each VM to use the xe CLI or XenCenter. VM performance can be slow unless you install the tools. Without the tools, you can't do any of the following:

- Cleanly shut down, restart, or suspend a VM.
- View the VM performance data in XenCenter.
- Migrate a running VM (through `XenMotion`).
- Create snapshots or snapshots with memory (checkpoints), and revert to snapshots.
- Adjust the number of vCPUs on a running Linux VM.

1. Run the following command to mount Citrix VM Tools named guest-tools.iso.

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

2. Run the following command to install the `xe-guest-utilities` package based on your Linux distribution.

   For RHEL/CentOS/Rocky Linux:

```
sudo rpm -i /mnt/Linux/xe-guest-utilities_{
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 package-version }
 _all.rpm
<!--NeedCopy-->
```

For Ubuntu/Debian:

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

For SUSE:

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

3. Check the virtualization state of the template VM on the **General** tab in XenCenter. If Citrix VM Tools are installed correctly, the virtualization state is **Optimized**.

(For Azure, AWS, and GCP) Step 3b: Configure cloud-init for Ubuntu 18.04

1. To ensure that a VDA host name persists when a VM is restarted or stopped, run the following command:

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

Verify that the following lines are present under the **system_info** section in the /etc/cloud/-cloud.cfg file:

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

2. To use SSH for remotely accessing MCS-created VMs on AWS, enable password authentication because no key name is attached to those VMs. Do the following as needed.

   - Edit the `cloud-init` configuration file, /etc/cloud/cloud.cfg. Ensure that the **ssh_pwauth: true** line is present. Remove or comment the **set-password** line and the following lines if they exist.

     ```
     users:
     - default
     <!--NeedCopy-->
     ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- If you plan to use the default user `ec2-user` or `ubuntu` created by `cloud-init`, you can change the user password by using the `passwd` command. Keep the new password in mind for later use to log in to the MCS-created VMs.
- Edit the `/etc/ssh/sshd_config` file to ensure that the following line is present:

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

Save the file and run the `sudo service sshd restart` command.

Step 3c: Disable RDNS for Ubuntu 20.04 on GCP On the template VM, add the **rdns = false** line under **[libdefaults]** in /etc/krb5.conf.

Step 3d: Install the Linux VDA package on the template VM

> **Note:**
>
> To use a currently running VDA as the template VM, skip this step.
>
> Before installing the Linux VDA package on the template VM, install .NET Runtime 6.0.

Based on your Linux distribution, run the following command to set up the environment for the Linux VDA:

For RHEL/CentOS/Rocky Linux:

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

> **Note:**
>
> For RHEL and CentOS, install the EPEL repository before you can install the Linux VDA and run `deploymcs.sh` successfully. For information on how to install EPEL, see the instructions at https://docs.fedoraproject.org/en-US/epel/.

For Ubuntu/Debian:

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

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

For SUSE:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 3e: Enable repositories to install the tdb-tools package (for RHEL 7 only) **For RHEL 7 server:**

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

For RHEL 7 workstation:

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

Step 3f: (On SUSE) Manually install ntfs-3g On the SUSE platform, no repository provides ntfs-3g. Download the source code, compile, and install ntfs-3g manually:

1. Install the GNU Compiler Collection (GCC) compiler system and the make package:

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

2. Download the ntfs-3g package.
3. Decompress the ntfs-3g package:

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

4. Enter the path to the ntfs-3g package:

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

5. Install ntfs-3g:

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

Step 3g: Specify a database to use As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL after installing the Linux VDA package. To do so, complete the following steps:

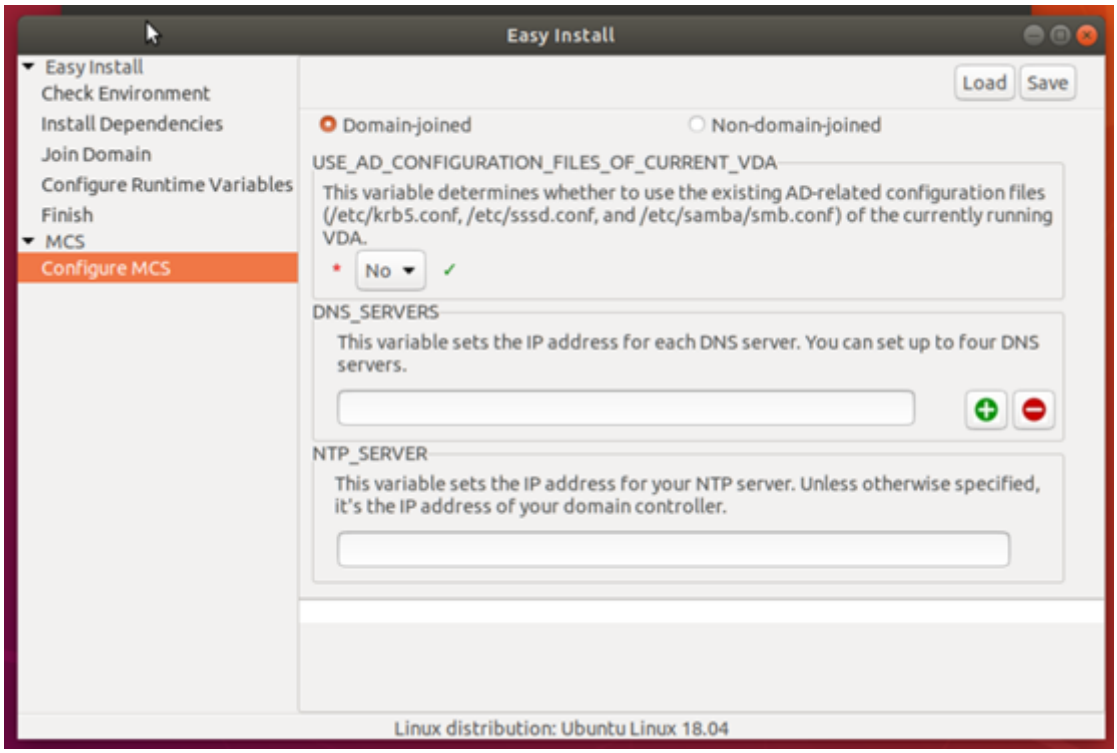
1. Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.
2. Edit `/etc/xdl/db.conf` before running `deploymcs.sh`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - We recommend you use SQLite for VDI mode only.
> - For easy install and MCS, you can switch between SQLite and PostgreSQL without having to install them manually. Unless otherwise specified through `/etc/xdl/db.conf`, the Linux VDA uses PostgreSQL by default.
> - You can also use `/etc/xdl/db.conf` to configure the port number for PostgreSQL.

Step 3h: Configure MCS variables There are two ways to configure MCS variables:

- Edit the `/etc/xdl/mcs/mcs.conf` file.
- Use the easy install GUI. To open the easy install GUI, run the `/opt/Citrix/VDA/bin/easyinstall` command in the desktop environment of your Linux VDA.



> **Tip:**
>
> Click **Save** to save variable settings to a local file under the path you specify. Click **Load** to load variable settings from a file that you specify.

The following are MCS variables that you can configure for non-domain-joined and domain-joined scenarios:

- **For non-domain-joined scenarios**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
DESKTOP_ENVIRONMENT= **gnome | mate \**
REGISTER_SERVICE=**Y | N**
ADD_FIREWALL_RULES=**Y | N**
VDI_MODE=**Y | N**
START_SERVICE=**Y | N**
```

- **For domain-joined scenarios**
  - `Use_AD_Configuration_Files_Of_Current_VDA`: Determines whether to use the existing AD-related configuration files (/etc/krb5.conf, /etc/sssd.conf, and /etc/samba/smb.conf) of the currently running VDA. If set to Y, the configuration files on MCS-created machines are the same as the equivalents on the currently running VDA. However, you still must configure the `dns` and `AD_INTEGRATION` variables. The default value is N, which means the configuration templates on the master image determine the configuration files on MCS-created machines.
  - `dns`: Sets the IP address for each DNS server. You can set up to four DNS servers.
  - `NTP_SERVER`: Sets the IP address for your NTP server. Unless otherwise specified, it's the IP address of your domain controller.
  - `WORKGROUP`: Sets the workgroup name to the NetBIOS name (case-sensitive) that you configured in AD. Otherwise, MCS uses the part of the domain name that immediately follows the machine hostname as the workgroup name. For example, if the machine account is **user1.lvda.citrix.com**, MCS uses **lvda** as the workgroup name while **citrix** is the correct choice. Ensure that you set the workgroup name correctly.
  - `AD_INTEGRATION`: Sets Winbind, SSSD, PBIS, or Centrify. For a matrix of the Linux distributions and domain joining methods that MSC supports, see Supported distributions in this article.
  - `CENTRIFY_DOWNLOAD_PATH`: Sets the path for downloading the Server Suite Free (formerly Centrify Express) package. The value takes effect only when you set the `AD_INTEGRATION` variable to Centrify.
  - `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Sets the path for downloading the Centrify Samba package. The value takes effect only when you set the `AD_INTEGRATION` variable to Centrify.
  - `PBIS_DOWNLOAD_PATH`: Sets the path for downloading the PBIS package. The value takes effect only when you set the `AD_INTEGRATION` variable to PBIS.
  - `UPDATE_MACHINE_PW`: Enables or disables automating machine account password updates. For more information, see Automate machine account password updates.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Linux VDA configuration variables:

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

Step 3i: Write or update registry values for MCS On the template machine, add command lines to the /etc/xdl/mcs/mcs_local_setting.reg file for writing or updating registry values as required. This action prevents the loss of data and settings every time an MCS-provisioned machine restarts.

Each line in the /etc/xdl/mcs/mcs_local_setting.reg file is a command for setting or updating a registry value.

For example, you can add the following command lines to the /etc/xdl/mcs/mcs_local_setting.reg file to write or update a registry value respectively:

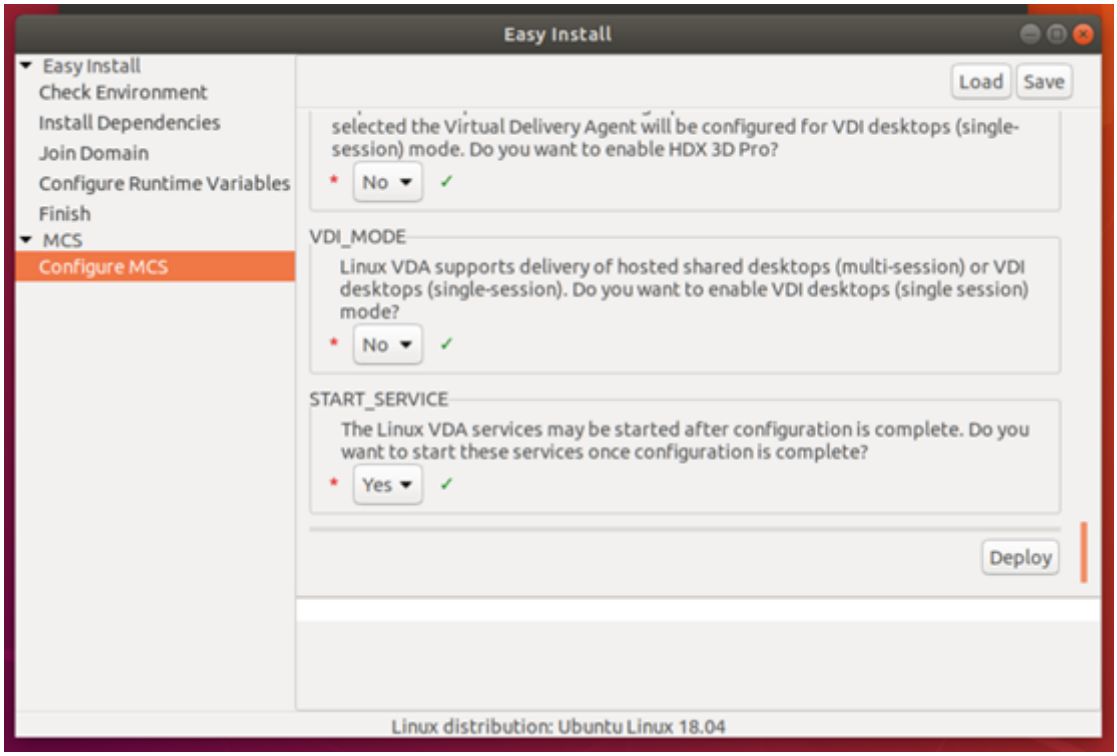
```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels
     \Clipboard\ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0
     x00000003" --force
2 <!--NeedCopy-->
```

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

Step 3j: Create a master image

1. If you configure MCS variables by editing /etc/xdl/mcs/mcs.conf, run /opt/Citrix/VDA/sbin/deploymcs.sh. If you configure MCS variables by using the GUI, click **Deploy**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



After you click **Deploy** on the GUI, the variables you set on the GUI override the variables you set in the `/etc/xdl/mcs/mcs.conf` file.

2. (If you are using a currently running VDA as the template VM or if it is a non-domain-joined scenario, skip this step.) On the template VM, update the configuration templates to customize the relevant `/etc/krb5.conf`, `/etc/samba/smb.conf`, and `/etc/sssd/sssd.conf` files on all created VMs.

   For Winbind users, update the `/etc/xdl/ad_join/winbind_krb5.conf.tmpl` and `/etc/xdl/ad_join/winbind_smb.conf.tmpl` templates.

   For SSSD users, update the `/etc/xdl/ad_join/sssd.conf.tmpl`, `/etc/xdl/ad_join/sssd_krb5.conf.tmpl`, and `/etc/xdl/ad_join/sssd_smb.conf.tmpl` templates.

   For Centrify users, update the `/etc/xdl/ad_join/centrify_krb5.conf.tmpl` and `/etc/xdl/ad_join/centrify_smb.conf.tmpl` templates.

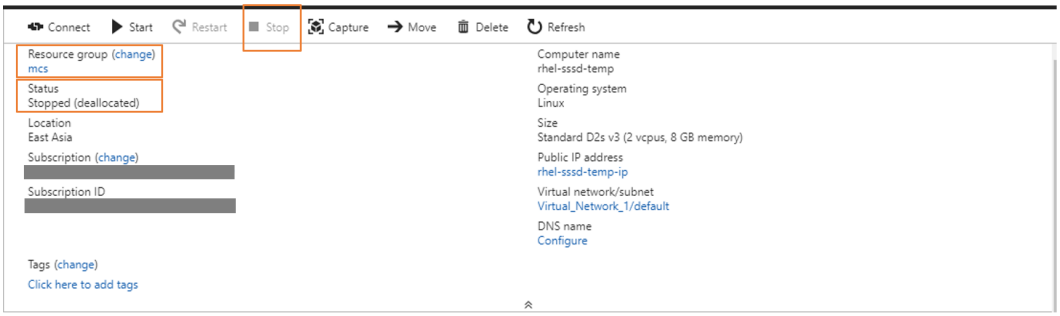
   > **Note:**
   >
   > Keep the existing format used in the template files and use variables such as $WORKGROUP, $REALM, $realm, ${new_hostname}, and $AD_FQDN.

3. Create and name a snapshot of your master image based on the public cloud you use.

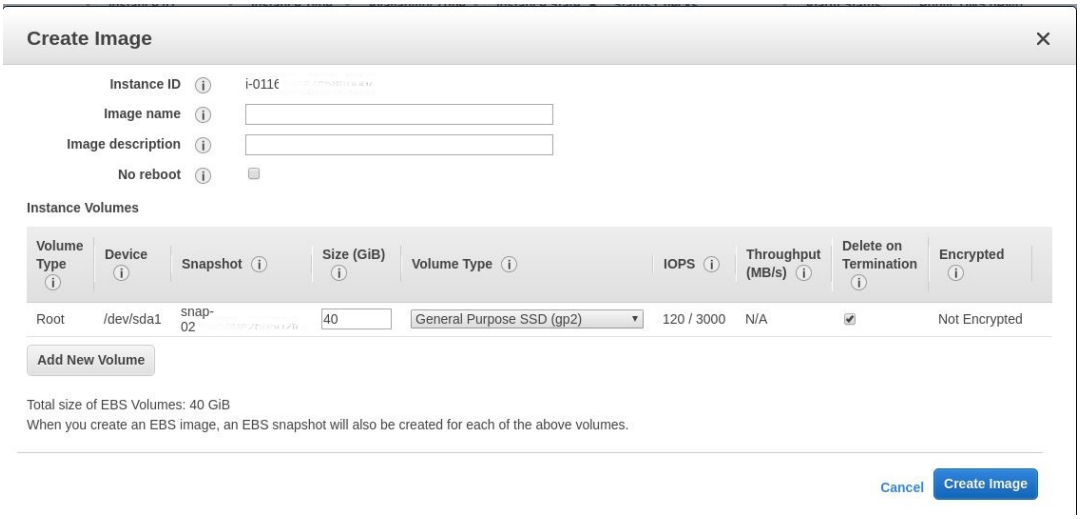
   - **(For Citrix Hypervisor, GCP, and VMware vSphere)** Install applications on the template VM and shut down the template VM. Create and name a snapshot of your master image.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **(For Azure)** Install applications on the template VM and shut down the template VM from the Azure portal. Ensure that the power status of the template VM is **Stopped (deallocated)**. Remember the name of the resource group here. You need the name to locate your master image on Azure.



- **(For AWS)** Install applications on the template VM and shut down the template VM from the AWS EC2 portal. Ensure that the instance state of the template VM is **Stopped**. Right-click the template VM and select **Image > Create Image**. Type information and make settings as needed. Click **Create Image**.



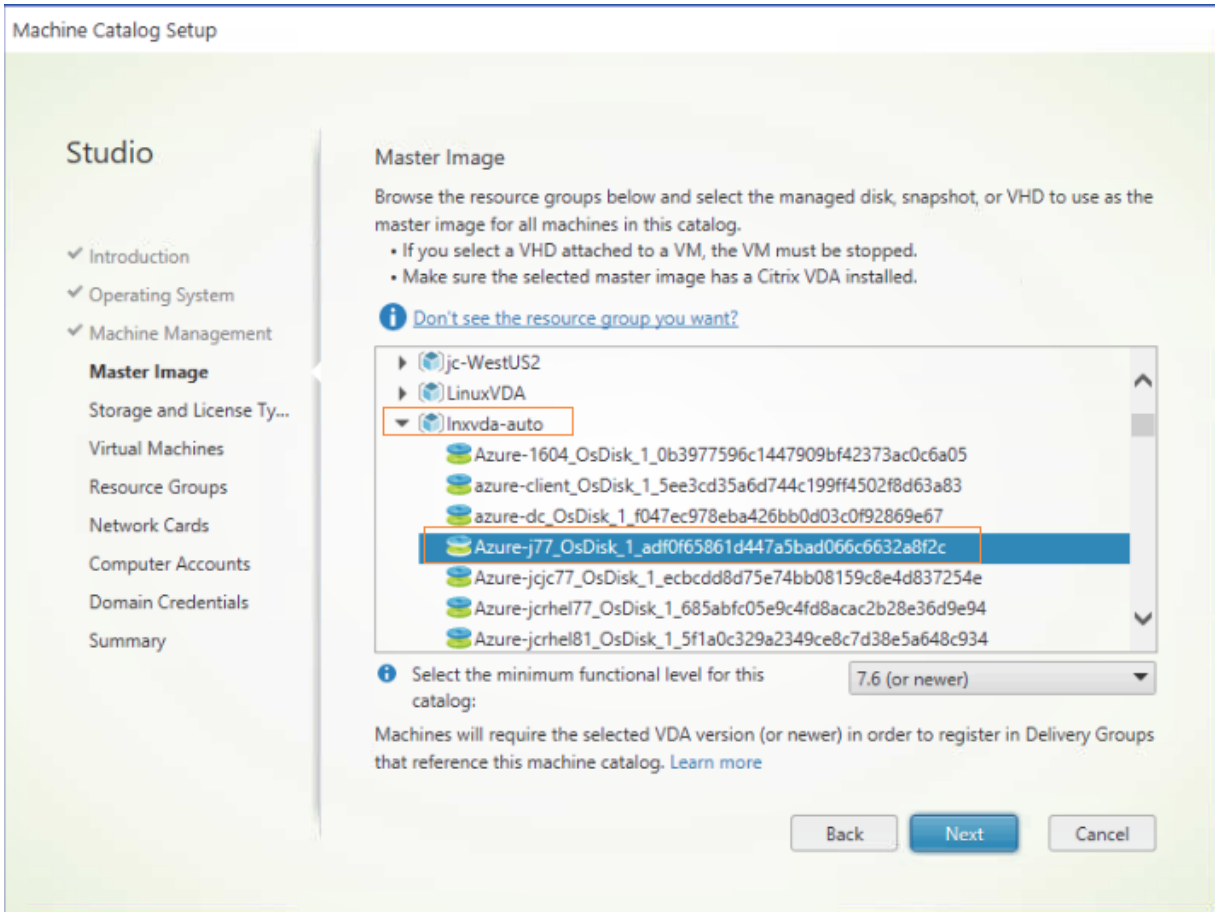
- **(For Nutanix)** On Nutanix AHV, shut down the template VM. Create and name a snapshot of your master image.

> **Note:**
>
> You must prefix Acropolis snapshot names with XD_ for use in Citrix Virtual Apps and Desktops. Use the Acropolis console to rename your snapshots when needed. After you rename a snapshot, restart the **Create Catalog** wizard to obtain a refreshed list.

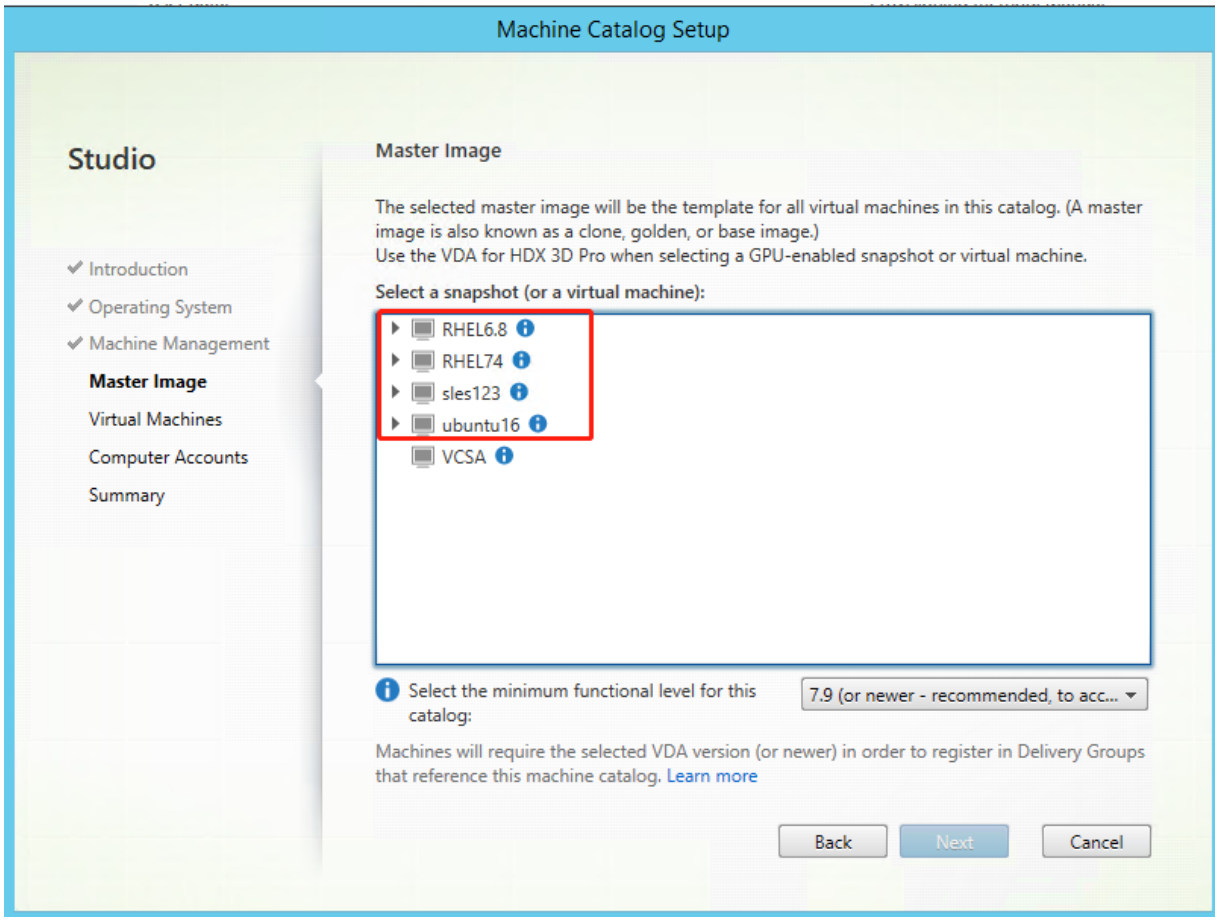
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 4: Create a machine catalog

In Citrix Studio, create a machine catalog and specify the number of VMs to create in the catalog. When creating the machine catalog, choose your master image. The following are examples:



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



On the **Container** page that is unique to Nutanix, select the container that you specified for the template VM earlier. On the **Master Image** page, select the image snapshot. On the **Virtual Machines** page, check for the number of virtual CPUs and the number of cores per vCPU.

> **Note:**
>
> If your machine catalog creation process on the Delivery Controller takes a significant amount of time, go to Nutanix Prism and power on the machine prefixed with **Preparation** manually. This approach helps to continue the creation process.

Do other configuration tasks as needed. For more information, see Create a machine catalog using Studio.

Step 5: Create a delivery group

A delivery group is a collection of machines selected from one or more machine catalogs. It specifies which users can use those machines, and the applications and desktops available to those users. For more information, see Create delivery groups.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Use MCS to update your Linux VDA

To use MCS to update your Linux VDA, do the following:

1. Ensure that you installed .NET Runtime 6.0 before you update your Linux VDA to the current release.
2. update your Linux VDA on the template machine:

> **Note:**
>
> You can also use the Linux VDA self-update feature to schedule automatic software updates. To achieve this goal, add command lines to the etc/xdl/mcs/mcs_local_setting.reg file on the template machine.
> For example, you can add the following command lines:

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

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

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

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

For RHEL 7 and CentOS 7:

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

For RHEL 8 and Rocky Linux 8:

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

For RHEL 9.0 and Rocky Linux 9.0:

```
sudo rpm -U XenDesktopVDA-<version>.el9x.x86_64.rpm
<!--NeedCopy-->
```

For SUSE:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

For Ubuntu 18.04:

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

For Ubuntu 20.04:

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

For Ubuntu 22.04:

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

3. Edit /etc/xdl/mcs/mcs.conf and /etc/xdl/mcs/mcs_local_setting.reg.
4. Take a new snapshot.
5. In Citrix Studio, select the new snapshot to update your machine catalog. Wait before each machine restarts. Do not restart a machine manually.

Automate machine account password updates

Machine account passwords, by default, expire 30 days after the machine catalog is created. To prevent password expiration and to automate machine account password updates, do the following:

1. Add the following entry to /etc/xdl/mcs/mcs.conf before running /opt/Citrix/VDA/sbin/deploymcs.sh.

   ```
   UPDATE_MACHINE_PW="Y"
   ```

2. After running /opt/Citrix/VDA/sbin/deploymcs.sh, open /etc/cron.d/mcs_update_password_cronjob to set the update time and frequency. The default setting updates machine account passwords weekly at 2:30AM, Sunday.

After each machine account password update, the ticket cache on the Delivery Controller becomes invalid and the following error might appear in /var/log/xdl/jproxy.log:

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

To eliminate the error, clear the ticket cache regularly. You can schedule a cache cleanup task on all Delivery Controllers or on the domain controller.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enable FAS on MCS-created VMs

You can enable FAS on MCS-created VMs that run on the following distributions:

	Winbind	SSSD	Centrify	PBIS
RHEL 9.0	Yes	No	No	No
RHEL 8	Yes	No	No	Yes
Rocky Linux 9.0	Yes	No	No	No
Rocky Linux 8	Yes	No	No	No
RHEL 7, CentOS 7	Yes	Yes	No	Yes
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Yes	No	No	No
Debian 11.3	Yes	No	No	No
SUSE 15.3	Yes	No	No	No

Enable FAS when you are preparing a master image on the template VM

1. Import the root CA certificate.

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

2. Run ctxfascfg.sh. For more information, see Run ctxfascfg.sh.
3. Set variables in `/etc/xdl/mcs/mcs.conf`.

> **Note:**
>
> Set all necessary variables in `/etc/xdl/mcs/mcs.conf` because these variables are called upon VM startup.

   a) Set the value of `Use_AD_Configuration_Files_Of_Current_VDA` to Y.
   b) Set the `FAS_LIST` variable to your FAS server address or multiple FAS server addresses. Separate multiple addresses with semicolons and enclose the address or addresses with single quotes, for example, `FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'`.
   c) Set the other variables as required, such as `VDI_MODE`.

4. Run the script `/opt/Citrix/VDA/sbin/deploymcs.sh`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enable FAS on an MCS-created VM

If FAS is not enabled on the template machine as described earlier, you can enable FAS on each MCS-created VM.

To enable FAS on an MCS-created VM, do the following:

1. Set variables in /etc/xdl/mcs/mcs.conf.

   > **Note:**
   >
   > Set all necessary variables in `/etc/xdl/mcs/mcs.conf` because these variables are called upon VM startup.

   a) Set the value of `Use_AD_Configuration_Files_Of_Current_VDA` to Y.
   b) Set the `FAS_LIST` variable to your FAS server address.
   c) Set the other variables as required, such as `VDI_MODE`.

2. Import the root CA certificate.

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

3. Run the `/opt/Citrix/VDA/sbin/ctxfascfg.sh` script. For more information, see Run ctxfascfg.sh.

Create Linux VDAs using Citrix Provisioning

January 23, 2023

You can create domain-joined VDAs using Citrix Provisioning.

This article provides information about streaming Linux target devices. Using this feature, you can provision Linux virtual desktops directly in the Citrix Virtual Apps and Desktops environment.

The following Linux distributions are supported:

- Ubuntu 22.04
- Ubuntu 20.04
- Ubuntu 18.04
- RHEL 8.6
- Rocky Linux 8.6
- RHEL 8.4
- RHEL 7.9
- SUSE 15.3

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important:**
>
> - We recommend that you use the most recent installation package of Citrix Provisioning. Use the package based on your Linux distribution. Citrix Provisioning Server 2109 or later is required to use Linux streaming agent 2109 and later.
> - When using Citrix Provisioning to stream Linux target devices, create a separate boot partition on the single shared-disk image so that the provisioned devices can boot as expected.
> - Avoid formatting any partition with **btrfs**. GRUB2 has an intrinsic problem finding **btrfs** partitions. **GRUB** stands for **GRand Unified Bootloader**.

For more information, see Streaming Linux target devices in the Citrix Provisioning documentation.

Create Linux VDAs in Citrix DaaS Standard for Azure

May 16, 2023

You can create both domain-joined and non-domain-joined Linux VDAs in Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure) to deliver virtual apps and desktops to any device from Microsoft Azure. For more information, see Citrix DaaS Standard for Azure.

Supported Linux distributions

The following Linux distributions support this feature:

- RHEL 9.0
- RHEL 8.6
- RHEL 8.4
- Rocky Linux 8.6
- Rocky Linux 9.0
- Ubuntu 22.04
- Ubuntu 20.04
- Ubuntu 18.04

Step 1: Prepare a master image in Azure

> **Note:**
>
> You can also use the Linux VDA self-update feature to schedule automatic software updates. To achieve this goal, add command lines to the etc/xdl/mcs/mcs_local_setting.reg file on the mas-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ter image.
>
> For example, you can add the following command lines:

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

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

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

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

1. In Azure, create a Linux VM of a supported distribution.
2. Install a desktop environment on the Linux VM if necessary.
3. On the VM, install .NET Runtime 6.0 according to the instructions at https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.
4. (For Ubuntu only) Add the `source /etc/network/interfaces.d/*` line to the `/etc/network/interfaces` file.
5. (For Ubuntu only) Point `/etc/resolv.conf` to `/run/systemd/resolve/resolv.conf` instead of pointing it to `/run/systemd/resolve/stub-resolv.conf`:

   ```
   unlink /etc/resolv.conf

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

6. Install the Linux VDA package.
7. Specify a database to use.

   As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL after installing the Linux VDA package. To do so, complete the following steps:

   a) Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.

   b) Edit `/etc/xdl/db.conf` before running `deploymcs.sh`.

   > **Note:**
   >
   > - We recommend you use SQLite for VDI mode only.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - For easy install and MCS, you can switch between SQLite and PostgreSQL without having to install them manually. Unless otherwise specified through `/etc/xdl/db.conf`, the Linux VDA uses PostgreSQL by default.
> - You can also use `/etc/xdl/db.conf` to configure the port number for PostgreSQL.

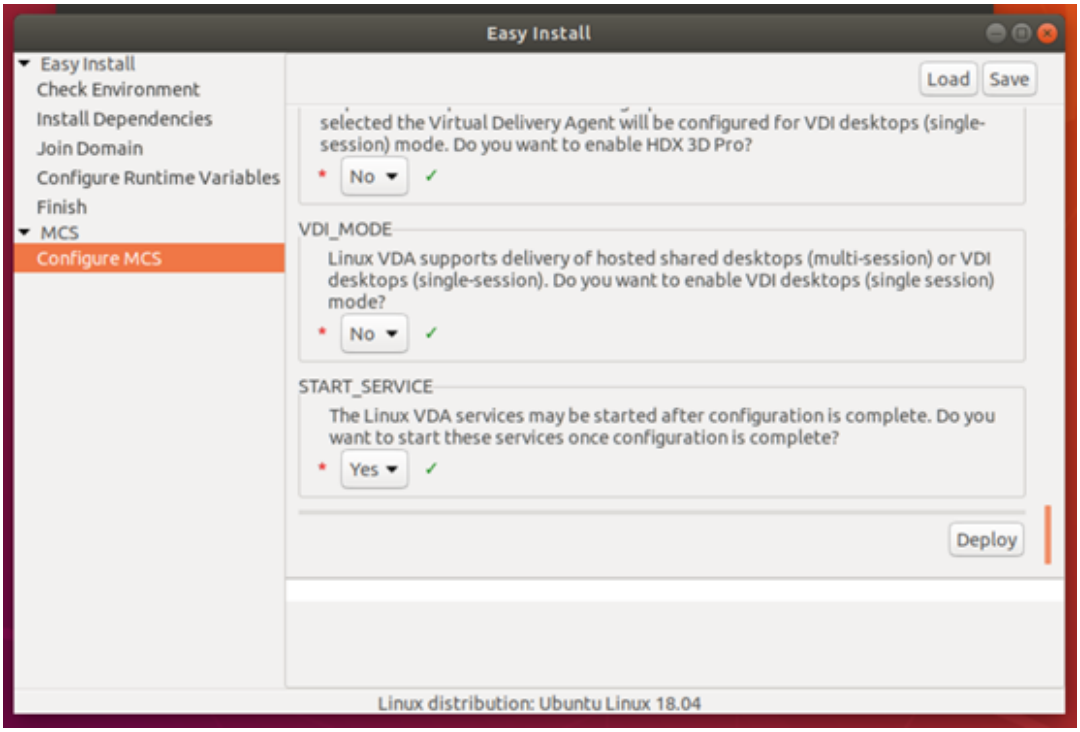
8. Change MCS variables.

   There are two ways to configure MCS variables:

   - Edit the `/etc/xdl/mcs/mcs.conf` file.
   - Use the easy install GUI. To open the easy install GUI, run the `/opt/Citrix/VDA/bin/easyinstall` command in the desktop environment of your Linux VDA.

     > **Note:**
     >
     > Leave the `dns` variable unspecified.
     > If you select the **Static** or **Random** type when creating a machine catalog, set `VDI_MODE=Y`.

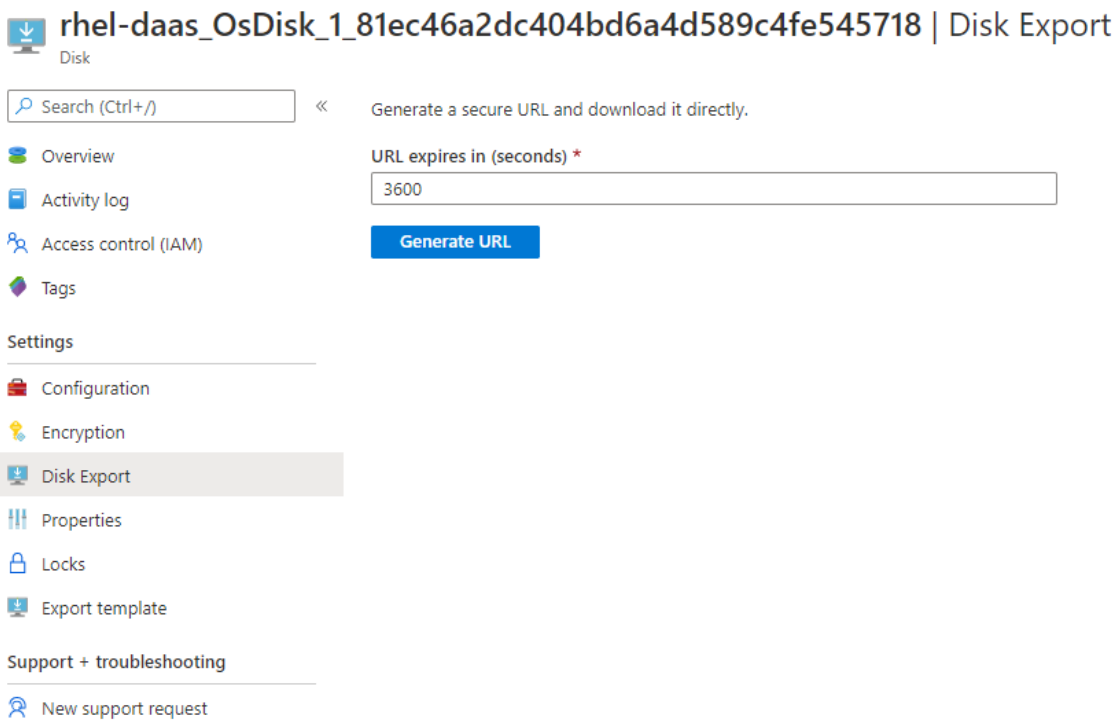
     If you configure MCS variables by editing `/etc/xdl/mcs/mcs.conf`, run `/opt/Citrix/VDA/sbin/deploymcs.sh`. If you configure MCS variables by using the GUI, click **Deploy**.



     After you click **Deploy** on the GUI, the variables you set on the GUI override the variables you set in the `/etc/xdl/mcs/mcs.conf` file.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. In Azure, stop (or deallocate) the VM. Click **Disk Export** to generate a SAS URL for the Virtual Hard Disk (VHD) file that you can use as a master image to create other VMs.



10. (Optional) Make group policy settings on the master image. You can use the `ctxreg` tool to make group policy settings. For example, the following command enables the **Auto-create PDF Universal Printer** policy for PDF printing.

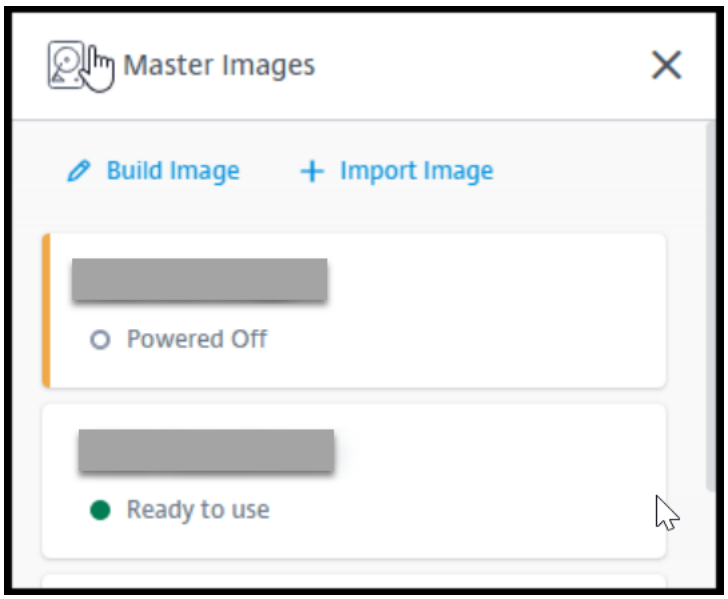
```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   GroupPolicy\Defaults\PrintingPolicies" -t "REG_DWORD" -v "
   AutoCreatePDFPrinter" -d "0x00000001" –force
<!--NeedCopy-->
```

Step 2: Import the master image from Azure

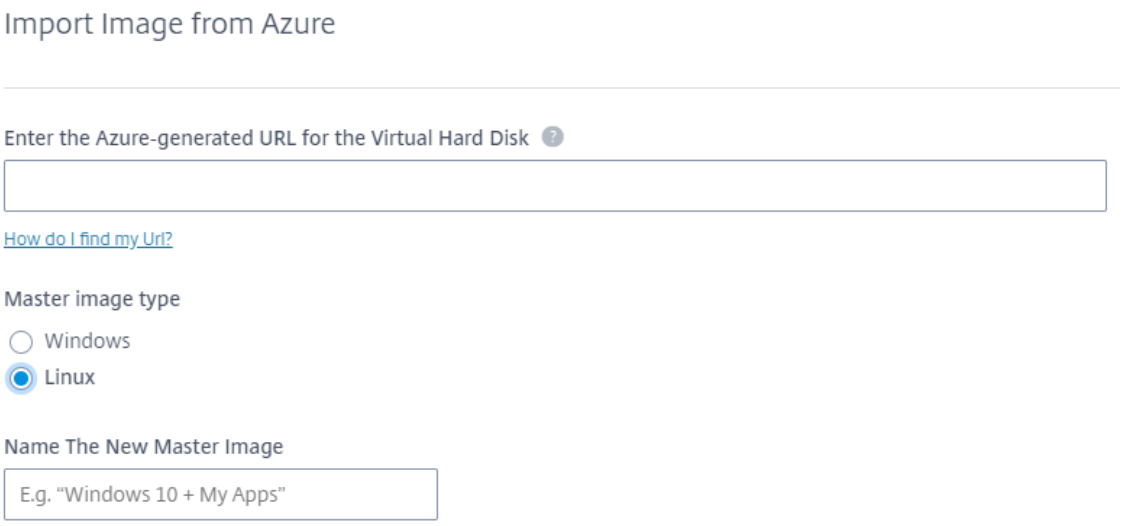
1. From the Manage dashboard, expand **Master Images** on the right. The display lists the master images that Citrix provides, and images that you created and imported.

> **Tip:**
>
> Most of the administrator activities for this service are managed through the **Manage** and **Monitor** dashboards. After you create your first catalog, the **Manage** dashboard launches automatically after you sign in to Citrix Cloud and select the **Managed Desktops** service.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. Click **Import Image**.
3. Enter the SAS URL for the VHD file that you generated in Azure. Select **Linux** for the master image type.



4. Follow the instructions in the wizard to complete importing the master image.

Step 3: Create a Machine Catalog

Access the Manage dashboard and click **Create Catalog**. When creating the Machine Catalog, choose the master image you created earlier.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> The VM used as a master image is not accessible through SSH or RDP. To access the VM, use the Serial Console in the Azure portal.

Install the Linux VDA manually

January 23, 2023

You can install the Linux VDA on the following Linux distributions manually:

- Amazon Linux 2, CentOS, RHEL, and Rocky Linux
- SUSE
- Ubuntu
- Debian

Install the Linux VDA on Amazon Linux 2, CentOS, RHEL, and Rocky Linux manually

August 22, 2023

> **Important:**
>
> For fresh installations, we recommend you use easy install for a quick installation. Easy install saves time and labor and is less error-prone than the manual installation detailed in this article.

Step 1: Prepare configuration information and the Linux machine

Step 1a: Verify the network configuration

Make sure that the network is connected and configured correctly. For example, you must configure the DNS server on the Linux VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 1b: Set the host name

To make sure that the host name of the machine is reported correctly, change the **/etc/hostname** file to contain only the host name of the machine.

```
hostname
```

Step 1c: Assign a loopback address to the host name

To make sure that the DNS domain name and Fully Qualified Domain Name (FQDN) of the machine are reported back correctly, change the following line of the `/etc/hosts` file to include the FQDN and host name 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. The host name 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 host name with a number and do not end with a hyphen. This rule also applies to Delivery Controller host names.

Step 1d: Check the host name

Verify that the host name is set correctly:

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

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

Verify that the FQDN is set correctly:

```
1 hostname -f
2 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

This command returns the FQDN of the machine.

Step 1e: Check name resolution and service reachability

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

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

Step 1f: Configure clock synchronization

Maintaining accurate clock synchronization between the VDAs, Delivery Controllers, and domain controllers is crucial. Hosting the Linux VDA as a virtual machine (VM) can cause clock skew problems. For this reason, synchronizing time with a remote time service is preferred.

An RHEL default environment uses the Chrony daemon (`chronyd`) for clock synchronization.

Configure the Chrony service As a root user, 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
<!--NeedCopy-->
```

In a typical deployment, synchronize time 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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 1g: Install PulseAudio (For RHEL 9.0 and Rocky Linux 9.0 only)

Run the following command to install **pulseaudio**:

```
sudo yum -y install pulseaudio --allowerasing
<!--NeedCopy-->
```

Open `/etc/pulse/client.conf` and add the following entry:

```
autospawn = yes
<!--NeedCopy-->
```

Step 1h: Install OpenJDK 11

The Linux VDA requires the presence of OpenJDK 11.

- If you are using CentOS, RHEL, or Rocky Linux, OpenJDK 11 is automatically installed as a dependency when you install the Linux VDA.
- If you are using Amazon Linux 2, run the following command to enable and install OpenJDK 11:

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

Confirm the correct version:

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

The prepackaged OpenJDK might be an earlier version. Update to OpenJDK 11:

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

Step 1i: Install and specify a database to use

As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL by editing `/etc/xdl/db.conf` after installing the Linux VDA package. For manual installations, you must install SQLite and PostgreSQL manually before being able to switch between them.

This section describes how to install the PostgreSQL and SQLite databases and how to specify a database to use.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> We recommend you use SQLite for VDI mode only.

Install PostgreSQL The Linux VDA requires PostgreSQL:

- PostgreSQL 9 for Amazon Linux 2, RHEL 7, and CentOS 7
- PostgreSQL 10 for RHEL 8 and Rocky Linux 8.6
- PostgreSQL 13 for RHEL 9.0 and Rocky Linux 9.0

Run the following commands to install PostgreSQL:

```
sudo yum -y install postgresql-server

sudo yum -y install postgresql-jdbc
<!--NeedCopy-->
```

For RHEL 8 and RHEL 9.0, run the following command to install `libpq` for PostgreSQL:

```
sudo yum -y install libpq
<!--NeedCopy-->
```

Run the following command to initialize the database. This action creates database files under **/var/lib/pgsql/data**.

```
sudo postgresql-setup initdb
<!--NeedCopy-->
```

Run the following commands to start PostgreSQL upon machine startup or immediately, respectively:

```
sudo systemctl enable postgresql

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

Check the version of PostgreSQL by using:

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

(RHEL 7 only) Verify that the data directory is set by using the **psql** command-line utility:

```
sudo -u postgres psql -c 'show data_directory'
<!--NeedCopy-->
```

Install SQLite Run the following command to install SQLite:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo yum -y install sqlite
<!--NeedCopy-->
```

Specify a database to use After you install SQLite, PostgreSQL, or both, you can specify a database to use by editing `/etc/xdl/db.conf` after installing the Linux VDA package. To do so, complete the following steps:

1. Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.
2. Edit `/etc/xdl/db.conf` to specify a database to use.
3. Run `ctxsetup.sh`.

> **Note:**
>
> You can also use **/etc/xdl/db.conf** to configure the port number for PostgreSQL.

Step 2: Prepare the hypervisor

Some changes are required when running the Linux VDA as a VM on a supported hypervisor. Make the following changes based on 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 Hypervisor

When the Citrix Hypervisor Time Sync feature is enabled, within each paravirtualized Linux VM you experience issues with NTP and Citrix Hypervisor. Both try to manage the system clock. To avoid the clock becoming out of sync with other servers, ensure that the system clock within each Linux guest is synchronized with the NTP. This case requires disabling host time synchronization. No changes are required in HVM mode.

If you are running a paravirtualized Linux kernel with Citrix VM Tools installed, you can check whether the Citrix Hypervisor Time Sync feature is present and enabled from within the Linux VM:

```
su -

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

This command returns 0 or 1:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
<!--NeedCopy-->
```

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

```
xen.independent_wallclock = 1
```

To verify these changes, restart the system:

```
su -

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

This command returns the value 1.

Fix time synchronization on Microsoft Hyper-V

The Linux VMs with Hyper-V Linux Integration Services installed can apply the Hyper-V time synchronization feature to use the time of the host operating system. To ensure that the system clock remains accurate, you must enable this feature alongside the 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. Make sure that **Time synchronization** is selected.

> **Note:**
>
> This approach is different from VMware and Citrix Hypervisor, 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

When the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you experience issues with the NTP and the hypervisor. Both try to synchronize the system clock. To avoid the clock becoming out of sync with other servers, ensure that the system clock within each Linux guest is synchronized with the NTP. This case requires disabling host time synchronization.

If you are running a paravirtualized Linux kernel with VMware Tools installed:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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**.

Step 3: Add the Linux VM to the Windows domain

The following methods are available for adding Linux machines to the Active Directory (AD) domain:

- Samba Winbind
- Quest Authentication Services
- Centrify DirectControl
- SSSD
- PBIS

Follow instructions based on your chosen method.

> **Note:**
>
> Session launches might fail when the same user name is used for the local account in the Linux VDA and the account in AD.

Samba Winbind

Install or update the required packages:

For RHEL 8.x/9.0 and Rocky Linux 8.6/9.0:

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

For Amazon Linux 2, CentOS 7, and RHEL 7:

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

Enable Winbind daemon to start upon machine startup The Winbind daemon must be configured to start upon machine startup:

```
sudo /sbin/chkconfig winbind on
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure Winbind Authentication Configure the machine for Kerberos authentication by using Winbind:

1. Run the following command.

   For RHEL 8.x/9.0 and Rocky Linux 8.6/9.0:

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

   For Amazon Linux 2, CentOS 7, and RHEL 7:

   ```
   sudo authconfig --disablecache --disablesssd --disablesssdauth --
       enablewinbind --enablewinbindauth --disablewinbindoffline --
       smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM --
       krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --
       winbindtemplateshell=/bin/bash --enablemkhomedir --updateall
   <!--NeedCopy-->
   ```

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

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

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

   Ignore any errors returned from the `authconfig` command about the `winbind` service failing to start. The errors can occur when `authconfig` tries to start the `winbind` service without the machine yet being joined to the domain.

2. 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
   winbind offline logon = no
   ```

3. (For RHEL 8.x/9.0 and Rocky Linux 8.6/9.0 only) Open **/etc/krb5.conf** and add entries under the `[libdefaults]`, `[realms]`, and `[domain_realm]` sections:

   Under the `[libdefaults]` section:

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

   Under the `[realms]` section:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

}

Under the [domain_realm] section:

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

The Linux VDA requires the system keytab file /etc/krb5.keytab to authenticate and register with the Delivery Controller. The previous kerberos method setting forces Winbind to create the system keytab file when the machine is first joined to the domain.

Join Windows domain Your domain controller must be reachable and you must have an Active Directory user account with permissions to add computers to the domain:

For RHEL 8.x/9.0 and Rocky Linux 8.6/9.0:

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

For Amazon Linux 2 and RHEL 7:

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

REALM is the Kerberos realm name in uppercase, and **user** is a domain user who has 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
```

Make sure that any leading semicolons from each setting are removed. These changes require restarting the Winbind daemon:

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

> **Tip:**
>
> The `winbind` daemon stays running only if the machine is joined to a domain.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 }
```

For RHEL 9.0 and Rocky Linux 9.0, run the following commands to prevent `pam_winbind` from changing the ownership of the root directory and to resolve the SELinux issue with Winbind:

```
usermod -d /nonexistent nobody

ausearch -c 'winbindd' --raw | audit2allow -M my-winbindd -p /etc/
    selinux/targeted/policy/policy.*

semodule -X 300 -i my-winbindd.pp
<!--NeedCopy-->
```

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in **Active Directory**.

Run the **net ads** command of **Samba** to verify that the machine is joined to a domain:

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

Run the following command to verify extra domain and computer object information:

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

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

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

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Examine the account details of the machine using:

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

Verify user authentication Use the **wbinfo** tool to verify that domain users can authenticate with the domain:

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

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 returns a message indicating success or failure.

To verify that the Winbind PAM module is configured correctly, log on to the Linux VDA using a domain user account that has not been used before.

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

Verify that the tickets in the Kerberos credential cache are valid and not expired:

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

Exit the session.

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

A similar test can be performed by logging on to the Gnome or KDE console directly. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

Quest Authentication Services

Configure Quest on domain controller Assume that 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 To enable domain users to establish HDX sessions on a Linux VDA machine:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. In the Active Directory Users and Computers management console, open Active Directory user properties for that user account.
2. Select the **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

Work around SELinux policy enforcement The default RHEL environment has SELinux fully enforced. This enforcement interferes with the Unix domain socket IPC mechanisms used by Quest, and prevents domain users from logging on.

The convenient way to work around this issue is to disable SELinux. As a root user, edit **/etc/selinux/-config** and change the **SELinux** setting:

```
SELINUX=permissive
```

This change requires a machine restart:

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

> **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 Autorenewal of Kerberos tickets must be enabled and disconnected. Authentication (offline logon) must 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
<!--NeedCopy-->
```

This command sets the renewal interval to nine hours (32,400 seconds) which is one hour less than the default 10-hour ticket lifetime. Set this parameter to a lower value on systems with a shorter ticket lifetime.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure PAM and NSS To enable domain user logon through HDX and other services such as su, ssh, and RDP, run the following commands to configure PAM and NSS manually:

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

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

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
<!--NeedCopy-->
```

The user is any domain user who has 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 Delivery Controller requires that all VDA machines (Windows and Linux VDAs) 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
<!--NeedCopy-->
```

If the machine is joined to a domain, this command returns the domain name. If the machine is not joined to any domain, the following error appears:

```
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 through PAM, log on to the Linux VDA using a domain user account that has not been used before.

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

Verify that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verify that the tickets in the Kerberos credential cache are valid and not expired:

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

Exit the session.

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

A similar test can be performed by logging on to the Gnome or KDE console directly. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

Centrify DirectControl

Join a 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
<!--NeedCopy-->
```

The user parameter is any Active Directory domain user who has permissions to join computers to the Active Directory domain. The **domain-name** is the name of the domain to join the Linux machine to.

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in Active Directory. To verify that a Centrify-joined Linux machine is on the domain:

```
su -
adinfo
<!--NeedCopy-->
```

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

Test connectivity to the various Active Directory and Kerberos services.

```
adinfo --test
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

SSSD

If you are using SSSD, follow the instructions in this section. This section includes instructions for joining a Linux VDA machine to a Windows domain and provides guidance for configuring Kerberos authentication.

To set up SSSD on RHEL and CentOS, do the following:

1. Join the domain and create host keytab
2. Set up SSSD
3. Enable SSSD
4. Verify the Kerberos configuration
5. Verify user authentication

Join the domain and create host keytab SSSD does not provide Active Directory client functions for joining the domain and managing the system keytab file. You can use **adcli**, **realmd**, or **Samba** instead.

This section describes the **Samba** approach for Amazon Linux 2 and RHEL 7 and the `adcli` approach for RHEL 8. For **realmd**, see the RHEL or CentOS documentation. These steps must be followed before configuring SSSD.

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

  Install or update the required packages:

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

  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
  <!--NeedCopy-->
  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

> **Note:**
>
> Settings in this article are meant for the single-domain, single-forest model. Configure Kerberos based on your AD infrastructure.

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

```
--enablekrb5kdcdns --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
winbind offline logon = no
```

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

```
1  sudo net ads join REALM -U user
2  <!--NeedCopy-->
```

REALM is the Kerberos realm name in uppercase and **user** is a domain user who has permissions to add computers to the domain.

- **Adcli (RHEL 8.x/9.0 and Rocky Linux 8.6/9.0):**

  Install or update the required packages:

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

  Configure the machine for **Samba** and Kerberos authentication:

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

  Open **/etc/krb5.conf** and add the entries under the [realms] and [domain_realm] sections.

  Under the [realms] section:

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

  Under the [domain_realm] section:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

```
sudo realm join REALM -U user
<!--NeedCopy-->
```

REALM is the Kerberos realm name in uppercase and **user** is a domain user who has permissions to add computers to the domain.

Set up SSSD Setting up SSSD consists of the following steps:

- Install the **sssd-ad** package on the Linux VDA by running the `sudo yum -y install sssd` command.
- Make configuration changes to various files (for example, sssd.conf).
- Start the **sssd** service.

An example **sssd.conf** configuration for RHEL 7 (extra 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
# 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

(RHEL 8.x/9.0 and Rocky Linux 8.6/9.0 only)
Open **/etc/sssd/sssd.conf** and add the following entries under the [domain/ad.example.com] section:

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

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
```

Enable SSSD **For RHEL 8.x/9.0 and Rocky Linux 8.6/9.0:**

Run the following commands to enable SSSD:

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

For Amazon Linux 2, CentOS 7, and RHEL 7:

Use **authconfig** to enable SSSD. Install **oddjob-mkhomedir** to ensure that the home directory creation is compatible with SELinux:

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

sudo service sssd start

sudo chkconfig sssd on
<!--NeedCopy-->
```

Verify Kerberos configuration Verify that the system **keytab** file has been created and contains valid keys:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. 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
<!--NeedCopy-->
```

Verify user authentication Use the **getent** command to verify that the logon format is supported and the NSS works:

```
sudo getent passwd DOMAIN\\username
<!--NeedCopy-->
```

The **DOMAIN** parameter indicates the short version domain name. If another logon format 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 to the Linux VDA using a domain user account that has not been used before.

```
sudo ssh localhost  – l DOMAIN\\username

id -u
<!--NeedCopy-->
```

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

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verify that the tickets in the user's Kerberos credential cache are valid and not expired.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

PBIS

Download the required PBIS package

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

Make the PBIS installation script executable

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

Run the PBIS installation script

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

Join Windows domain Your domain controller must be reachable and you must have an Active Directory user account with permissions to add computers to the domain:

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

The **user** is a domain user who has permissions to add computers to the Active Directory domain. The **domain-name** is the DNS name of the domain, for example, example.com.

Note: To set Bash as the default shell, run the **/opt/pbis/bin/config LoginShellTemplate/bin/bash** command.

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in Active Directory. To verify that a PBIS-joined Linux machine is on the domain:

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

If the machine is joined to a domain, this command returns the information about the currently joined AD domain and OU. Otherwise, only the host name appears.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verify user authentication To verify that PBIS can authenticate domain users through PAM, log on to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\user

id -u
<!--NeedCopy-->
```

Verify that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

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

Exit the session.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

Step 4: Install .NET Runtime 6.0

Before installing the Linux VDA, install .NET Runtime 6.0 according to the instructions at https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

After installing .NET Runtime 6.0, run the **which dotnet** command to find your runtime path.

Based on the command output, set the .NET runtime binary path. For example, if the command output is /aa/bb/dotnet, use /aa/bb as the .NET binary path.

Step 5: Download the Linux VDA package

1. Go to the Citrix Virtual Apps and Desktops download page.
2. Expand the appropriate version of Citrix Virtual Apps and Desktops.
3. Click **Components** to download the Linux VDA package that matches your Linux distribution and the GPG public key that you can use to verify the integrity of the Linux VDA package.

   To verify the integrity of the Linux VDA package, import the public key into the RPM database and run the following commands:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 
   ```

Step 6: Install the Linux VDA

You can do a fresh installation or upgrade an existing installation from the previous two versions and from an LTSR release.

To do a fresh installation

1. (Optional) Uninstall the old version

   If you installed an earlier version other than the previous two and an LTSR release, uninstall it before installing the new version.

   a) Stop the Linux VDA services:

   ```
   sudo /sbin/service ctxvda stop

   sudo /sbin/service ctxhdx stop
   <!--NeedCopy-->
   ```

   > **Note:**
   >
   > Before you stop the `ctxvda` and `ctxhdx` services, run the **service ctxmonitorservice stop** command to stop the monitor service daemon. Otherwise, the monitor service daemon restarts the services you stopped.

   b) Uninstall the package:

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

   > **Note:**
   >
   > To run 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. Download the Linux VDA package

   Go to the Citrix Virtual Apps and Desktops download page. Expand the appropriate version of Citrix Virtual Apps and Desktops and click **Components** to download the Linux VDA package that matches your Linux distribution.

3. Install the Linux VDA

   > **Note:**
   >
   > For CentOS, RHEL, and Rocky Linux, install the EPEL repository before you can install the Linux VDA successfully. For information on how to install EPEL, see the instructions at ht

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> tps://docs.fedoraproject.org/en-US/epel/.

- Install the Linux VDA software using Yum:

  For Amazon Linux 2:

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

  For RHEL 9.0 and Rocky Linux 9.0:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
  <!--NeedCopy-->
  ```

  For RHEL 8 and Rocky Linux 8.6:

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

  For CentOS 7 and RHEL 7:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
  <!--NeedCopy-->
  ```

- Install the Linux VDA software using the RPM package manager. Before doing so, you must resolve the following dependencies:

  For Amazon Linux 2:

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

  RHEL 9.0 and Rocky Linux 9.0:

  ```
  sudo rpm -i XenDesktopVDA-<version>.el9_x.x86_64.rpm
  <!--NeedCopy-->
  ```

  For RHEL 8 and Rocky Linux 8.6:

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

  For CentOS 7 and RHEL 7:

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

  RPM dependency list for RHEL 9.0 and Rocky Linux 9.0:

  ```
  java-11-openjdk >= 11

   icoutils >= 0.32

  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 libmspack >= 0.7

 krb5-workstation >= 1.13

 ibus >= 1.5

 nss-tools >= 3.44.0

 gperftools-libs >= 2.4

 cyrus-sasl-gssapi >= 2.1

 python3 >= 3.6~

 qt5-qtbase >= 5.5~

 qt5-qtbase-gui >= 5.5~

 qrencode-libs >= 3.4.4

 imlib2 >= 1.4.9

<!--NeedCopy-->
```

RPM dependency list for RHEL 8 and Rocky Linux 8.6:

```
java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9

libmspack >= 0.7

krb5-workstation >= 1.13

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

RPM dependency list for CentOS 7 and RHEL 7:

```
java-11-openjdk >= 11

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

libxml2 >= 2.9

libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
50
51  gperftools-libs >= 2.4
52
53  nss-tools >= 3.44.0
54
55  qt5-qtbase >= 5.5~
56
57  qt5-qtbase >= 5.5~
58
59  imlib2 >= 1.4.5
60  <!--NeedCopy-->
```

RPM dependency list for Amazon Linux 2:

```
1   java-11-openjdk >= 11
2
3   ImageMagick >= 6.7.8.9
4
5   firewalld >= 0.3.9
6
7   policycoreutils-python >= 2.0.83
8
9   dbus >= 1.6.12
10
11  dbus-x11 >= 1.6.12
12
13  xorg-x11-server-utils >= 7.7
14
15  xorg-x11-xinit >= 1.3.2
16
17  xorg-x11-server-Xorg >= 1.20.4
18
19  libXpm >= 3.5.10
20
21  libXrandr >= 1.4.1
22
23  libXtst >= 1.2.2
24
25  pam >= 1.1.8
26
27  util-linux >= 2.23.2
28
29  bash >= 4.2
30
31  findutils >= 4.5
32
33  gawk >= 4.0
34
35  sed >= 4.2
36
37  cups >= 1.6.0
38
39  foomatic-filters >= 4.0.9
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
40
41  libxml2 >= 2.9
42
43  libmspack >= 0.5
44
45  ibus >= 1.5
46
47  cyrus-sasl-gssapi >= 2.1
48
49  gperftools-libs >= 2.4
50
51  nss-tools >= 3.44.0
52
53  qt5-qtbase >= 5.5~
54
55  qrencode-libs >= 3.4.1
56
57  imlib2 >= 1.4.5
58  <!--NeedCopy-->
```

> **Note:**
>
> For a matrix of the Linux distributions and the Xorg versions that this version of the Linux VDA supports, see System requirements.
>
> After installing the Linux VDA on RHEL 7.x, run the `sudo yum install -y python-websockify x11vnc` command. The purpose is to install `python-websockify` and `x11vnc` manually for using the session shadowing feature. For more information, see Shadow sessions.

To upgrade an existing installation

You can upgrade an existing installation from the previous two versions and from an LTSR release.

> **Note:**
>
> Upgrading an existing installation overwrites the configuration files under /etc/xdl. Before you conduct an upgrade, make sure to back up the files.

- To upgrade your software using Yum:

  For Amazon Linux 2:

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

  For RHEL 9.0 and Rocky Linux 9.0:

  ```
  1  sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
  2  <!--NeedCopy-->
  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For RHEL 8 and Rocky Linux 8.6:

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

For CentOS 7 and RHEL 7:

```
sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
<!--NeedCopy-->
```

- To upgrade your software using the RPM package manager:

For Amazon Linux 2:

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

For RHEL 9.0 and Rocky Linux 9.0:

```
sudo rpm -U XenDesktopVDA-<version>.el9_x.x86_64.rpm
<!--NeedCopy-->
```

For RHEL 8 and Rocky Linux 8.6:

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

For CentOS 7 and RHEL 7:

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

> **Note:**
>
> If you are using RHEL 7, make sure to complete the following steps after you run the preceding upgrade commands:
>
> 1. run `/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_SZ"-v "DotNetRuntimePath"-d "/opt/rh/rh-dotnet31/root/usr/bin/"--force` to set the right .NET runtime path.
> 2. Restart the `ctxvda` service.
>
> **Important:**
>
> Restart the Linux VDA machine after upgrading the software.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 7: Install NVIDIA GRID drivers

Enabling HDX 3D Pro requires you to install the NVIDIA GRID drivers on your hypervisor and on the VDA machines.

> **Note:**
>
> To use HDX 3D Pro for Amazon Linux 2, we recommend you install NVIDIA driver 470. For more information, see System requirements.

To install and configure the NVIDIA GRID Virtual GPU Manager (the host driver) on the specific hypervisors, see the following guides:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

To install and configure the NVIDIA GRID guest VM drivers, perform the following steps:

1. Ensure that the guest VM is shut down.
2. In XenCenter, allocate a GPU to the VM.
3. Start the VM.
4. Prepare the VM for the NVIDIA GRID driver:

```
yum install gcc

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

systemctl set-default multi-user.target
<!--NeedCopy-->
```

5. 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:**
>
> After GPU pass-through is enabled, the Linux VM is no longer accessible through XenCenter. Use SSH to connect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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 multi-monitor capabilities, you need a valid NVIDIA license. To apply for the license, follow the product documentation from "GRID Licensing Guide.pdf - DU-07757-001 September 2015."

Step 8: Configure the Linux VDA

After installing the package, you must configure the Linux VDA by running the ctxsetup.sh script. Before making any changes, the script verifies the environment and ensures that all dependencies are installed. If necessary, you can rerun the script at any time to change settings.

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

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

Prompted configuration

Run a manual configuration with prompted questions:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. Set to N by default.
- **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 through a TCP/IP port, which is port 80 by default.
- **CTX_XDL_REGISTER_SERVICE=Y | N** - The Linux VDA services are started after machine startup. The value is set to Y by default.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –The Linux VDA services require incoming network connections to be allowed through the system firewall. You can open the required ports (ports 80 and 1494 by default) automatically in the system firewall for the Linux Virtual Desktop. Set to Y by default.
- **CTX_XDL_AD_INTEGRATION=1 | 2 | 3 | 4 | 5** –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 Services
  - 3 –Centrify DirectControl
  - 4 –SSSD
  - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO=Y | N** –The Linux VDA supports HDX 3D Pro, a set of GPU acceleration technologies designed to optimize the virtualization of graphics-intensive applications. If HDX 3D Pro is selected, the VDA is configured for VDI desktops (single-session) mode - (that is, 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 variable to Y. This variable is set to N by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_SITE_NAME=dns-name** –The Linux VDA discovers LDAP servers through DNS. To limit the DNS search results to a local site, specify a DNS site name. This variable is set to **<none>** by default.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –The Linux VDA queries DNS to discover LDAP servers. If DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP FQDNs with LDAP ports. For example, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. If you specify the LDAP port number as 389, the Linux VDA queries each LDAP server in the specified domain in polling mode. If there are x number of policies and y number of LDAP servers, the Linux VDA performs the total of X multiplied by Y queries. If the polling time exceeds the threshold, session logons might fail. To enable the faster LDAP queries, enable **Global Catalog** on a domain controller and specify the relevant LDAP port number as 3268. This variable is set to **<none>** by default.
- **CTX_XDL_SEARCH_BASE=search-base-set** –The Linux VDA queries LDAP through a search base set to the root of the Active Directory Domain (for example, DC=mycompany,DC=com). To improve search performance, you can specify a search base (for example, OU=VDI,DC=mycompany,DC=com). This variable is set to **<none>** by default.
- **CTX_XDL_FAS_LIST='list-fas-servers'**–The Federated Authentication Service (FAS) servers are configured through AD Group Policy. The Linux VDA does not support AD Group Policy, but you can provide a semicolon-separated list of FAS servers instead. The sequence must be the same as configured in AD Group Policy. If any server address is removed, fill its blank with the **<none>** text string and do not modify the order of server addresses. To communicate with FAS servers properly, make sure you append a port number consistent with the port number specified on the FAS servers, for example, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** –The path to install .NET Runtime 6.0 for supporting the new broker agent service (`ctxvda`). The default path is /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –Specifies the GNOME, GNOME Classic, or MATE desktop environment to use in sessions. If you leave the variable unspecified, the desktop currently installed on the VDA is used. However, if the currently installed desktop is MATE, you must set the variable value to **mate**.

  You can also change the desktop environment for a target session user by completing the following steps:

  1. Create an `.xsession` or `.Xclients` file under the **$HOME/<username>** directory on the VDA. If you are using Amazon Linux 2, create a `.Xclients` file. If you are using other distributions, create an `.xsession` file.
  2. Edit the `.xsession` or `.Xclients` file to specify a desktop environment.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **For MATE desktop**

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

- **For GNOME Classic desktop**

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

- **For GNOME desktop**

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

3. Share the 700 file permission with the target session user.

Starting with Version 2209, session users can customize their desktop environments. To enable this feature, you must install switchable desktop environments on the VDA in advance. For more information, see Custom desktop environments by session users.

- **CTX_XDL_START_SERVICE=Y | N** –Whether or not the Linux VDA services are started when the Linux VDA configuration is complete. Set to Y by default.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** –The socket port for listening for Citrix Scout. The default port is 7503.
- **CTX_XDL_TELEMETRY_PORT** –The port for communicating with Citrix Scout. The default port is 7502.

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|5

export CTX_XDL_HDX_3D_PRO=Y|N
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
      none>'
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

When running the sudo command, type the **-E** option to pass the existing environment variables to the new shell it creates. We recommend that you create a shell script file from the preceding commands with **#!/bin/bash** as the first line.

Alternatively, you can specify all parameters by using a single command:

```
1  sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3  CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5  CTX_XDL_VDA_PORT=port-number \
6
7  CTX_XDL_REGISTER_SERVICE=Y|N \
8
9  CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

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
<!--NeedCopy-->
```

To remove configuration changes:

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

> **Important:**
>
> This script deletes all configuration data from the database and renders 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.

Step 9: Run XDPing

Run `sudo /opt/Citrix/VDA/bin/xdping` to check for common configuration issues with a Linux VDA environment. For more information, see XDPing.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 10: Run the Linux VDA

After configuring the Linux VDA by using the **ctxsetup.sh** script, you can run the following commands to control the Linux VDA.

Start the Linux VDA:

To start the Linux VDA services:

```
sudo /sbin/service ctxhdx start

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

Stop the Linux VDA:

To stop the Linux VDA services:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

> **Note:**
>
> Before you stop the `ctxvda` and `ctxhdx` services, run the `service ctxmonitorservice stop` command to stop the monitor service daemon. Otherwise, the monitor service daemon restarts the services you stopped.

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
<!--NeedCopy-->
```

Check the status of the Linux VDA:

To check the running status of the Linux VDA services:

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 11: Create machine catalogs

The process for creating machine catalogs and adding Linux VDA machines is 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:
  - The **Multi-session OS** option for a hosted shared desktops delivery model.
  - The **Single-session OS** option for a VDI dedicated desktop delivery model.
- 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 single user per machine delivery model.
>
> **Tip:**
>
> When you rejoin a removed machine to the Active Directory domain, remove the machine from and add it back to its machine catalog.

Step 12: Create delivery groups

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:

- Ensure that the AD users and groups that 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:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 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.

For information about how to create machine catalogs and delivery groups, see Citrix Virtual Apps and Desktops 7 2212.

Install the Linux VDA on SUSE manually

January 11, 2024

> **Important:**
>
> For fresh installations, we recommend you use easy install for a quick installation. Easy install saves time and labor and is less error-prone than the manual installation detailed in this article.

Step 1: Prepare configuration information and the Linux machine

Step 1a: Launch the 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
<!--NeedCopy-->
```

To launch the UI-based YaST tool:

```
su -

yast2 &
<!--NeedCopy-->
```

Step 1b: Configure networking

The following sections provide information on configuring the various networking settings and services used by the Linux VDA. Configuring networking is 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 that is not documented here.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure host name and Domain Name System (DNS)

1. Launch the UI-based YaST tool.
2. Select **System** and then **Network Settings**.
3. Open the **Hostname/DNS** tab.
4. Select the **no** option for **Set Hostname via DHCP**.
5. Select the **Use Custom Policy** option for **Modify DNS Configuration**.
6. Edit the following to reflect your networking setup:
   - **Static Hostname** –Add the DNS host name of the machine.
   - **Name Server** –Add the IP address of the DNS server. It is typically the IP address of the AD Domain Controller.
   - **Domain Search List** –Add the DNS domain name.
7. Change the following line of the `/etc/hosts` file to include the FQDN and host name as the first two entries:

   ```
   127.0.0.1 <FQDN of the VDA> <hostname of the VDA> localhost
   ```

> **Note:**
>
> The Linux VDA currently does not support NetBIOS name truncation. Therefore, the host name 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 host name with a number and do not end with a hyphen. This rule also applies to Delivery Controller host names.

Check the host name Verify that the host name is set correctly:

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

This command returns only the machine's host name and not its Fully Qualified Domain Name (FQDN).

Verify that the FQDN is set correctly:

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

This command returns the machine's FQDN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Check name resolution and service reachability Verify that you can resolve the FQDN and ping the domain controller and Delivery Controller:

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

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

Step 1c: Configure the NTP service

It is crucial to maintain accurate clock synchronization between the VDAs, Delivery Controllers, and domain controllers. Hosting the Linux VDA as a virtual machine (VM) 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.

For SUSE 15.3:

1. Launch the UI-based YaST tool.
2. Select **Network Services** and then **NTP Configuration**.
3. In the **Start NTP Daemon** section, select **Now and on Boot**.
4. Select **Dynamic** for **Configuration Source**.
5. Add NTP servers as needed. The NTP service is normally hosted on the Active Directory domain controller.
6. Delete or comment the following line in /etc/chrony.conf if it exists.

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

   After editing chrony.conf, restart the `chronyd` service.

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

Step 1d: Install Linux VDA dependent packages

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

- OpenJDK 11

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Open Motif Runtime Environment 2.3.1 or later
- Cups 1.6.0 or later
- ImageMagick 6.8 or later

Add repositories You can obtain most required packages except ImageMagick from official repositories. To obtain the ImageMagick packages, enable the `sle-module-desktop-applications` repository by using YaST or the following command:

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

Install the Kerberos client Install the Kerberos client for mutual authentication between the Linux VDA and the Delivery Controllers:

```
1 sudo zypper install krb5-client
2 <!--NeedCopy-->
```

The Kerberos client configuration depends on which Active Directory integration approach is used. See the following description.

Install OpenJDK 11 The Linux VDA requires the presence of OpenJDK 11.

To install OpenJDK 11, run the following command:

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

Install and specify a database to use As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL by editing `/etc/xdl/db.conf` after installing the Linux VDA package. For manual installations, you must install SQLite and PostgreSQL manually before being able to switch between them.

This section describes how to install the PostgreSQL and SQLite databases and how to specify a database to use.

> **Note:**
>
> We recommend you use SQLite for VDI mode only.

Install PostgreSQL To install `Postgresql`, run the following commands:

```
1 sudo zypper install postgresql-server
2
3 sudo zypper install postgresql-jdbc
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Run the following commands to start PostgreSQL upon machine startup or immediately, respectively:

```
sudo systemctl enable postgresql

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

Install SQLite For SUSE, run the following command to install SQLite:

```
sudo zypper install sqlite3
<!--NeedCopy-->
```

Specify a database to use After you install SQLite, PostgreSQL, or both, you can specify a database to use by editing `/etc/xdl/db.conf` after installing the Linux VDA package. To do so, complete the following steps:

1. Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.
2. Edit `/etc/xdl/db.conf` to specify a database to use.
3. Run `ctxsetup.sh`.

> **Note:**
>
> You can also use `/etc/xdl/db.conf` to configure the port number for PostgreSQL.

Step 2: Prepare the hypervisor

Some changes are required when running the Linux VDA as a VM on a supported hypervisor. Make the following changes based on 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 Hypervisor

If the Citrix Hypervisor Time Sync feature is enabled, within each paravirtualized Linux VM you experience issues with NTP and Citrix Hypervisor. Both try to manage the system clock. To avoid the clock becoming out of sync with other servers, synchronize the system clock within each Linux guest with NTP. This case requires disabling host time synchronization. No changes are required in HVM mode.

If you are running a paravirtualized Linux kernel with Citrix VM Tools installed, you can check whether the Citrix Hypervisor Time Sync feature is present and enabled from within the Linux VM:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
su -

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

This command returns 0 or 1:

- 0 - The time sync feature is enabled, and must 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
<!--NeedCopy-->
```

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

```
xen.independent_wallclock = 1
```

To verify these changes, restart the system:

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

After restart, verify that the setting is correct:

```
su -

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

This command returns the value 1.

Fix time synchronization on Microsoft Hyper-V

Linux VMs with Hyper-V Linux Integration Services installed can apply the Hyper-V time synchronization feature to use the host operating system's time. To ensure that the system clock remains accurate, enable this feature alongside the 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 that **Time synchronization** is selected.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> This approach is different from VMware and Citrix Hypervisor, 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 experience issues with NTP and the hypervisor. Both try to synchronize the system clock. To avoid the clock becoming out of sync with other servers, synchronize the system clock within each Linux guest with NTP. This case 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**.

Step 3: Add the Linux VM to the Windows domain

The following methods are available for adding Linux machines to the Active Directory (AD) domain:

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Follow instructions based on your chosen method.

> **Note:**
>
> Session launches might fail when the same user name is used for the local account in the Linux VDA and for the account in AD.

Samba Winbind

Join Windows domain Your domain controller must be reachable and you must have an Active Directory user account with permissions to add machines to the domain:

1. Launch YaST, select **Network Services** and then **Windows Domain Membership**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 that the domain name is in uppercase.
    - Check **Use SMB information for Linux Authentication**.
        - Check **Create Home Directory on Login**.
        - Check **Single Sign-on for SSH**.
        - Ensure that **Offline Authentication** is not checked. This option is not compatible with the Linux VDA.

3. Click **OK**. If you are prompted to install some packages, click **Install**.
4. If a domain controller is found, it asks whether you want to join the domain. Click **Yes**.
5. When prompted, type the credentials of a domain user with permission to add machines to the domain and click **OK**.
6. Restart your services manually or restart the machine. We recommend you restart the machine:

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

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in Active Directory.

Run the **net ads** command of **Samba** to verify that the machine is joined to a domain:

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

Run the following command to verify extra domain and computer object information:

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

Verify Kerberos configuration Make sure that the system keytab file has been created and contains valid keys:

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

This command displays 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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

The machine and realm names must be specified in uppercase. 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
<!--NeedCopy-->
```

Examine the machine account details using:

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

Verify user authentication Use the **wbinfo** tool to verify that domain users can authenticate with the domain:

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

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 returns a message indicating success or failure.

Verify that the Winbind PAM module is configured correctly. To do so, log on to the Linux VDA using a domain user account that has not been used before.

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

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

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

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

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

Exit the session.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

A similar test can be performed by logging on to the Gnome or KDE console directly. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

Quest authentication service

Configure Quest on domain controller Assume that you have installed and configured the Quest software on the 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 To enable domain users 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 the **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 Autorenewal of Kerberos tickets must be enabled and disconnected. Authentication (offline logon) must 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
<!--NeedCopy-->
```

This command sets the renewal interval to nine hours (32,400 seconds) which is one hour less than the default 10-hour ticket lifetime. Set this parameter to a lower value on systems with a shorter ticket lifetime.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure PAM and NSS To enable domain user logons through HDX and other services such as su, ssh, and RDP, configure PAM and NSS manually:

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

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

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
<!--NeedCopy-->
```

The **user** is any domain user who has permissions to join machines to the Active Directory domain. The **domain-name** is the DNS name of the domain, for example, example.com.

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) 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
<!--NeedCopy-->
```

If the machine is joined to a domain, this command returns the domain name. If the machine is not joined to any domain, the following error appears:

```
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 Verify that Quest can authenticate domain users through PAM. To do so, log on to the Linux VDA using a domain user account that has not been used before.

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verify that the tickets in the Kerberos credential cache are valid and not expired:

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

Exit the session.

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

A similar test can be performed by logging on to the Gnome or KDE console directly. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

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:

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

The **user** is any Active Directory domain user who has permissions to join machines to the Active Directory domain. The **domain-name** is the name of the domain to join the Linux machine to.

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in Active Directory. To verify that a Centrify-joined Linux machine is on the domain:

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

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

Test connectivity to the various Active Directory and Kerberos services.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SSSD

If you are using SSSD on SUSE, follow the instructions in this section. This section includes instructions for joining a Linux VDA machine to a Windows domain and provides guidance for configuring Kerberos authentication.

To set up SSSD on SUSE, complete the following steps:

1. Join the domain and create host keytabs
2. Configure PAM for SSSD
3. Set up SSSD
4. Enable SSSD
5. Verify domain membership
6. Verify the Kerberos configuration
7. Verify user authentication

Join the domain and create host keytab SSSD does not provide Active Directory client functions for joining the domain and managing the system keytab file. You can use the **Samba** approach instead. Complete the following steps before configuring SSSD.

1. Stop and disable the Name Service Cache Daemon (NSCD) daemon.

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

2. Check the host name and Chrony time synchronization.

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

3. Install or update the required packages:

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

4. Edit the `/etc/krb5.conf` file as a root user to permit the **kinit** utility to communicate with the target domain. Add the following entries under the **[libdefaults]**, **[realms]**, and **[domain_realm]** sections:

> **Note:**
>
> Configure Kerberos based on your AD infrastructure. The following settings are meant for the single-domain, single-forest model.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
[libdefaults]

    dns_canonicalize_hostname = false

    rdns = false

    default_realm = REALM

    forwardable = true

[realms]

    REALM = {


        kdc = fqdn-of-domain-controller

        default_domain = realm

        admin_server = fqdn-of-domain-controller
     }

[domain_realm]

    .realm = REALM
<!--NeedCopy-->
```

realm is the Kerberos realm name, such as example.com. **REALM** is the Kerberos realm name in uppercase, such as EXAMPLE.COM.

5. Edit `/etc/samba/smb.conf` as a root user to permit the **net** utility to communicate with the target domain. Add the following entries under the **[global]** section:

```
[global]
    workgroup = domain

    client signing = yes

    client use spnego = yes

    kerberos method = secrets and keytab

    realm = REALM

    security = ADS
<!--NeedCopy-->
```

domain is the short NetBIOS name of an Active Directory domain, such as EXAMPLE.

6. Modify the **passwd** and **group** entries in the `/etc/nsswitch.conf` file to reference SSSD when resolving users and groups.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
passwd: compat sss

group: compat sss
<!--NeedCopy-->
```

7. Use the configured Kerberos client to authenticate to the target domain as Administrator.

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

8. Use the **net** utility to join the system to the domain and generate a system keytab file.

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

Configure PAM for SSSD Before configuring PAM for SSSD, install or update the required packages:

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

Configure the PAM module for user authentication through SSSD and create home directories for user logons.

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

Set up SSSD

1. Edit `/etc/sssd/sssd.conf` as a root user to permit the SSSD daemon to communicate with the target domain. An example `sssd.conf` configuration (extra options can be added as needed):

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
14
15 # Kerberos settings
16     krb5_ccachedir = /tmp
17     krb5_ccname_template = FILE:%d/krb5cc_%U
18
19 # Comment out if the users have the shell and home dir set on the
       AD side
20
21     fallback_homedir = /home/%d/%u
22     default_shell = /bin/bash
23
24 # Uncomment and adjust if the default principal SHORTNAME$@REALM
       is not available
25
26 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
27
28     ad_gpo_access_control = permissive
29
30 <!--NeedCopy-->
```

domain-dns-name is the DNS domain name, such as example.com.

> **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. **ad_gpo_access_control** is set to **permissive** to prevent an invalid logon error for Linux sessions. See the man pages for `sssd.conf` and `sssd-ad`.

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

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

Enable SSSD Run the following commands to enable and start the SSSD daemon at system startup:

```
1 sudo systemctl enable sssd
2 sudo systemctl start sssd
3 <!--NeedCopy-->
```

Verify domain membership

1. Run the `net ads` command of **Samba** to verify that the machine is joined to a domain:

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

2. Run the following command to verify extra domain and computer object information:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Verify Kerberos configuration Make sure that the system keytab file has been created and contains valid keys:

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

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. 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
<!--NeedCopy-->
```

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 to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\username

id -u

klist

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

Verify that the Kerberos tickets returned by the `klist` command are correct for that user and have not expired.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

A similar test can be performed by logging on to the Gnome or KDE console directly. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

PBIS

Download the required PBIS package For example:

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

Make the PBIS installation script executable For example:

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

Run the PBIS installation script For example:

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

Join a Windows domain Your domain controller must be reachable and you must have an Active Directory user account with permissions to add machines to the domain:

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

The **user** is a domain user who has permissions to add machines to the Active Directory domain. The **domain-name** is the DNS name of the domain, for example, example.com.

Note: To set Bash as the default shell, run the **/opt/pbis/bin/config LoginShellTemplate/bin/bash** command.

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in `Active Directory`. To verify that a PBIS-joined Linux machine is on the domain:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

If the machine is joined to a domain, this command returns the information about the currently joined AD domain and OU. Otherwise, only the host name appears.

Verify user authentication Verify that PBIS can authenticate domain users through PAM. To do so, log on to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\user

id -u
<!--NeedCopy-->
```

Verify that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

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

Exit the session.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

Step 4: Install .NET Runtime 6.0

Before installing the Linux VDA, install .NET Runtime 6.0 according to the instructions at https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

After installing .NET Runtime 6.0, run the **which dotnet** command to find your runtime path.

Based on the command output, set the .NET runtime binary path. For example, if the command output is /aa/bb/dotnet, use /aa/bb as the .NET binary path.

Step 5: Download the Linux VDA package

1. Go to the Citrix Virtual Apps and Desktops download page.
2. Expand the appropriate version of Citrix Virtual Apps and Desktops.
3. Click **Components** to download the Linux VDA package that matches your Linux distribution and the GPG public key that you can use to verify the integrity of the Linux VDA package.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To verify the integrity of the Linux VDA package by using the public key, import the public key into the RPM database and run the following commands:

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

Step 6: Install the Linux VDA

Step 6a: Uninstall the old version

If you installed an earlier version other than the previous two and an LTSR release, uninstall it before installing the new version.

1. Stop the Linux VDA services:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

> **Note:**
>
> Before you stop the `ctxvda` and `ctxhdx` services, run the `service ctxmonitorservice stop` command to stop the monitor service daemon. Otherwise, the monitor service daemon restarts the services you stopped.

2. Uninstall the package:

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

> **Important:**
>
> Upgrading from the latest two versions is supported.
>
> **Note:**
>
> You can find installed components under **/opt/Citrix/VDA/**.
>
> To run a command, the full path is needed; alternatively, you can add **/opt/Citrix/VDA/sbin** and **/opt/Citrix/VDA/bin** to the system path.

Step 6b: Install the Linux VDA

Install the Linux VDA software using Zypper:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Install the Linux VDA software using the RPM package manager:

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

Step 6c: Upgrade the Linux VDA (optional)

You can upgrade an existing installation from the previous two versions and from an LTSR release.

> **Note:**
>
> Upgrading an existing installation overwrites the configuration files under /etc/xdl. Before you conduct an upgrade, make sure to back up the files.

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

RPM Dependency list for SUSE 15:

```
java-11-openjdk >= 11

ImageMagick >= 7.0

dbus-1 >= 1.12.2

dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.4

cups >= 2.2

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
cups-filters >= 1.25

libxml2-2 >= 2.9

libmspack0 >= 0.6

ibus >= 1.5

libtcmalloc4 >= 2.5

libcap-progs >= 2.26

mozilla-nss-tools >= 3.53.1

libpython3_6m1_0 >= 3.6~

libQt5Widgets5 >= 5.12

libqrencode4 >= 4.0.0

libImlib2-1 >= 1.4.10
<!--NeedCopy-->
```

> **Important:**
>
> Restart the Linux VDA machine after upgrading.

Step 7: Install NVIDIA GRID drivers

Enabling HDX 3D Pro requires you to install the NVIDIA GRID drivers on your hypervisor and on the VDA machines.

To install and configure the NVIDIA GRID Virtual GPU Manager (the host driver) on the specific hypervisors, see the following guides:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

To install and configure the NVIDIA GRID guest VM drivers, perform the following general steps:

1. Make sure that the guest VM is shut down.
2. In the hypervisor control panel, allocate a GPU to the VM.
3. Start the VM.
4. Install the guest VM driver on the VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 8: Configure the Linux VDA

After installing the package, you must configure the Linux VDA by running the `ctxsetup.sh` script. Before the script makes any changes, it verifies the environment and ensures that all dependencies are installed. If necessary, you can rerun the script at any time to change settings.

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

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

Prompted configuration

Run a manual configuration with prompted questions:

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

Automated configuration

For an automated installation, 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. Set to N by default.
- **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 through a TCP/IP port, which is port 80 by default.
- **CTX_XDL_REGISTER_SERVICE=Y | N** - The Linux VDA services are started after machine startup. The value is set to Y by default.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –The Linux VDA services require incoming network connections to be allowed through the system firewall. You can open the required ports (ports 80 and 1494 by default) automatically in the system firewall for the Linux VDA. Set to Y by default.
- **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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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** –The Linux VDA supports HDX 3D Pro, a set of GPU acceleration technologies designed to optimize the virtualization of rich graphics applications. If HDX 3D Pro is selected, the VDA is configured for VDI desktops (single-session) mode - (that is, 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 variable to Y. This variable is set to N by default.
- **CTX_XDL_SITE_NAME=dns-name** –The Linux VDA discovers LDAP servers through DNS. To limit the DNS search results to a local site, specify a DNS site name. This variable is set to **<none>** by default.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –The Linux VDA queries DNS to discover LDAP servers. If DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP FQDNs with LDAP ports. For example, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. If you specify the LDAP port number as 389, the Linux VDA queries each LDAP server in the specified domain in polling mode. If there are x number of policies and y number of LDAP servers, the Linux VDA performs the total of X multiplied by Y queries. If the polling time exceeds the threshold, session logons might fail. To enable the faster LDAP queries, enable **Global Catalog** on a domain controller and specify the relevant LDAP port number as 3268. This variable is set to **<none>** by default.
- **CTX_XDL_SEARCH_BASE=search-base-set** –The Linux VDA queries LDAP through a search base set to the root of the Active Directory Domain (for example, DC=mycompany,DC=com). To improve search performance, you can specify a search base (for example, OU=VDI,DC=mycompany,DC=com). This variable is set to **<none>** by default.
- **CTX_XDL_FAS_LIST='list-fas-servers'**–The Federated Authentication Service (FAS) servers are configured through AD Group Policy. The Linux VDA does not support AD Group Policy, but you can provide a semicolon-separated list of FAS servers instead. The sequence must be the same as configured in AD Group Policy. If any server address is removed, fill its blank with the **<none>** text string and do not modify the order of server addresses. To communicate with FAS servers properly, make sure you append a port number consistent with that specified on the FAS servers, for example, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** –The path to install .NET Runtime 6.0 for supporting the new broker agent service (`ctxvda`). The default path is /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –Specifies the GNOME, GNOME Classic, or MATE desktop environment to use in sessions. If you leave the variable unspecified, the desktop currently installed on the VDA is used. However, if the currently installed desktop is MATE, you must set the variable value to **mate**.

  You can also change the desktop environment for a target session user by completing the following steps:

  1. Create an `.xsession` file under the **$HOME/<username>** directory on the VDA.
  2. Edit the `.xsession` file to specify a desktop environment.
     - **For MATE desktop on SUSE 15**

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

     - **For GNOME Classic desktop on SUSE 15**

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

     - **For GNOME desktop on SUSE 15**

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

  3. Share the 700 file permission with the target session user.

  Starting with Version 2209, session users can customize their desktop environments. To enable this feature, you must install switchable desktop environments on the VDA in advance. For more information, see Custom desktop environments by session users.

- **CTX_XDL_START_SERVICE=Y | N** –Whether or not the Linux VDA services are started when the Linux VDA configuration is complete. Set to Y by default.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** –The socket port for listening for Citrix Scout. The default port is 7503.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_TELEMETRY_PORT** –The port for communicating with Citrix Scout. The default port is 7502.

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-site-name | '<none>'

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

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

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

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

When running the sudo command, type the **-E** option to pass the existing environment variables to the new shell it creates. We recommend that you create a shell script file from the preceding commands with **#!/bin/bash** as the first line.

Alternatively, you can specify all parameters by using a single command:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

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
<!--NeedCopy-->
```

To remove configuration changes:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important:**
>
> This script deletes all configuration data from the database and renders 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.

Step 9: Run XDPing

Run `sudo /opt/Citrix/VDA/bin/xdping` to check for common configuration issues with a Linux VDA environment. For more information, see XDPing.

Step 10: Run the Linux VDA

After configuring the Linux VDA by using the **ctxsetup.sh** script, you can run the following commands to control the Linux VDA.

Start the Linux VDA:

To start the Linux VDA services:

```
sudo /sbin/service ctxhdx start

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

Stop the Linux VDA:

To stop the Linux VDA services:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx stop
<!--NeedCopy-->
```

> **Note:**
>
> Before you stop the `ctxvda` and `ctxhdx` services, run the `service ctxmonitorservice stop` command to stop the monitor service daemon. Otherwise, the monitor service daemon

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> restarts the services you stopped.

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
<!--NeedCopy-->
```

Check the Linux VDA status:

To check the running status of the Linux VDA services:

```
sudo /sbin/service ctxvda status

sudo /sbin/service ctxhdx status
<!--NeedCopy-->
```

Step 11: Create machine catalogs

The process for creating machine catalogs and adding Linux VDA machines is 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:
  - The **Multi-session OS** option for a hosted shared desktops delivery model.
  - The **Single-session OS** option for a VDI dedicated desktop delivery model.
- 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 single user per machine delivery model.
>
> **Tip:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> If you remove and rejoin a machine to the Active Directory domain, you must remove and add the machine to the machine catalog again.

Step 12: Create delivery groups

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:

- Make sure that the AD users and groups that 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.

For information about how to create machine catalogs and delivery groups, see Citrix Virtual Apps and Desktops 7 2212.

Install the Linux VDA on Ubuntu manually

April 23, 2023

> **Important:**
>
> For fresh installations, we recommend you use easy install for a quick installation. Easy install saves time and labor and is less error-prone than the manual installation detailed in this article.

Step 1: Prepare configuration information and the Linux machine

Step 1a: Verify the network configuration

Make sure that the network is connected and configured correctly. For example, you must configure the DNS server on the Linux VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

If you are using a Ubuntu 18.04 Live Server, make the following change in the **/etc/cloud/cloud.cfg** configuration file before setting the host name:

```
preserve_hostname: true
```

Step 1b: Set the host name

To make sure that the host name of the machine is reported correctly, change the **/etc/hostname** file to contain only the host name of the machine.

```
hostname
```

Step 1c: Assign a loopback address to the host name

Make sure that the DNS domain name and Fully Qualified Domain Name (FQDN) of the machine are reported back correctly. The way is to change the following line of the **/etc/hosts** file to include the FQDN and host name 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 host name 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 host name with a number and do not end with a hyphen. This rule also applies to Delivery Controller host names.

Step 1d: Check the host name

Verify that the host name is set correctly:

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

This command returns only the host name of the machine and not its FQDN.

Verify that the FQDN is set correctly:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

This command returns the FQDN of the machine.

Step 1e: 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
```

Step 1f: Check name resolution and service reachability

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

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

Step 1g: Configure clock synchronization (chrony)

Maintaining accurate clock synchronization between the VDAs, Delivery Controllers and domain controllers is crucial. Hosting the Linux VDA as a virtual machine (VM) can cause clock skew problems. For this reason, synchronizing time with a remote time service is preferred.

Install chrony:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

As a root user, edit **/etc/chrony/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, synchronize time 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:

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

Step 1h: Install OpenJDK 11

The Linux VDA requires the presence of OpenJDK 11.

On Ubuntu 20.04 and Ubuntu 18.04, install OpenJDK 11 by using:

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

Step 1i: Install and specify a database to use

As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL by editing `/etc/xdl/db.conf` after installing the Linux VDA package. For manual installations, you must install SQLite and PostgreSQL manually before being able to switch between them.

This section describes how to install the PostgreSQL and SQLite databases and how to specify a database to use.

> **Note:**
>
> We recommend you use SQLite for VDI mode only.

Install PostgreSQL Run the following commands to install PostgreSQL:

```
sudo apt-get install -y postgresql

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Run the following commands to start PostgreSQL upon machine startup or immediately, respectively:

```
sudo systemctl enable postgresql

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

Install SQLite For Ubuntu, run the following command to install SQLite:

```
sudo apt-get install -y sqlite3
<!--NeedCopy-->
```

Specify a database to use After you install SQLite, PostgreSQL, or both, you can specify a database to use by editing `/etc/xdl/db.conf` after installing the Linux VDA package. To do so, complete the following steps:

1. Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.
2. Edit `/etc/xdl/db.conf` to specify a database to use.
3. Run `ctxsetup.sh`.

> **Note:**
>
> You can also use **/etc/xdl/db.conf** to configure the port number for PostgreSQL.

Step 1j: Install Motif

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

Step 1k: Install other packages

For Ubuntu 22.04:

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

For Ubuntu 20.04, Ubuntu 18.04:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.4-2
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Step 2: Prepare the hypervisor

Some changes are required when running the Linux VDA as a VM on a supported hypervisor. Make the following changes based on 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 Hypervisor

When the Citrix Hypervisor Time Sync feature is enabled, within each paravirtualized Linux VM you experience issues with NTP and Citrix Hypervisor. Both try to manage the system clock. To avoid the clock becoming out of sync with other servers, make sure that the system clock within each Linux guest is synchronized with the NTP. This case requires disabling host time synchronization. No changes are required in HVM mode.

If you are running a paravirtualized Linux kernel with Citrix VM Tools installed, you can check whether the Citrix Hypervisor Time Sync feature is present and enabled from within the Linux VM:

```
su -

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

This command returns 0 or 1:

- 0 - The time sync feature is enabled, and must 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
<!--NeedCopy-->
```

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

```
xen.independent_wallclock = 1
```

To verify these changes, restart the system:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
su -

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

This command returns the value 1.

Fix time synchronization on Microsoft Hyper-V

Linux VMs with Hyper-V Linux Integration Services installed can use the Hyper-V time synchronization feature to use the host operating system's time. To make sure that the system clock remains accurate, enable this feature 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 that **Time synchronization** is selected.

> **Note:**
>
> This approach is different from VMware and Citrix Hypervisor, 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

When the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you experience issues with the NTP and the hypervisor. Both try to synchronize the system clock. To avoid the clock becoming out of sync with other servers, make sure that the system clock within each Linux guest is synchronized with the NTP. This case 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**.

Step 3: Add the Linux VM to the Windows domain

The following methods are available for adding Linux machines to the Active Directory (AD) domain:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Follow instructions based on your chosen method.

> **Note:**
>
> Session launches might fail when the same user name is used for the local account in the Linux VDA and the account in AD.

Samba Winbind

Install or update the required packages

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

Enable the Winbind daemon to start on machine startup The Winbind daemon must be configured to start on machine startup:

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

> **Note:**
>
> Ensure that the `winbind` script is located under `/etc/init.d`.

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

> **Note:**
>
> Configure Kerberos based on your AD infrastructure. The following settings are meant for the single-domain, single-forest model.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

The **domain-dns-name** parameter 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 Configure Winbind manually because 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 Your domain controller must be reachable and you must have an Active Directory user account with permissions to add computers to the domain:

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
<!--NeedCopy-->
```

Configure PAM for Winbind Run the following command and make sure that the **Winbind NT/Active Directory authentication** and **Create home directory on login** options are selected:

```
sudo pam-auth-update
<!--NeedCopy-->
```

> **Tip:**
>
> The **winbind** daemon stays running only if the machine is joined to a domain.

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

Run the **net ads** command of **Samba** to verify that the machine is joined to a domain:

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

Run the following command to verify extra domain and computer object information:

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

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

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

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. The dollar sign ($) must be escaped with a backslash (\) to prevent shell substitution. In some environments, the DNS domain name is

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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
<!--NeedCopy-->
```

Examine the account details of the machine using:

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

Verify user authentication Use the **wbinfo** tool to verify that domain users can authenticate with the domain:

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

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 returns a message indicating success or failure.

To verify that the Winbind PAM module is configured correctly, log on to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\username

id -u
<!--NeedCopy-->
```

> **Note:**
>
> To run an SSH command successfully, make sure that SSH is enabled and working properly.

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

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

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

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

Exit the session.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

A similar test can be performed by logging on to the Gnome or KDE console directly. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

> **Tip:**
>
> If you succeed in user authentication but cannot show your desktop when logging on with a domain account, restart the machine and then try again.

Quest authentication service

Configure Quest on domain controller Assume that 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 To enable domain users 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 the **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

Work around SELinux policy enforcement The default RHEL environment has SELinux fully enforced. This enforcement interferes with the Unix domain socket IPC mechanisms used by Quest, and prevents domain users from logging on.

The convenient way to work around this issue is to disable SELinux. As a root user, edit **/etc/selinux/config** and change the **SELinux** setting:

```
SELINUX=disabled
```

This change requires a machine restart:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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 Autorenewal of Kerberos tickets must be enabled and disconnected. Authentication (offline logon) must 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
<!--NeedCopy-->
```

This command sets the renewal interval to nine hours (32,400 seconds) which is one 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 To enable domain user logon through HDX and other services such as su, ssh, and RDP, run the following commands to configure PAM and NSS manually:

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

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

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
<!--NeedCopy-->
```

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

If the machine is joined to a domain, this command returns the domain name. If the machine is not joined to any domain, the following error appears:

```
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 through PAM, log on to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\username

id -u
<!--NeedCopy-->
```

Verify that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

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

Verify that the tickets in the Kerberos credential cache are valid and not expired:

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

Exit the session.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

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
<!--NeedCopy-->
```

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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verify domain membership The Delivery 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
<!--NeedCopy-->
```

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

Test connectivity to the various Active Directory and Kerberos services.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

SSSD

Configure Kerberos Run the following command to install Kerberos:

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

To configure Kerberos, open **/etc/krb5.conf** as root and set the parameters:

> **Note:**
>
> Configure Kerberos based on your AD infrastructure. The following settings are meant for the single-domain, single-forest model.

```
[libdefaults]

default_realm = REALM

dns_lookup_kdc = false

[realms]

REALM = {
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

The domain-dns-name parameter 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. You can use **adcli**, **realmd**, or **Samba** instead.

> **Note:**
>
> This section only provides information for **adcli** and **Samba**.

- **If you use adcli to join the domain, complete the following steps:**

1. Install **adcli**.

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

2. Join the 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
   <!--NeedCopy-->
   ```

   The **user** is a domain user with permissions to add machines to the domain. The **hostname-fqdn** is the host name in FQDN format for the machine.

   The **-H** option is necessary for **adcli** to generate SPN in the format of host/hostname-fqdn@REALM, which the Linux VDA requires.

3. Verify domain membership.

   For Ubuntu 22.04 and Ubuntu 20.04 machines, run the `adcli testjoin` command to test whether the machines are joined to the domain.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For a Ubuntu 18.04 machine, run the `sudo klist -ket` command. The capability of the **adcli** tool is limited. The tool doesn't provide a way to test whether a machine is joined to the domain. The best alternative is to ensure that the system keytab file has been created. Verify that the timestamp for each key matches the time the machine was joined to the domain.

- **If you use Samba to join the domain, complete the following steps:**

1. Install the package.

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

2. 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.

3. Join the domain with **Samba**.

   Your domain controller must be reachable and you must have a Windows account with permissions to add computers to the domain.

   ```
   sudo net ads join REALM -U user
   <!--NeedCopy-->
   ```

   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
<!--NeedCopy-->
```

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

> **Note:**
>
> By default, the install process in Ubuntu configures **nsswitch.conf** and the PAM login module automatically.

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 created manually. 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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. PAM service `ctxhdx` is added to ad_gpo_map_remote_interactive.
>
> The **domain-dns-name** parameter 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.
>
> For information about the 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
<!--NeedCopy-->
```

Start SSSD daemon Run the following commands to start the SSSD daemon now and to enable the daemon to start upon machine startup:

```
sudo systemctl start sssd

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

PAM configuration Run the following command and make sure that the **SSS authentication** and **Create home directory on login** options are selected:

```
sudo pam-auth-update
<!--NeedCopy-->
```

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in `Active Directory`.

- If you use **adcli** to verify domain membership, run the `sudo adcli info domain-dns-name` command to show the domain information.
- If you use **Samba** to verify domain membership, run the `sudo net ads testjoin` command to verify that the machine is joined to a domain and the `sudo net ads info` command to verify extra domain and computer object information.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. 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 for the machine account has been cached using:

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

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 to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\username

id -u

klist

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

Verify that the Kerberos tickets returned by the **klist** command are correct for that user and have not expired.

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

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

A similar test can be performed by logging on to KDE or Gnome Display Manager. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

PBIS

Download the required PBIS package

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

Make the PBIS installation script executable

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

Run the PBIS installation script

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

Join Windows domain Your domain controller must be reachable and you must have an Active Directory user account with permissions to add computers to the domain:

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

The **user** is a domain user who has permissions to add computers to the Active Directory domain. The **domain-name** is the DNS name of the domain, for example, example.com.

Note: To set Bash as the default shell, run the **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** command.

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in `Active Directory`. To verify that a PBIS-joined Linux machine is on the domain:

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

If the machine is joined to a domain, this command returns the information about the currently joined AD domain and OU. Otherwise, only the host name appears.

Verify user authentication To verify that PBIS can authenticate domain users through PAM, log on to the Linux VDA using a domain user account that has not been used before.

```
sudo ssh localhost -l domain\\user

id -u
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verify that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

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

Exit the session.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

Step 4: Install .NET Runtime 6.0

Before installing the Linux VDA, install .NET Runtime 6.0 according to the instructions at https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

After installing .NET Runtime 6.0, run the **which dotnet** command to find your runtime path.

Based on the command output, set the .NET runtime binary path. For example, if the command output is /aa/bb/dotnet, use /aa/bb as the .NET binary path.

Step 5: Download the Linux VDA package

1. Go to the Citrix Virtual Apps and Desktops download page.
2. Expand the appropriate version of Citrix Virtual Apps and Desktops.
3. Click **Components** to download the Linux VDA package that matches your Linux distribution and the GPG public key that you can use to verify the integrity of the Linux VDA package.

   To verify the integrity of the Linux VDA package by using the public key, import the public key into the DEB database and run the following commands:

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

### Step 6: Install the Linux VDA

#### Step 6a: Install the Linux VDA

Install the Linux VDA software using the Debian package manager:

© 1999–2024 Cloud Software Group, Inc. All rights reserved. 
   ```

For Ubuntu 22.04:

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

For Ubuntu 20.04:

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

> **Note:**
>
> For Ubuntu 20.04 on GCP, disable RDNS. To do so, add the **rdns = false** line under **[libdefaults]** in /etc/krb5.conf.

For Ubuntu 18.04:

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

Debian dependency list for Ubuntu 22.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.11

libgtkmm-3.0-1v5 >= 3.24.5

ufw >= 0.36

ubuntu-desktop >= 1.481

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.37

gtk3-nocsd >= 3

bash >= 5.1

findutils >= 4.8.0

sed >= 4.8

cups >= 2.4

libmspack0 >= 0.10

ibus >= 1.5
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
libgoogle-perftools4 >= 2.9~

libpython3.10 >= 3.10~

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

libnss3-tools >= 2:3.68

libqt5widgets5 >= 5.15~

libqrencode4 >= 4.1.1

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

Debian dependency list for Ubuntu 20.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

libgtkmm-3.0-1v5 >= 3.24.2

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.8 >= 3.8~
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

libnss3-tools >= 2:3.49

libqt5widgets5 >= 5.7~

libqrencode4 >= 4.0.0

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

Debian dependency list for Ubuntu 18.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.8.9.9

ufw >= 0.35

libgtkmm-3.0-1v5 >= 3.22.2

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

gtk3-nocsd >= 3

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libmspack0 >= 0.6

ibus >= 1.5

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

libgoogle-perftools4 >= 2.4~

libpython3.6 >= 3.6~

libnss3-tools >= 2:3.35
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
40
41 libqt5widgets5 >= 5.7~
42
43 libqrencode3 >= 3.4.4
44
45 libimlib2 >= 1.4.10
46 <!--NeedCopy-->
```

> **Note:**
>
> For a matrix of the Linux distributions and the Xorg versions that this version of the Linux VDA supports, see System requirements.

Step 6b: Upgrade the Linux VDA (optional)

You can upgrade an existing installation from the previous two versions and from an LTSR release.

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

> **Note:**
>
> Upgrading an existing installation overwrites the configuration files under /etc/xdl. Before you conduct an upgrade, make sure to back up the files.

Step 7: Install NVIDIA GRID drivers

Enabling HDX 3D Pro requires you to install the NVIDIA GRID drivers on your hypervisor and on the VDA machines.

To install and configure the NVIDIA GRID Virtual GPU Manager (the host driver) on the specific hypervisors, see the following guides:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

To install and configure the NVIDIA GRID guest VM drivers, perform the following general steps:

1. Ensure that the guest VM is shut down.
2. In the hypervisor control panel, allocate a GPU to the VM.
3. Start the VM.
4. Install the guest VM driver on the VM.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 8: Configure the Linux VDA

After installing the package, you must configure the Linux VDA by running the ctxsetup.sh script. Before making any changes, the script verifies the environment and ensures that all dependencies are installed. If necessary, you can rerun the script at any time to change settings.

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

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

Prompted configuration

Run a manual configuration with prompted questions:

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

Automated configuration

For an automated install, the options required by the setup script can be provided with environment variables. If all 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. Set to N by default.
- **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 through a TCP/IP port, which is port 80 by default.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –The Linux VDA services are started after machine startup. Set to Y by default.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –The Linux VDA services require incoming network connections to be allowed through the system firewall. You can open the required ports (ports 80 and 1494 by default) automatically in the system firewall for the Linux VDA. Set to Y by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_AD_INTEGRATION=1 | 2 | 3 | 4 |5** –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
  - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO=Y | N** –The Linux VDA supports HDX 3D Pro, a set of GPU acceleration technologies designed to optimize the virtualization of rich graphics applications. If HDX 3D Pro is selected, the VDA is configured for VDI desktops (single-session) mode - (that is, 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 variable to Y. This variable is set to N by default.
- **CTX_XDL_SITE_NAME=dns-name** –The Linux VDA discovers LDAP servers through DNS. To limit the DNS search results to a local site, specify a DNS site name. This variable is set to **<none>** by default.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –The Linux VDA queries DNS to discover LDAP servers. If DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP FQDNs with LDAP ports. For example, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. If you specify the LDAP port number as 389, the Linux VDA queries each LDAP server in the specified domain in polling mode. If there are x number of policies and y number of LDAP servers, the Linux VDA performs the total of X multiplied by Y queries. If the polling time exceeds the threshold, session logons might fail. To enable the faster LDAP queries, enable **Global Catalog** on a domain controller and specify the relevant LDAP port number as 3268. This variable is set to **<none>** by default.
- **CTX_XDL_SEARCH_BASE=search-base-set** –The Linux VDA queries LDAP through a search base set to the root of the Active Directory Domain (for example, DC=mycompany,DC=com). However, to improve search performance, you can specify a search base (for example, OU=VDI,DC=mycompany,DC=com). This variable is set to **<none>** by default.
- **CTX_XDL_FAS_LIST='list-fas-servers'**–The Federated Authentication Service (FAS) servers are configured through AD Group Policy. The Linux VDA does not support AD Group Policy, but you can provide a semicolon-separated list of FAS servers instead. The sequence must be the same as configured in AD Group Policy. If any server address is removed, fill its blank with the **<none>** text string and do not modify the order of server addresses. To communicate

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

with FAS servers properly, make sure you append a port number consistent with that specified on the FAS servers, for example, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.

- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** –The path to install .NET Runtime 6.0 for supporting the new broker agent service (`ctxvda`). The default path is /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –Specifies the GNOME, GNOME Classic, or MATE desktop environment to use in sessions. If you leave the variable unspecified, the desktop currently installed on the VDA is used. However, if the currently installed desktop is MATE, you must set the variable value to **mate**.

  You can also change the desktop environment for a target session user by completing the following steps:

  1. Create an `.xsession` file under the **$HOME/<username>** directory on the VDA.
  2. Edit the `.xsession` file to specify a desktop environment based on distributions.
     - **For MATE desktop**

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

     - **For GNOME Classic desktop**

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

     - **For GNOME desktop**

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

  3. Share the 700 file permission with the target session user.

  Starting with Version 2209, session users can customize their desktop environments. To enable this feature, you must install switchable desktop environments on the VDA in advance. For more information, see Custom desktop environments by session users.

- **CTX_XDL_START_SERVICE=Y | N** –Whether or not the Linux VDA services are started when the Linux VDA configuration is complete. Set to Y by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** –The socket port for listening for Citrix Scout. The default port is 7503.
- **CTX_XDL_TELEMETRY_PORT** –The port for communicating with Citrix Scout. The default port is 7502.

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|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

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

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

When running the sudo command, type the **-E** option to pass the existing environment variables to the new shell it creates. We recommend that you create a shell script file from the preceding commands with **#!/bin/bash** as the first line.

Alternatively, you can specify all parameters by using a single command:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

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

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

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
<!--NeedCopy-->
```

To remove configuration changes:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important:**
>
> This script deletes all configuration data from the database and renders 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

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

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

To view more detailed information:

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

To uninstall the Linux VDA software:

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

> **Note:**
>
> Uninstalling the Linux VDA software deletes the associated PostgreSQL and other configuration data. However, the PostgreSQL package and other dependent packages that were set up before the installation of the Linux VDA are not deleted.
>
> **Tip:**
>
> The information in this section does not cover the removal of dependent packages including PostgreSQL.

Step 9: Run XDPing

Run `sudo /opt/Citrix/VDA/bin/xdping` to check for common configuration issues with a Linux VDA environment. For more information, see XDPing.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 10: Run the Linux VDA

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
<!--NeedCopy-->
```

Stop the Linux VDA:

To stop the Linux VDA services:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

> **Note:**
>
> Before you stop the `ctxvda` and `ctxhdx` services, run the `service ctxmonitorservice stop` command to stop the monitor service daemon. Otherwise, the monitor service daemon restarts the services you stopped.

Restart the Linux VDA:

To restart the Linux VDA services:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

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

Check the Linux VDA status:

To check the running status of the Linux VDA services:

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 11: Create machine catalogs

The process for creating machine catalogs and adding Linux VDA machines is 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:
  - The **Multi-session OS** option for a hosted shared desktops delivery model.
  - The **Single-session OS** option for a VDI dedicated desktop delivery model.
- 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 single user per machine delivery model.
>
> **Tip:**
>
> If you remove and rejoin a machine to the Active Directory domain, you must remove and add the machine to the machine catalog again.

Step 12: Create delivery groups

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:

- Ensure that the AD users and groups that 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.

For information about how to create machine catalogs and delivery groups, see Citrix Virtual Apps and Desktops 7 2212.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Install the Linux VDA on Debian manually

February 1, 2023

> **Important:**
>
> For fresh installations, we recommend you use easy install for a quick installation. Easy install saves time and labor and is less error-prone than the manual installation detailed in this article.

Step 1: Prepare configuration information and the Linux machine

Step 1a: Verify the network configuration

Make sure that the network is connected and configured correctly. For example, you must configure the DNS server on the Linux VDA.

Step 1b: Set the host name

To make sure that the host name of the machine is reported correctly, change the **/etc/hostname** file to contain only the host name of the machine.

```
hostname
```

Step 1c: Assign a loopback address to the host name

Make sure that the DNS domain name and Fully Qualified Domain Name (FQDN) of the machine are reported back correctly. The way is to change the following line of the **/etc/hosts** file to include the FQDN and host name 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. The host name must not exceed 15 characters.
>
> **Tip:**
>
> Use a–z, A–Z, 0–9, and hyphen (-) characters only. Avoid underscores (_), spaces, and other sym-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> bols. Do not start a host name with a number and do not end with a hyphen. This rule also applies to Delivery Controller host names.

Step 1d: Check the host name

Verify that the host name is set correctly:

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

This command returns only the host name of the machine and not its FQDN.

Verify that the FQDN is set correctly:

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

This command returns the FQDN of the machine.

Step 1e: 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:

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

To:

```
hosts: files dns
```

Step 1f: Check name resolution and service reachability

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 1g: Configure clock synchronization (chrony)

Maintaining accurate clock synchronization between the VDAs, Delivery Controllers and domain controllers is crucial. Hosting the Linux VDA as a virtual machine (VM) can cause clock skew problems. For this reason, synchronizing time with a remote time service is preferred.

Install chrony:

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

As a root user, edit **/etc/chrony/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, synchronize time 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:

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

Step 1h: Install packages

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

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

Step 1i: Add repositories to install necessary dependencies

For Debian 11.3, add the `deb http://deb.debian.org/debian/ bullseye main` line to the /etc/apt/sources.list file.

Step 1j: Install and specify a database to use

As an experimental feature, you can use SQLite in addition to PostgreSQL. You can also switch between SQLite and PostgreSQL by editing `/etc/xdl/db.conf` after installing the Linux VDA package. For manual installations, you must install SQLite and PostgreSQL manually before being able to switch between them.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

This section describes how to install the PostgreSQL and SQLite databases and how to specify a database to use.

> **Note:**
>
> We recommend you use SQLite for VDI mode only.

Install PostgreSQL Run the following commands to install PostgreSQL:

```
sudo apt-get install -y postgresql

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

Run the following commands to start PostgreSQL upon machine startup or immediately, respectively:

```
sudo systemctl enable postgresql

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

Install SQLite For Debian, run the following command to install SQLite:

```
sudo apt-get install -y sqlite3
<!--NeedCopy-->
```

Specify a database to use After you install SQLite, PostgreSQL, or both, you can specify a database to use by editing `/etc/xdl/db.conf` after installing the Linux VDA package. To do so, complete the following steps:

1. Run `/opt/Citrix/VDA/sbin/ctxcleanup.sh`. Omit this step if it is a fresh installation.
2. Edit `/etc/xdl/db.conf` to specify a database to use.
3. Run `ctxsetup.sh`.

> **Note:**
>
> You can also use **/etc/xdl/db.conf** to configure the port number for PostgreSQL.

Step 2: Prepare the hypervisor

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fix time synchronization on Citrix Hypervisor

When the Citrix Hypervisor Time Sync feature is enabled, within each paravirtualized Linux VM you experience issues with NTP and Citrix Hypervisor. Both try to manage the system clock. To avoid the clock becoming out of sync with other servers, make sure that the system clock within each Linux guest is synchronized with the NTP. This case requires disabling host time synchronization. No changes are required in HVM mode.

If you are running a paravirtualized Linux kernel with Citrix VM Tools installed, you can check whether the Citrix Hypervisor Time Sync feature is present and enabled from within the Linux VM:

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

This command returns 0 or 1:

- 0 - The time sync feature is enabled, and must 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
<!--NeedCopy-->
```

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

```
xen.independent_wallclock = 1
```

To verify these changes, restart the system:

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

This command returns the value 1.

Fix time synchronization on Microsoft Hyper-V

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

From the management operating system:

1. Open the Hyper-V Manager console.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. For the settings of a Linux VM, select **Integration Services**.
3. Ensure that **Time synchronization** is selected.

> **Note:**
>
> This approach is different from VMware and Citrix Hypervisor, 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

When the VMware Time Synchronization feature is enabled, within each paravirtualized Linux VM you experience issues with the NTP and the hypervisor. Both try to synchronize the system clock. To avoid the clock becoming out of sync with other servers, ensure that the system clock within each Linux guest is synchronized with the NTP. This case 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**.

Step 3: Add the Linux VM to the Windows domain

The following methods are available for adding Linux machines to the Active Directory (AD) domain:

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Follow instructions based on your chosen method.

> **Note:**
>
> Session launches might fail when the same user name is used for the local account in the Linux VDA and the account in AD.

Samba Winbind

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Install or update the required packages

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

Enable the Winbind daemon to start on machine startup The Winbind daemon must be configured to start on machine startup:

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

> **Note:**
>
> Ensure that the `winbind` script is located under `/etc/init.d`.

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

> **Note:**
>
> Configure Kerberos based on your AD infrastructure. The following settings are meant for the single-domain, single-forest model.

```
[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** parameter 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**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure Winbind Authentication 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: systemd winbind
group: systemd winbind
```

Join Windows Domain Your domain controller must be reachable and you must have an Active Directory user account with permissions to add computers to the domain:

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Configure PAM for Winbind Run the following command and ensure that the **Winbind NT/Active Directory authentication** and **Create home directory on login** options are selected:

```
sudo pam-auth-update
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Tip:**
>
> The `winbind` daemon stays running only if the machine is joined to a domain.

Verify Domain Membership The Delivery Controller requires that all VDA machines, whether Windows or Linux, have a computer object in `Active Directory`.

Run the **net ads** command of **Samba** to verify that the machine is joined to a domain:

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

Run the following command to verify extra domain and computer object information:

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

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

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

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. 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
<!--NeedCopy-->
```

Examine the account details of the machine using:

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

Verify user authentication Use the **wbinfo** tool to verify that domain users can authenticate with the domain:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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 returns a message indicating success or failure.

To verify that the Winbind PAM module is configured correctly, log on to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\username

id -u
<!--NeedCopy-->
```

> **Note:**
>
> To run an SSH command successfully, ensure that SSH is enabled and working properly.

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

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

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

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

Exit the session.

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

A similar test can be performed by logging on to the Gnome or KDE console directly. Proceed to Step 6: Install the Linux VDA after the domain joining verification.

> **Tip:**
>
> If you succeed in user authentication but cannot show your desktop when logging on with a domain account, restart the machine and try again.

Quest authentication service

Configure Quest on domain controller Assume that 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`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enable domain users to log on to Linux VDA machines To enable domain users 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 the **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

Work around SELinux policy enforcement The default RHEL environment has SELinux fully enforced. This enforcement interferes with the Unix domain socket IPC mechanisms used by Quest, and prevents domain users from logging on.

The convenient way to work around this issue is to disable SELinux. As a root user, edit **/etc/selinux/config** and change the **SELinux** setting:

```
SELINUX=disabled
```

This change requires a machine restart:

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

> **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 Autorenewal of Kerberos tickets must be enabled and disconnected. Authentication (offline logon) must 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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

This command sets the renewal interval to nine hours (32,400 seconds) which is one 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 To enable domain user logon through HDX and other services such as su, ssh, and RDP, run the following commands to configure PAM and NSS manually:

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

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
<!--NeedCopy-->
```

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

If the machine is joined to a domain, this command returns the domain name. If the machine is not joined to any domain, the following error appears:

```
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 through PAM, log on to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\username

id -u
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verify that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

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

Verify that the tickets in the Kerberos credential cache are valid and not expired:

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

Exit the session.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

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
<!--NeedCopy-->
```

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

Verify 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
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
2
3 adinfo --diag
4 <!--NeedCopy-->
```

Test connectivity to the various Active Directory and Kerberos services.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

SSSD

Configure Kerberos Run the following command to install Kerberos:

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

To configure Kerberos, open **/etc/krb5.conf** as root and set the parameters:

> **Note:**
>
> Configure Kerberos based on your AD infrastructure. The following settings are meant for the single-domain, single-forest model.

```
[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 parameter 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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. You can use **adcli**, **realmd**, or **Samba** instead.

> **Note:**
>
> This section only provides information for **adcli** and **Samba**.

- **If you use adcli to join the domain, complete the following steps:**

1. Install **adcli**.

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

2. Join the 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
<!--NeedCopy-->
```

   The **user** is a domain user with permissions to add machines to the domain. The **hostname-fqdn** is the host name in FQDN format for the machine.

   The **-H** option is necessary for **adcli** to generate SPN in the format of host/hostname-fqdn@REALM, which the Linux VDA requires.

3. Verify system keytab.

   Run the `sudo klist -ket` command to ensure that the system keytab file has been created.

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

- **If you use Samba to join the domain, complete the following steps:**

1. Install the package.

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

2. Configure **Samba**.

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

   ```
   [global]

   workgroup = WORKGROUP
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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.

3. Join the domain with **Samba**.

   Your domain controller must be reachable and you must have a Windows account with permissions to add computers to the domain.

   ```
   sudo net ads join REALM -U user
   <!--NeedCopy-->
   ```

   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
<!--NeedCopy-->
```

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

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

> **Note:**
>
> By default, the install process in Ubuntu automatically configures **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 created manually. As root, either create or open **/etc/sssd/sssd.conf** and make the following settings:

```
[sssd]

services = nss, pam

config_file_version = 2
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
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, `Active Directory` must be able to provide POSIX extensions. PAM service `ctxhdx` is added to ad_gpo_map_remote_interactive.
>
> The **domain-dns-name** parameter 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.
>
> For information about the 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
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Start SSSD daemon Run the following commands to start the SSSD daemon now and to enable the daemon to start upon machine startup:

```
sudo systemctl start sssd

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

PAM configuration Run the following command and ensure that the **SSS authentication** and **Create home directory on login** options are selected:

```
sudo pam-auth-update
<!--NeedCopy-->
```

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in `Active Directory`.

- If you use **adcli** to verify domain membership, run the `sudo adcli info domain-dns-name` command to show the domain information.
- If you use **Samba** to verify domain membership, run the `sudo net ads testjoin` command to verify that the machine is joined to a domain and the `sudo net ads info` command to verify extra domain and computer object information.

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

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

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. 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 for the machine account has been cached using:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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 to the Linux VDA using a domain user account that has not been used before.

```
ssh localhost -l domain\\username

id -u

klist

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

Verify that the Kerberos tickets returned by the **klist** command are correct for that user and have not expired.

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

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

A similar test can be performed by logging on to KDE or Gnome Display Manager. Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

PBIS

Download the required PBIS package

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

Make the PBIS installation script executable

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

Run the PBIS installation script

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Join Windows domain Your domain controller must be reachable and you must have an Active Directory user account with permissions to add computers to the domain:

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

The **user** is a domain user who has permissions to add computers to the Active Directory domain. The **domain-name** is the DNS name of the domain, for example, example.com.

Note: To set Bash as the default shell, run the **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** command.

Verify domain membership The Delivery Controller requires that all VDA machines (Windows and Linux VDAs) have a computer object in `Active Directory`. To verify that a PBIS-joined Linux machine is on the domain:

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

If the machine is joined to a domain, this command returns the information about the currently joined AD domain and OU. Otherwise, only the host name appears.

Verify user authentication To verify that PBIS can authenticate domain users through PAM, log on to the Linux VDA using a domain user account that has not been used before.

```
sudo ssh localhost -l domain\\user

id -u
<!--NeedCopy-->
```

Verify that a corresponding Kerberos credential cache file was created for the UID returned by the **id -u** command:

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

Exit the session.

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

Proceed to Step 6: Install the Linux VDA after the domain-joining verification.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 4: Install .NET Runtime 6.0

Before installing the Linux VDA, install .NET Runtime 6.0 according to the instructions at https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

After installing .NET Runtime 6.0, run the **which dotnet** command to find your runtime path.

Based on the command output, set the .NET runtime binary path. For example, if the command output is /aa/bb/dotnet, use /aa/bb as the .NET binary path.

Step 5: Download the Linux VDA package

1. Go to the Citrix Virtual Apps and Desktops download page.
2. Expand the appropriate version of Citrix Virtual Apps and Desktops.
3. Click **Components** to download the Linux VDA package that matches your Linux distribution and the GPG public key that you can use to verify the integrity of the Linux VDA package.

   To verify the integrity of the Linux VDA package, import the public key into the DEB database and run the following commands:

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

### Step 6: Install the Linux VDA

#### Step 6a: Install the Linux VDA

Install the Linux VDA software using the Debian package manager:

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

Dependency list for Debian 11.3:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

ufw >= 0.36

desktop-base >= 10.0.2

libxrandr2 >= 2:1.5.1
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.
```

```
libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.33

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.6.0

sed >= 4.7

cups >= 2.2

ghostscript >= 9.53~

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.9 >= 3.9~

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

libqt5widgets5 >= 5.5~

mutter >= 3.38.6~

libqrencode4 >= 4.0.0

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

> **Note:**
>
> For a matrix of the Linux distributions and the Xorg versions that this version of the Linux VDA supports, see System requirements.

Step 6b: Upgrade the Linux VDA (optional)

You can upgrade an existing installation from the previous two versions and from an LTSR release.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Upgrading an existing installation overwrites the configuration files under /etc/xdl. Before you conduct an upgrade, make sure to back up the files.

Step 7: Install NVIDIA GRID drivers

Enabling HDX 3D Pro requires you to install the NVIDIA GRID drivers on your hypervisor and on the VDA machines.

To install and configure the NVIDIA GRID Virtual GPU Manager (the host driver) on the specific hypervisors, see the following guides:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

To install and configure the NVIDIA GRID guest VM drivers, perform the following general steps:

1. Ensure that the guest VM is shut down.
2. In the hypervisor control panel, allocate a GPU to the VM.
3. Start the VM.
4. Install the guest VM driver on the VM.

Step 8: Configure the Linux VDA

After installing the package, you must configure the Linux VDA by running the ctxsetup.sh script. Before making any changes, the script verifies the environment and ensures that all dependencies are installed. If necessary, you can rerun the script at any time to change settings.

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

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

Prompted configuration

Run a manual configuration with prompted questions:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Automated configuration

For an automated install, the options required by the setup script can be provided with environment variables. If all 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. Set to N by default.
- **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 through a TCP/IP port, which is port 80 by default.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –The Linux VDA services are started after machine startup. Set to Y by default.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –The Linux VDA services require incoming network connections to be allowed through the system firewall. You can open the required ports (ports 80 and 1494 by default) automatically in the system firewall for the Linux VDA. Set to Y by default.
- **CTX_XDL_AD_INTEGRATION=1 | 2 | 3 | 4 |5** –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
  - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO=Y | N** –The Linux VDA supports HDX 3D Pro, a set of GPU acceleration technologies designed to optimize the virtualization of rich graphics applications. If HDX 3D Pro is selected, the VDA is configured for VDI desktops (single-session) mode - (that is, 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 variable to Y. This variable is set to N by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_SITE_NAME=dns-name** –The Linux VDA discovers LDAP servers through DNS. To limit the DNS search results to a local site, specify a DNS site name. This variable is set to **<none>** by default.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –The Linux VDA queries DNS to discover LDAP servers. If DNS cannot provide LDAP service records, you can provide a space-separated list of LDAP FQDNs with LDAP ports. For example, ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268. If you specify the LDAP port number as 389, the Linux VDA queries each LDAP server in the specified domain in polling mode. If there are x number of policies and y number of LDAP servers, the Linux VDA performs the total of X multiplied by Y queries. If the polling time exceeds the threshold, session logons might fail. To enable the faster LDAP queries, enable **Global Catalog** on a domain controller and specify the relevant LDAP port number as 3268. This variable is set to **<none>** by default.
- **CTX_XDL_SEARCH_BASE=search-base-set** –The Linux VDA queries LDAP through a search base set to the root of the Active Directory Domain (for example, DC=mycompany,DC=com). However, to improve search performance, you can specify a search base (for example, OU=VDI,DC=mycompany,DC=com). This variable is set to **<none>** by default.
- **CTX_XDL_FAS_LIST='list-fas-servers'**–The Federated Authentication Service (FAS) servers are configured through AD Group Policy. The Linux VDA does not support AD Group Policy, but you can provide a semicolon-separated list of FAS servers instead. The sequence must be the same as configured in AD Group Policy. If any server address is removed, fill its blank with the **<none>** text string and do not modify the order of server addresses. To communicate with FAS servers properly, make sure you append a port number consistent with that specified on the FAS servers, for example, CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** –The path to install .NET Runtime 6.0 for supporting the new broker agent service (`ctxvda`). The default path is /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** –Specifies the GNOME, GNOME Classic, or MATE desktop environment to use in sessions. If you leave the variable unspecified, the desktop currently installed on the VDA is used. However, if the currently installed desktop is MATE, you must set the variable value to **mate**.

  You can also change the desktop environment for a target session user by completing the following steps:

  1. Create an `.xsession` file under the **$HOME/<username>** directory on the VDA.
  2. Edit the `.xsession` file to specify a desktop environment based on distributions.
     - **For MATE desktop**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

- **For GNOME Classic desktop**

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

- **For GNOME desktop**

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

3. Share the 700 file permission with the target session user.

Starting with Version 2209, session users can customize their desktop environments. To enable this feature, you must install switchable desktop environments on the VDA in advance. For more information, see Custom desktop environments by session users.

- **CTX_XDL_START_SERVICE=Y | N** –Whether or not the Linux VDA services are started when the Linux VDA configuration is complete. Set to Y by default.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** –The socket port for listening for Citrix Scout. The default port is 7503.
- **CTX_XDL_TELEMETRY_PORT** –The port for communicating with Citrix Scout. The default port is 7502.

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|5

export CTX_XDL_HDX_3D_PRO=Y|N

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
export CTX_XDL_VDI_MODE=Y|N

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

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

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

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

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

When running the sudo command, type the **-E** option to pass the existing environment variables to the new shell it creates. We recommend that you create a shell script file from the preceding commands with **#!/bin/bash** as the first line.

Alternatively, you can specify all parameters by using 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|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

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:

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

To remove configuration changes:

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

> **Important:**
>
> This script deletes all configuration data from the database and renders 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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To view more detailed information:

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

To uninstall the Linux VDA software:

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

> **Note:**
>
> Uninstalling the Linux VDA software deletes the associated PostgreSQL and other configuration data. However, the PostgreSQL package and other dependent packages that were set up before the installation of the Linux VDA are not deleted.
>
> **Tip:**
>
> The information in this section does not cover the removal of dependent packages including PostgreSQL.

Step 9: Run XDPing

Run `sudo /opt/Citrix/VDA/bin/xdping` to check for common configuration issues with a Linux VDA environment. For more information, see XDPing.

Step 10: Run the Linux VDA

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
<!--NeedCopy-->
```

Stop the Linux VDA:

To stop the Linux VDA services:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Before you stop the `ctxvda` and `ctxhdx` services, run the `service ctxmonitorservice stop` command to stop the monitor service daemon. Otherwise, the monitor service daemon restarts the services you stopped.

Restart the Linux VDA:

To restart the Linux VDA services:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

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

Check the Linux VDA status:

To check the running status of the Linux VDA services:

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```

Step 11: Create machine catalogs

The process for creating machine catalogs and adding Linux VDA machines is 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:
  - The **Multi-session OS** option for a hosted shared desktops delivery model.
  - The **Single-session OS** option for a VDI dedicated desktop delivery model.
- 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 single user per machine delivery model.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Tip:**
>
> If you remove and rejoin a machine to the Active Directory domain, you must remove and add the machine to the machine catalog again.

Step 12: Create delivery groups

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:

- Ensure that the AD users and groups that 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.

For information about how to create machine catalogs and delivery groups, see Citrix Virtual Apps and Desktops 7 2212.

Configure

January 23, 2023

This section details the features of the Linux VDA, including feature description, configuration, and troubleshooting.

Administration

January 23, 2023

This section contains the following topics:

- CEIP
- HDX Insight
- Integration with the Citrix Telemetry Service

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Linux VDA self-update for Citrix DaaS Standard for Azure
- Linux VM and Linux session metrics
- Log collection
- Session shadowing
- The monitor service daemon
- Tools and utilities
- Others
  - Citrix Workspace app for HTML5 support
  - Create a Python3 virtual environment
  - Integrate NIS with Active Directory
  - IPv6
  - LDAPS
  - **Xauthority**

Citrix Customer Experience Improvement Program (CEIP)

January 23, 2023

When you participate in the CEIP, anonymous statistics and usage information are sent to Citrix to help improve the quality and performance of Citrix products. In addition, a copy of the anonymous data is sent to Google Analytics (GA) for fast and efficient analysis. GA is disabled by default.

Registry settings

By default, you automatically participate in the CEIP when you install the Linux VDA. The first upload of data occurs approximately seven days after you install the Linux VDA. You can change this default setting in the registry.

- **CEIPSwitch**

Registry setting that enables or disables the CEIP (default = 0):

Location: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: **CEIPSwitch**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Value: 1 = disabled, 0 = enabled

When unspecified, the CEIP is enabled.

You can run the following command on a client to disable the CEIP:

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

- **GASwitch**

Registry setting that enables or disables GA (default = 1):

Location: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: **GASwitch**

Value: 1 = disabled, 0 = enabled

When unspecified, GA is disabled.

You can run the following command on a client to enable GA:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\CEIP" -v "GASwitch" -d "0"
<!--NeedCopy-->
```

- **DataPersistPath**

Registry setting that controls the data persisting path (default = /var/xdl/ceip):

Location: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: DataPersistPath

Value: String

You can run the following command to set this path:

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

If the configured path does not exist or cannot be accessed, data is saved in the default path.

CEIP data collected from the Linux VDA

The following table gives an example of the types of anonymous information collected. The data does not contain any details that identify you as a customer.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Data Point	Key Name	Description
Machine GUID	**machine_guid**	Identifying the machine where the data originates
AD solution	**ad_solution**	Text string denoting the machine's domain-joining method
Linux kernel version	**kernel_version**	Text string denoting the machine's kernel version
LVDA version	**vda_version**	Text string denoting the installed version of the Linux VDA.
LVDA update or fresh install	**update_or_fresh_install**	Text string denoting the current Linux VDA package is being freshly installed or updated
LVDA installed method	install_method	Text string denoting that the current Linux VDA package is installed by using MCS, PVS, easy install, or manual installation.
HDX 3D Pro enabled or not	**hdx_3d_pro**	Text string denoting whether HDX 3D Pro is enabled on the machine
VDI mode enabled or not	**vdi_mode**	Text string denoting whether VDI mode is enabled
System Locale	**system_locale**	Text string denoting the locale of this machine
LVDA key services last restart time	**ctxhdx ctxvda**	The last restart time of the `ctxhdx` and `ctxvda` services, in the format of dd-hh:mm:ss, for example, 10-17:22:19
GPU type	**gpu_type**	Denoting the GPU type of the machine
CPU cores	**cpu_cores**	Integer denoting the number of CPU cores of the machine
CPU frequency	**cpu_frequency**	Float denoting the CPU frequency in MHz
Physical memory size	**memory_size**	Integer denoting the physical memory size in KB

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Data Point	Key Name	Description
Launched session number	**session_launch**	Integer denoting the number of sessions launched (logged on or reconnected) on the machine at the time we collect this data point
Linux OS name and version	**os_name_version**	Text string denoting the Linux OS name and version of the machine
Session key	**session_key**	Identifying the session where the data originates
Resource type	**resource_type**	Text string denoting the resource type of the launched session: desktop or <appname>
Active session time	**active_session_time**	Used to save the session's active times. One session can have multiple active times because the session can disconnect/reconnect
Session duration time	**session_duration_time**	Used to save the session's duration from logon to logoff
Receiver client type	**receiver_type**	Integer denoting the type of Citrix Workspace app used to launch the session
Receiver client version	**receiver_version**	Text string denoting the version of Citrix Workspace app used to launch the session
Printing count	**printing_count**	Integer denoting the number of times the session uses the printing function
USB redirection count	**usb_redirecting_count**	Integer denoting the number of times the session uses a USB device
Gfx provider type	**gfx_provider_type**	Text string denoting the graphics provider type of the session

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Data Point	Key Name	Description
Shadowing count	**shadow_count**	Integer denoting the number of times the session has been shadowed
User selected Language	**ctxism_select**	Composed long string that contains all languages that users have selected
Smartcard redirecting count	**scard_redirecting_count**	Integer denoting the number of times smart card redirection is used for session logons and user authentication for in-session apps

HDX Insight

January 23, 2023

Overview

The Linux VDA partially supports the HDX Insight feature.

Installation

No dependent packages need installation.

Usage

HDX Insight analyzes the ICA messages passed through the Citrix ADC between Citrix Workspace app and the Linux VDA. All HDX Insight data is sourced from the NSAP virtual channel and sent uncompressed. The NSAP virtual channel is enabled by default.

The following commands disable and enable the NSAP virtual channel, respectively:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000000"
     --force
2 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"
    --force
<!--NeedCopy-->
```

Troubleshooting

No data points are displayed

There might be two causes:

- HDX Insight is not configured correctly.

  For example, AppFlow is not enabled on the Citrix ADC or an incorrect Citrix ADC instance is configured on the Citrix ADM.

- The ICA Control Virtual Channel is not started on the Linux VDA.

  ```
  ps aux | grep -i ctxctl
  ```

  If `ctxctl` is not running, contact your administrator to report a bug to Citrix.

No application data points are displayed

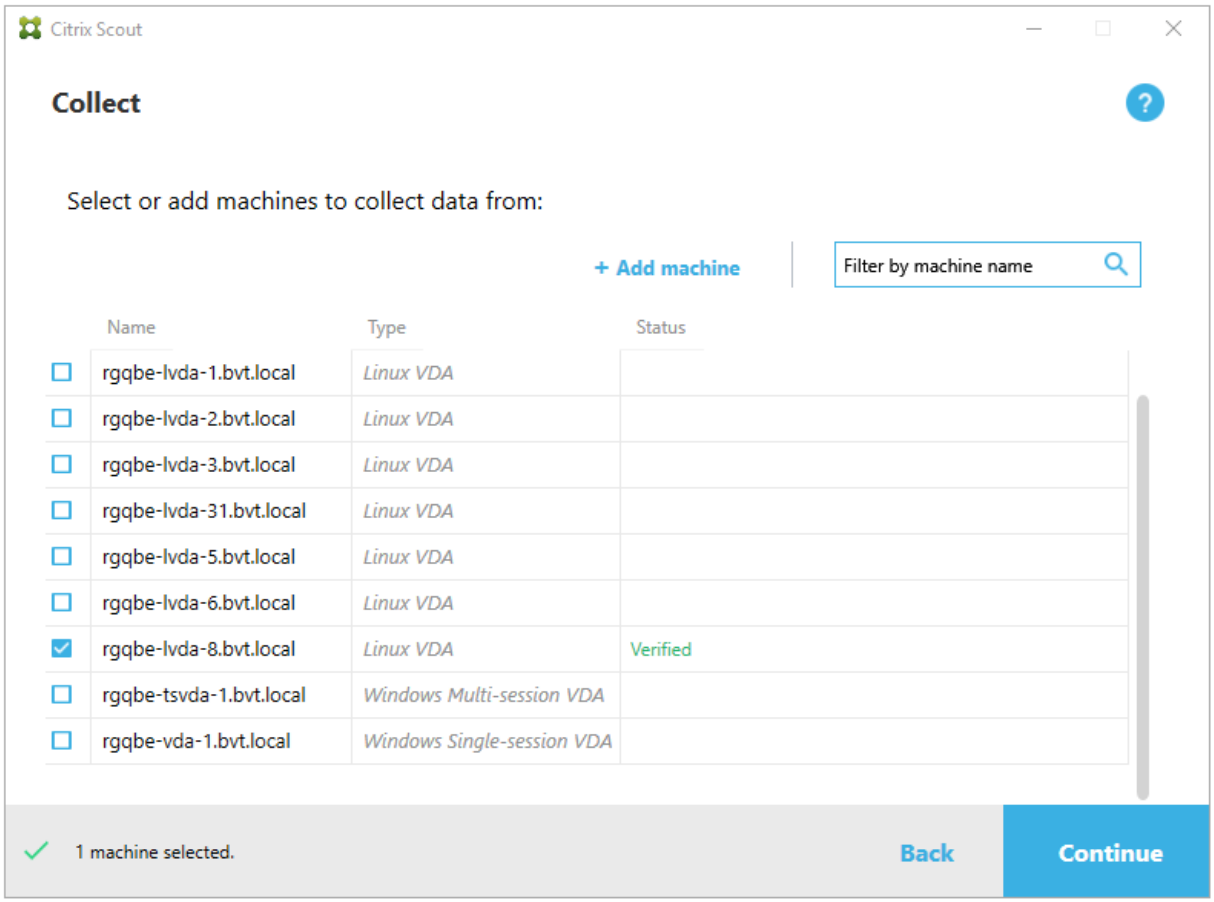
Verify that the seamless virtual channel is enabled and a seamless application is running.

Integration with the Citrix Telemetry Service

February 1, 2023

With the Citrix Telemetry Service (`ctxtelemetry`) integrated with the Linux VDA software, you can run Citrix Scout, which then uses the /opt/Citrix/VDA/bin/xdlcollect.sh script, to collect logs about the Linux VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Note:**
>
> After upgrading from Linux VDA 1912 and earlier versions, you must rerun /opt/Citrix/VDA/sbin/ctxsetup.sh to configure the variables for the Citrix Telemetry Service (`ctxtelemetry`). For more information about the variables, see Create domain-joined VDAs using easy install.

Enable and disable the Citrix Telemetry Service

- To enable the service, run the **sudo systemctl enable ctxtelemetry.socket** command.
- To disable the service, run **sudo systemctl disable ctxtelemetry.socket**.

Ports

The Citrix Telemetry Service (`ctxtelemetry`), by default, uses TCP/IP port 7503 to listen for Citrix Scout. It uses TCP/IP port 7502 on the Delivery Controller to communicate with Citrix Scout.

You can use the default ports or change ports through the following variables when you install the Linux VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** –The socket port for listening for Citrix Scout. The default port is 7503.
- **CTX_XDL_TELEMETRY_PORT** –The port for communicating with Citrix Scout. The default port is 7502.

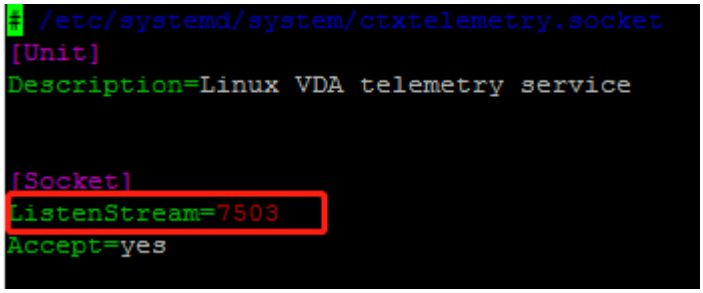
To change ports after you have your VDA installed, do the following:

1. To change a port for communicating with Scout, run the following command.

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number>
    -t REG_DWORD
<!--NeedCopy-->
```

2. To change the socket port for listening for Scout, run the following command to open and edit the ctxtelemetry.socket file.

```
sudo vi /etc/systemd/system/ctxtelemetry.socket
<!--NeedCopy-->
```



3. Run the following commands to restart the socket port.

```
sudo systemctl daemon-reload
sudo systemctl stop ctxtelemetry.socket
sudo systemctl start ctxtelemetry.socket
<!--NeedCopy-->
```

4. Enable the new ports in your firewall configuration.

   If you are using Ubuntu, for example, run the **sudo ufw allow 7503** command to enable port 7503.

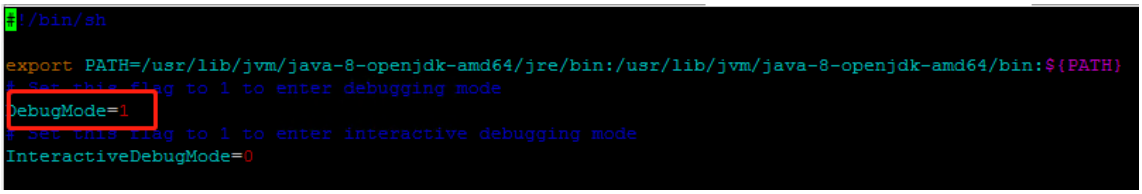
Debug mode

If the Citrix Telemetry Service does not work as expected, you can enable debug mode to determine the causes.

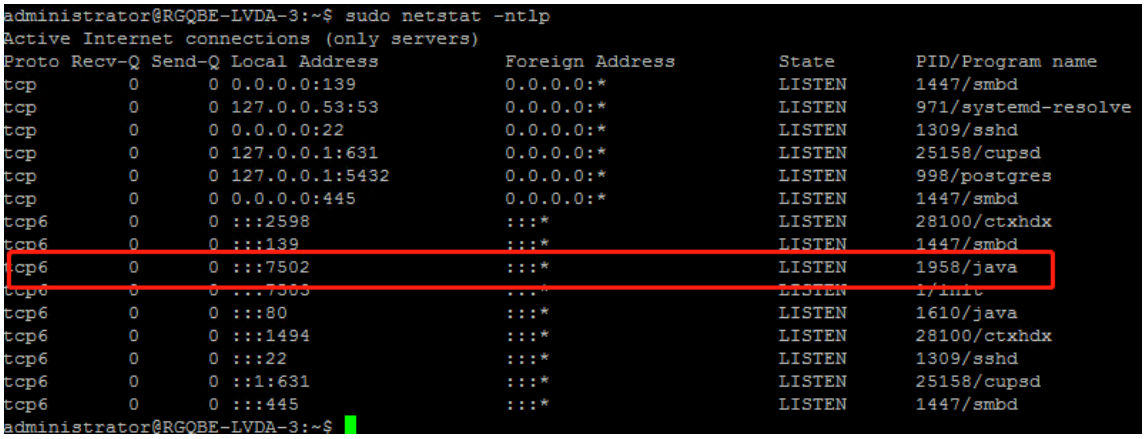
1. To enable debug mode, run the following command to open the `ctxtelemetry` file and then change the DebugMode value to 1.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
<!--NeedCopy-->
```



2. Manually stop the Citrix Telemetry Service, or wait 15 minutes for the service to stop automatically.



   In this example, you can run the following commands to stop the Citrix Telemetry Service.

```
sudo netstat -ntlp
Kill -9 1958
<!--NeedCopy-->
```

3. To restart the Citrix Telemetry Service, select your Linux VDA on Scout and find telemetry-debug.log in /var/log/xdl/.

Service wait time

The `systemd` daemon that opens the socket port starts by default and uses few resources. The Citrix Telemetry Service stops by default and starts only when there is a log collection request from the Delivery Controller. After log collection completes, the service awaits new collection requests for a duration of 15 minutes and stops again if there are not any. You can configure the wait time through the following command. The minimum value is 10 minutes. If you set a value less than 10 minutes, the minimum value, 10 minutes, takes effect. After setting the wait time, stop and restart the service.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -v "TelemetryServiceIdleTimeoutInMinutes" -d <
   number> -t REG_DWORD
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Verification tests

Before a collection starts, verification tests run automatically for each selected machine. These tests ensure that the requirements are met. If a test fails for a machine, Scout displays a message, with suggested corrective actions. For more information about verification tests, see the Verification tests section in the Citrix Scout documentation.

Linux VDA self-update for Citrix DaaS Standard for Azure

November 2, 2023

This feature helps to automatically update your Linux VDA software - immediately, or at a scheduled time. It is beneficial when you create Linux VDAs in Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure). You have no administrator privileges of the VMs in Azure. For more information, see Create Linux VDAs in Citrix DaaS Standard for Azure.

Configuration

To use this feature, complete the following steps:

Step 1: Upload update information and new VDA packages to your Azure container

Step 1a: Create a container under your Azure storage account and set your container access level to **Blob (Anonymous read access for blobs only)**.

> **Note:**
>
> Azure containers and blobs are exclusively held and managed by customers. Citrix is not liable for any security issues with them. To ensure data security and cost efficiency, set your container access level to **Private (no anonymous access)** after each **self-update**.

Step1b: Incorporate your VDA update information to a JSON file named UpdateInfo.json. For an example of the file format, see the following block:

```
{

 "Version": "21.04.200.4",
"Distributions":[
{

"TargetOS": "RHEL7_9",
"PackageName": "",
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
"PackageHash": ""
 }
 ,
{

"TargetOS": "UBUNTU18_04",
"PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",
"PackageHash": "4148
   cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"
 }
 ,
{

"TargetOS": "UBUNTU20_04",
"PackageName": "",
"PackageHash": ""
 }

]
 }

<!--NeedCopy-->
```

Where, **"Version"** indicates the new VDA version and **"Distributions"** is an array of update objects. Each object contains three items:

- **"TargetOS"**: must be "RHEL7_9"(for RHEL 7, CentOS 7, and Amazon Linux 2), "UBUNTU18_04" , or "UBUNTU20_04."The `ctxmonitorservice` does not recognize any other distributions.
- **"PackageName"**: Full name of the VDA package of the specified version.
- **"PackageHash"**: SHA-256 value that you compute by using the `shasum -a 256 <pkgname>` command.

Step1c: Upload the JSON file and the new version of Linux VDA packages to your Azure container.

Step 2: Enable the self-update feature on the master image or on each VDA

By default, **self-update** is disabled. If you create Linux VDAs in Citrix DaaS Standard for Azure, the feature enablement must be conducted on the master image. Otherwise, enable the feature on each target VDA directly.

To enable **self-update**, run commands similar to the following to edit the registry key at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SelfUpdate.

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

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
    Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "
    Immediately" --force

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

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

The following table describes the registry settings.

Registry setting	Description
fEnabled	This setting is required. By default, the value is 0, which means **self-update** is disabled. You can set it to 1 to enable **self-update**.
Url	This setting is required. It sets the URL of your Azure container to get the update information and new VDA packages.
ScheduledTime	This setting is required. You can set it to **Immediately** or **NextStart**. **Immediately** means to run an update immediately after downloading VDA packages. This option is appropriate when the download speed is high and your update is urgent. But it can disrupt the user experience if there are any live sessions when you download the package. **NextStart** means to run an update upon the next start of the `ctxmonitorservice`. This option is appropriate when the download speed is not high and your update is not urgent.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registry setting	Description
CaCertificate	This setting is optional. It sets the full path of a PEM certificate to verify the URL of your Azure container. For Azure blobs, it can be the certificate of portal.azure.com that is retrieved from the browser and then converted to PEM. For security, we recommend you add this registry setting, but it is supported only on Ubuntu. On RHEL, it misses linking some NSS libraries for the `curl` command. Make sure to set the least privileges of the certificate.

When the `ctxmonitorservice` restarts, it first queries **Url** to get the UpdateInfo.json file and retrieves the update version from the JSON file. Then the `ctxmonitorservice` compares the update version with the current version. If the current version is earlier, the service downloads the new version of the VDA package from Azure and saves it locally. After that, it runs an update according to the setting of **ScheduledTime**. For an on-premises deployment, you can restart the `ctxmonitorservice` directly to trigger the update. However, in Citrix DaaS Standard for Azure where you have no administrator privileges to the VMs, the `ctxmonitorservice` can be restarted only after the VDA machine is restarted. If an update fails, your VDA is rolled back to the existing version.

> **Note:**
>
> - The registry settings you configured on the master image cannot be changed.
> - If all VMs in an environment download a package at the same time, the local network can be congested.
> - User data is lost if both an update and rollback fail.
> - If an update fails but rollback succeeds, users on the same network might have different versions of the Linux VDA. This case is suboptimal.
> - An update typically takes several minutes to complete. There is no status indicator in Citrix Studio.

Linux VM and Linux session metrics

January 23, 2023

The following table lists some metrics that are available for Linux VMs and Linux sessions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metric	Min. VDA Version Required	Description	Remarks
Logon duration	2109	It is a measure of the logon process from the time a user connects from Citrix Workspace app to the time when a session is ready to use. To view the metric of a session, go to the Monitor tab of Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Monitor is available as the Director console to monitor and troubleshoot Citrix Virtual Apps and Desktops Current Release and LTSR deployments. On the Monitor tab, click **View Historical Trend** in the **Average Logon Duration** section. On the **Logon Performance** page, set filter conditions and click **Apply** to visualize metrics.	Available only in Monitor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Metric	Min. VDA Version Required	Description	Remarks
Session auto reconnect count	2109	To view the number of auto reconnects in a session, access the **Trends** view. Set conditions and click **Apply** to narrow search results. The **Session Auto Reconnect Count** column displays the number of auto reconnects in a session. Auto reconnect is enabled when the **Session Reliability** or the **Auto Client Reconnect** policies are in effect. For more information about session reconnections, see Sessions. For more information about policies, see Auto client reconnect policy settings and Session reliability policy settings	Available both in Citrix Director and in Monitor.
Idle time	2103	To access this metric, open the **All Sessions** page by selecting **Filters > Sessions > All Sessions**.	Available both in Citrix Director and in Monitor.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

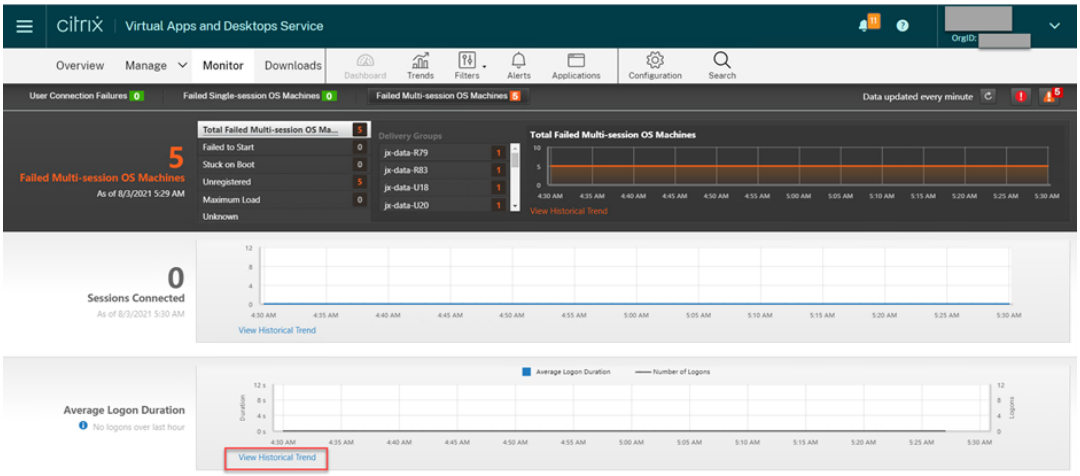
Metric	Min. VDA Version Required	Description	Remarks
Metrics of a Linux VM	2103	The following metrics for Linux VMs are available: the number of CPU cores, memory size, hard disk capacity, and current and historical CPU and memory utilization	Available both in Citrix Director and in Monitor.
Protocol	1909	The transport protocol of a Linux session appears as UDP or TCP in the **Session Details** panel.	Available both in Citrix Director and in Monitor.
ICA RTT	1903	ICA Round Trip Time (RTT) is the elapsed time from when you press a key until the response appears on the endpoint. To obtain ICA RTT metrics, create the **ICA round trip calculation** and **ICA round trip calculation interval** policies in Citrix Studio.	Available both in Citrix Director and in Monitor.

Examples of how to access the various metrics in Citrix Director and Monitor

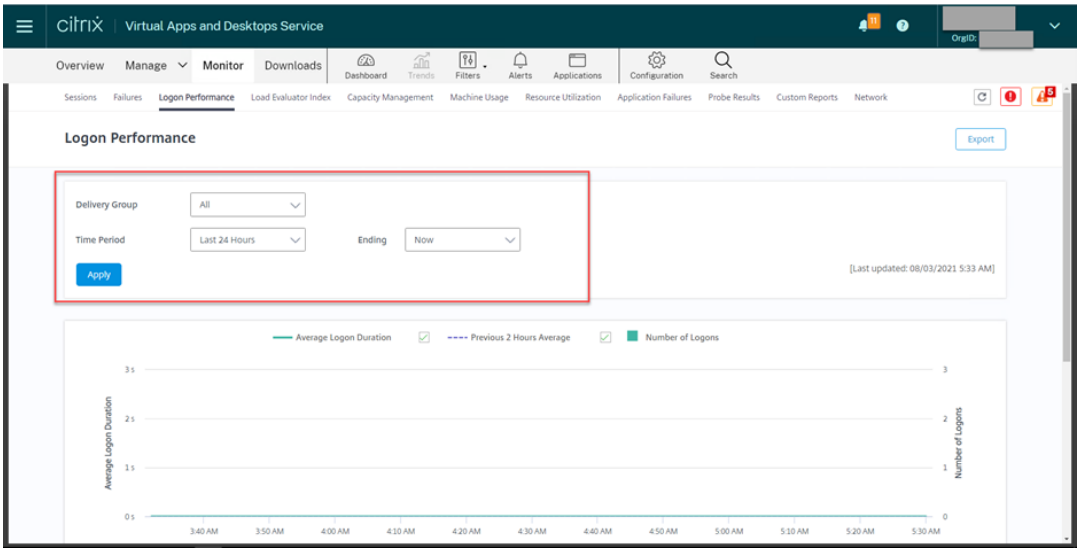
- Logon duration

  1. On the Monitor tab of Citrix DaaS, click **View Historical Trend** in the **Average Logon Duration** section.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

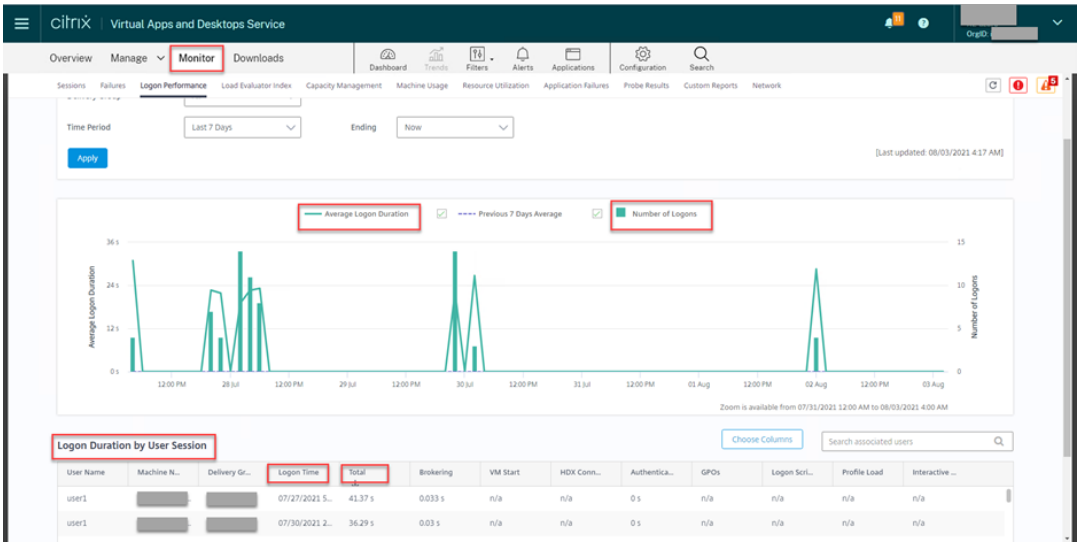


2. On the **Logon Performance** page, set filter conditions.



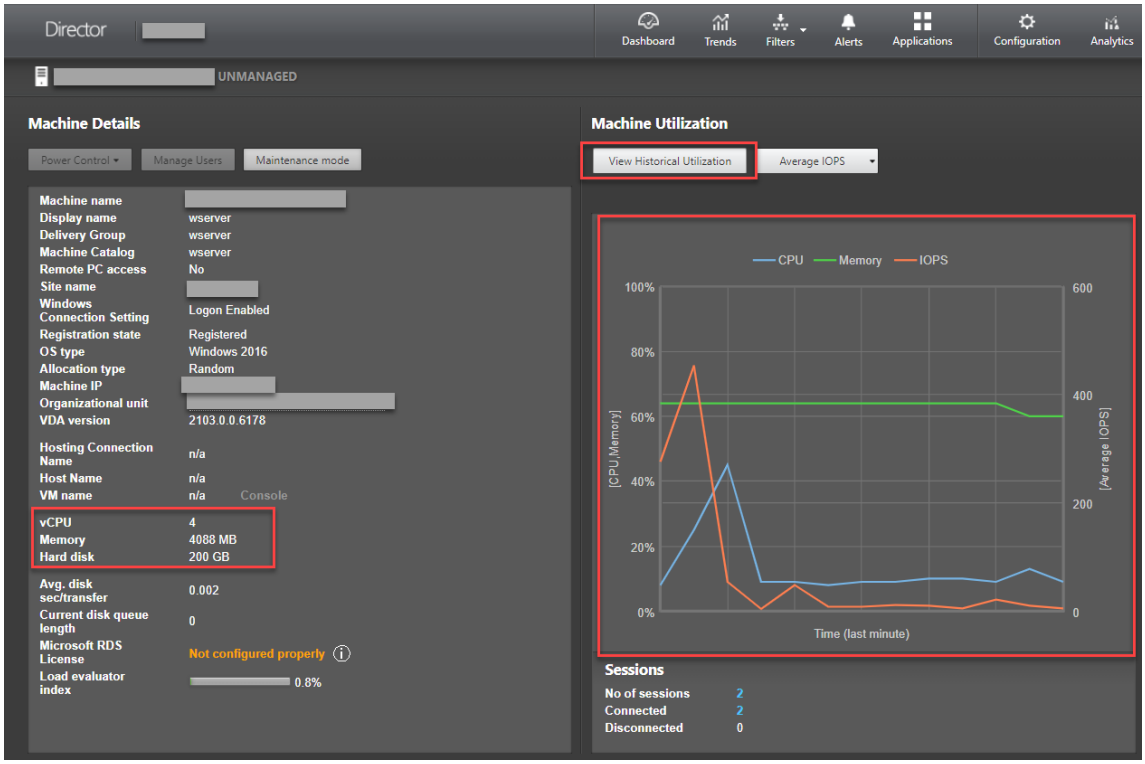
3. Click **Apply** to visualize the logon duration metrics.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

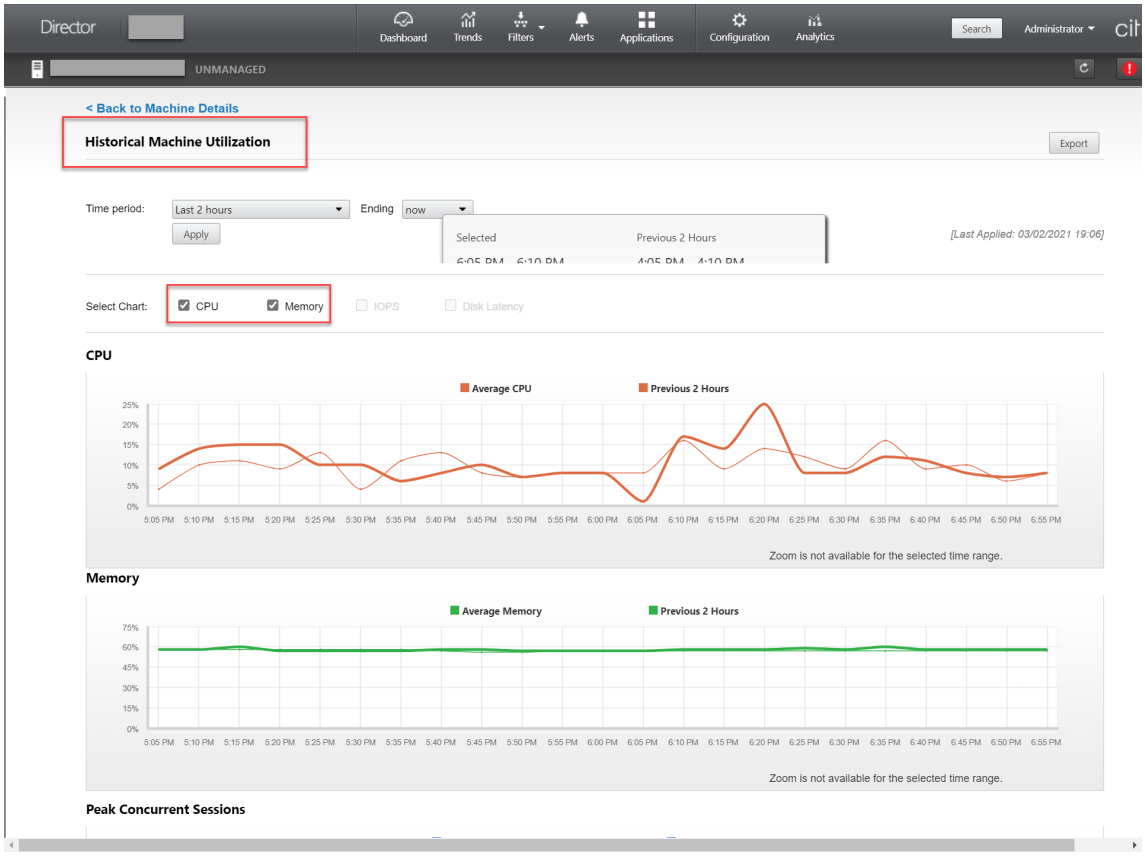


- The number of CPU cores, memory size, hard disk capacity, and current and historical CPU and memory utilization of a Linux VM

  To access these metrics of a Linux VM, find the VM in Citrix Director or Monitor and check the **Machine Detail**s panel. For example:

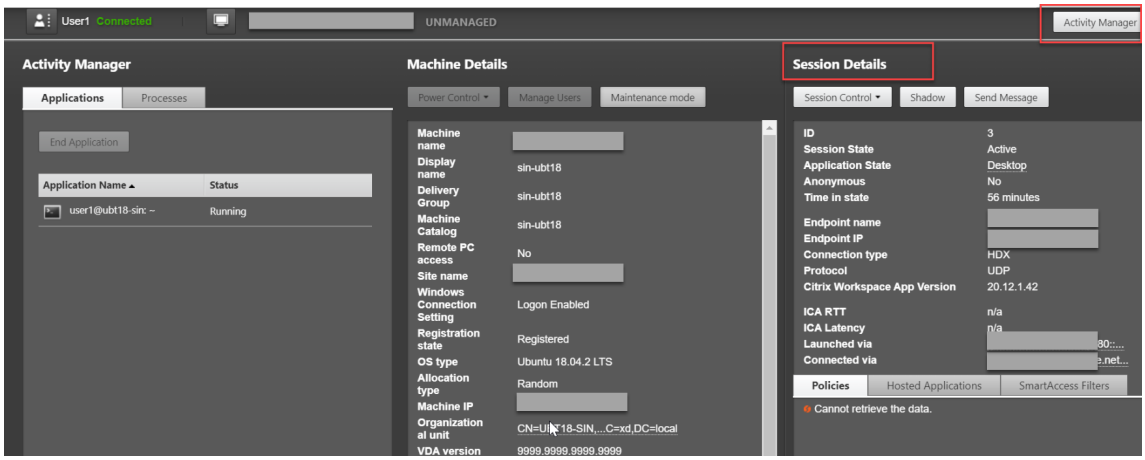


© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- ICA RTT, Protocol

  To view the metrics of a Linux session, open the **All Sessions** page by selecting **Filters > Sessions > All Sessions**, or access the **Session Details** panel. To access the **Session Details** panel, open the **All Sessions** page and click a target session to access its **Activity Manager** view. For example:



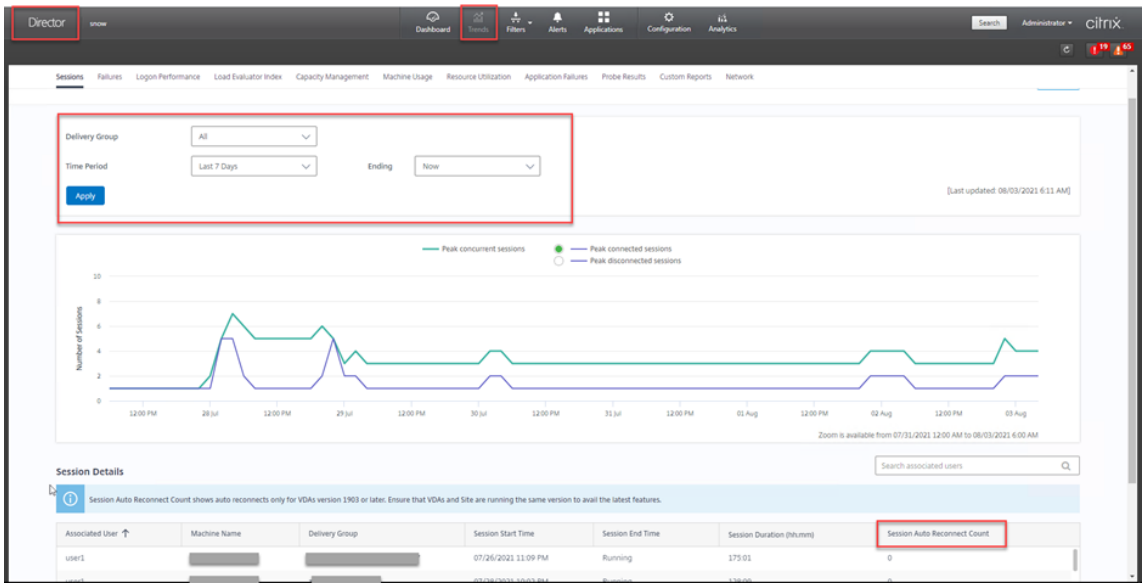
- Session auto reconnect count

  To view the number of auto reconnects in a session, access the **Trends** view. Set conditions and

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

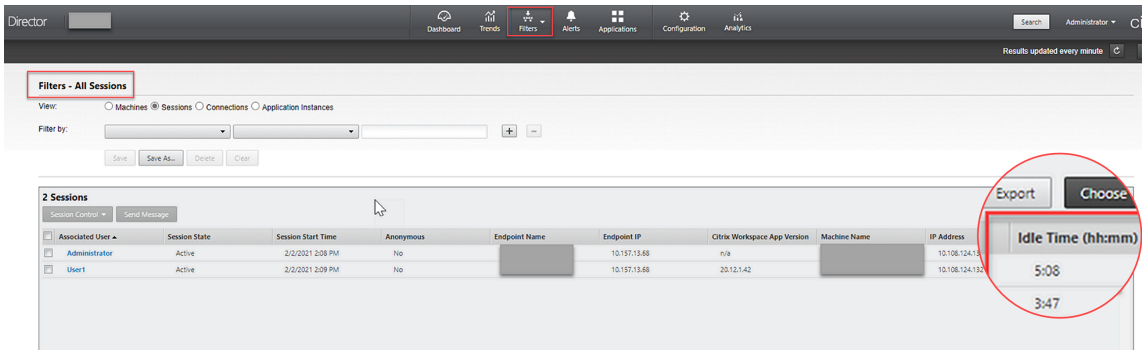
click **Apply** to narrow search results.

The **Session Auto Reconnect Count** column displays the number of auto reconnects in a session. For example:



- Idle time

  For example:



Log collection

January 23, 2023

Overview

Log collection is enabled for the Linux VDA by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration

The `ctxlogd` daemon and the `setlog` utility are included in the Linux VDA release package. By default, the `ctxlogd` daemon starts after you install and configure the Linux VDA.

The ctxlogd daemon

All the other services that are traced depend on the `ctxlogd` daemon. You can stop the `ctxlogd` daemon if you do not want to keep the Linux VDA traced.

The setlog utility

Log collection is configured using the `setlog` utility, which is under the **/opt/Citrix/VDA/bin/** path. Only the root user has the privilege to run it. You can use the GUI or run commands to view and change the configurations. Run the following command for help with the `setlog` utility:

```
setlog help
<!--NeedCopy-->
```

Values By default, **Log Output Path** is set to **/var/log/xdl/hdx.log**, **Max Log Size** is set to 200 MB, and you can save up to two old log files under **Log Output Path**.

View the current `setlog` values:

```
setlog values

log_path (Log Output Path) = /var/log/xdl/hdx.log

log_size (Max Log Size (MiB)) = 200

log_count (Max Old Log Files) = 2
<!--NeedCopy-->
```

View or set a single `setlog` value:

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

For example:

```
setlog value log_size 100
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Levels By default, log levels are set to **warning** (case-insensitive).

To view log levels set for different components, run the following command:

```
setlog levels
<!--NeedCopy-->
```

To set log levels (including Disabled, Inherited, Verbose, Information, Warnings, Errors, and Fatal Errors), run the following command:

```
setlog level <class> [<level>]
<!--NeedCopy-->
```

Log Level	Command Parameter (Case-Insensitive)
Disabled	none
Inherited	inherit
Verbose	verbose
Information	info
Warnings	warning
Errors	error
Fatal Errors	fatal

The **<class>** variable specifies one component of the Linux VDA. To cover all components, set it to all. For example:

```
setlog level all error
<!--NeedCopy-->
```

Flags By default, the flags are set as follows:

```
setlog flags

DATE = true

TIME = true

NAME = true

PID = true

TID = false

SID = true
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
14
15 UID = false
16
17 GID = false
18
19 CLASS = false
20
21 LEVEL = false
22
23 FUNC = true
24
25 FILE = false
26 <!--NeedCopy-->
```

View the current flags:

```
1 setlog flags
2 <!--NeedCopy-->
```

View or set a single log flag:

```
1 setlog flag <flag> [<state>]
2 <!--NeedCopy-->
```

Restore Defaults Revert all levels, flags, and values to the default settings:

```
1 setlog default
2 <!--NeedCopy-->
```

> **Important:**
>
> The `ctxlogd` service is configured using the **/var/xdl/.ctxlog** file, which only root users can create. Other users do not have write permission to this file. We recommend that root users not give write permission to other users. Failure to comply can cause the arbitrary or malicious configuration to `ctxlogd`, which can affect server performance and therefore the user experience.

Troubleshooting

The `ctxlogd` daemon fails and you cannot restart the `ctxlogd` service when the **/var/xdl/.ctxlog** file is missing (for example, accidentally deleted).

/var/log/messages:

```
1 Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
     configuration file.
2
3 Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
     =exited, status=1/FAILURE
4
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
<!--NeedCopy-->
```

To solve this issue, run `setlog` as a root user to recreate the **/var/xdl/.ctxlog** file. Then restart the `ctxlogd` service on which other services depend.

Session shadowing

March 11, 2024

Shadowing sessions allows domain administrators to view users' ICA sessions in an intranet. The feature uses noVNC to connect to the ICA sessions.

> **Note:**
>
> To use the feature, use `Citrix Director` 7.16 or later.

Installation and configuration

Dependencies

Two new dependencies, `python-websockify` and `x11vnc`, are required for session shadowing. Install `python-websockify` and `x11vnc` manually after you install the Linux VDA.

For RHEL 7.x and Amazon Linux2:

Run the following commands to install `python-websockify` and `x11vnc` (`x11vnc` version 0.9.13 or later):

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

(For RHEL 7.x) Resolve `python-websockify` and `x11vnc` by enabling the Extra Packages for Enterprise Linux (EPEL) and optional RPMs repositories:

- EPEL

  The EPEL repository is required for `x11vnc`. Run the following command to enable the EPEL repository:

  ```
  yum install https://dl.fedoraproject.org/pub/epel/epel-release-
     latest-7.noarch.rpm
  <!--NeedCopy-->
  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Optional RPMs

  Run the following command to enable the optional RPMs repository for installing some dependency packages of x11vnc:

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

For RHEL 8.x/9.0 and Rocky Linux 8.6/9.0:

Run the following commands to install python-websockify and x11vnc (x11vnc version 0.9.13 or later).

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

Resolve x11vnc by enabling the EPEL and CodeReady Linux Builder repositories:

```
dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-
   release-latest-8.noarch.rpm

subscription-manager repos --enable "codeready-builder  -for-rhel-8-
   x86_64-rpms"
<!--NeedCopy-->
```

For Ubuntu:

Run the following commands to install python-websockify and x11vnc (x11vnc version 0.9.13 or later):

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--NeedCopy-->
```

For SUSE:

Run the following commands to install python-websockify and x11vnc (x11vnc version 0.9.13 or later):

```
sudo pip3 install websockify
sudo zypper install x11vnc
<!--NeedCopy-->
```

For Debian:

Run the following commands to install python-websockify and x11vnc (x11vnc version 0.9.13 or later):

```
sudo pip3 install websockify
sudo apt-get install x11vnc
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Port

The session shadowing feature automatically selects available ports from within 6001-6099 to build up connections from the Linux VDA to `Citrix Director`. Therefore, the number of ICA sessions that you can shadow concurrently is limited to 99. Ensure that enough ports are available to meet your requirements, especially for multi-session shadowing.

Registry

The following table lists related registries:

Registry	Description	Default Value
EnableSessionShadowing	Enables or disables the session-shadowing feature	1 (Enabled)
ShadowingUseSSL	Determines whether to encrypt the connection between the Linux VDA and Citrix Director	0 (Disabled)

Run the `ctxreg` command on the Linux VDA to change the registry values. For example, to disable session shadowing, run the following command:

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

SSL

The noVNC connection between the Linux VDA and Citrix Director uses the WebSocket protocol. For session shadowing, whether `ws://` or `wss://` is chosen depends on the previously mentioned "ShadowingUseSSL"registry. By default, `ws://` is chosen. However, for security reasons, we recommend that you use `wss://` and install certificates on each Citrix Director client and on each Linux VDA server. Citrix disclaims any security responsibility for the Linux VDA session shadowing by using `ws://`.

Obtain server and root SSL certificates Certificates must be signed by a trusted Certificate Authority (CA).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

A separate server certificate (including the key) is required for each Linux VDA server on which you want to configure SSL. A server certificate identifies a specific computer, so you must know the Fully Qualified Domain Name (FQDN) of each server. You can use a wildcard certificate for the whole domain instead. In this case, you must know at least the domain name.

A root certificate is also required for each Citrix Director client that communicates with the Linux VDA. Root certificates are available from the same CAs that issue the server certificates.

You can install server and client certificates from the following CAs:

- A CA that is bundled with your operating system
- An enterprise CA (a CA that your organization makes accessible to you)
- A CA not bundled with your operating system

Consult the security team of your organization to find out which of the methods they require for getting certificates.

Important:

- The Common Name for a server certificate must be the exact FQDN of the Linux VDA or at least the correct wildcard plus domain characters. For example, vda1.basedomain.com or *.basedomain.com.
- Hashing algorithms including the SHA1 and MD5 are too weak for signatures in digital certificates for some browsers to support. So SHA-256 is specified as the minimum standard.

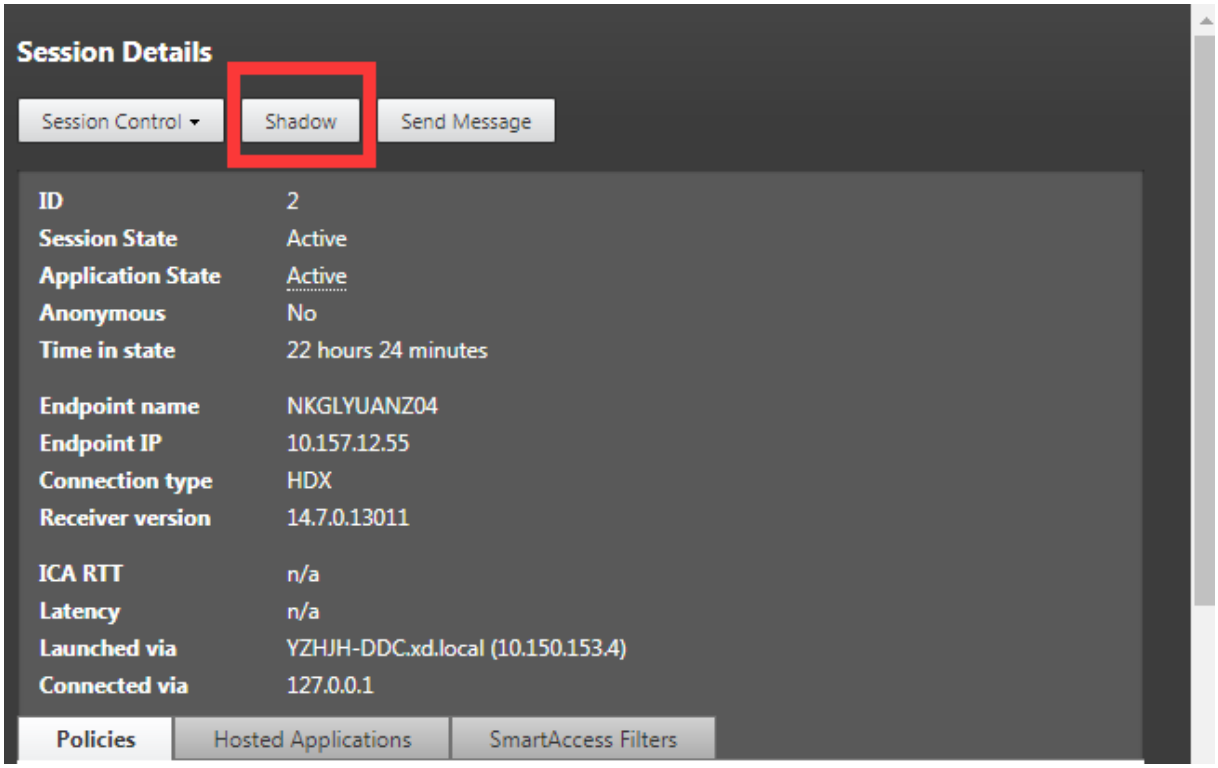
Install a root certificate on each Citrix Director client Session shadowing uses the same registry-based certificate store as IIS, so you can install root certificates using IIS or the Microsoft Management Console (MMC) Certificates snap-in. When you receive a certificate from a CA, you can restart the Web Server Certificate Wizard in IIS and the wizard installs the certificate. Alternatively, you can view and import certificates on the computer using the MMC and add the certificate as a standalone snap-in. Internet Explorer and Google Chrome import the certificates installed on your operation system by default. For Mozilla Firefox, you must import your root SSL certificates on the **Authorities** tab of Certificate Manager.

Install a server certificate and its key on each Linux VDA server Name the server certificates "shadowingcert.*"and the key file "shadowingkey.*"(* indicates the format, for example, shadowingcert.pem and shadowingkey.key). Put server certificates and key files under the path **/etc/xdl/shadowingssl** and protect them properly with restricted permissions. An incorrect name or path makes the Linux VDA unable to find a specific certificate or key file and therefore causes connection failure with `Citrix Director`.

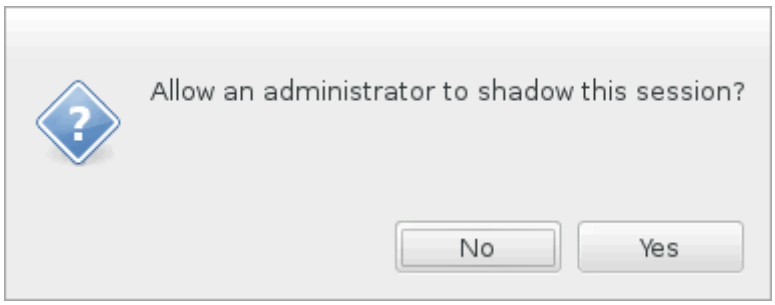
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Usage

From `Citrix Director`, find the target session and click **Shadow** in the **Session Details** view to send a shadowing request to the Linux VDA.



After the connection initializes, a confirmation appears on the ICA session client (not the `Citrix Director` client) to ask the user for permission to shadow the session.



If the user clicks **Yes**, a window appears on the `Citrix Director` side, indicating that the ICA session is being shadowed.

For more information about the usage, see the Citrix Director Documentation.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Limitations

- Session shadowing is designed for use in an Intranet only. It does not work for external networks even connecting through Citrix Gateway. Citrix disclaims any responsibility for the Linux VDA session shadowing in an external network.
- With session shadowing enabled, a domain administrator can only view the ICA sessions, but has no permission to write or control it.
- After an administrator clicks **Shadow** from `Citrix Director`, a confirmation appears to ask the user for permission to shadow the session. A session can be shadowed only when the session user gives the permission.
- The previously mentioned confirmation has a timeout limitation, which is 20s. A shadowing request fails when the time runs out.
- One session can be shadowed by only one administrator. For example, if administrator B sends a shadowing request for a session administrator A is shadowing, the confirmation for getting the user permission reappears on the user device. If the user agrees, the shadowing connection for administrator A stops and a new shadowing connection is built for administrator B. If an administrator sends another shadowing request for the same session, a new shadowing connection can also be built.
- To use session shadowing, install `Citrix Director` 7.16 or later.
- A `Citrix Director` client uses an FQDN rather than an IP address to connect to the target Linux VDA server. Therefore, the `Citrix Director` client must be able to resolve the FQDN of the Linux VDA server.

Troubleshooting

If session shadowing fails, do debugging on both the `Citrix Director` client and the Linux VDA.

On the Citrix Director client

Through the developer tools of the browser, check the output logs on the **Console** tab. Or, check the response of the ShadowLinuxSession API on the **Network** tab. If the confirmation for getting user permission appears but the connection build-up fails, ping the VDA's FQDN manually to verify that `Citrix Director` can resolve the FQDN. If there's an issue with the `wss://` connection, check your certificates.

On the Linux VDA

Verify that the confirmation for getting the user permission appears in response to a shadowing request. If it does not, check the vda.log and hdx.log files for clues. To obtain the vda.log file, do the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

following:

1. Find the /etc/xdl/ctx-vda.conf file. Uncomment the following line to enable the vda.log configuration:

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

2. Open /etc/xdl/log4j.xml, locate the com.citrix.dmc part, and change “info”to “trace”as follows:

   ```
   <!-- Broker Agent Plugin - Director VDA plugin Logger -->

    <logger name="com.citrix.dmc">

      <level value="trace"/>

    </logger>
   <!--NeedCopy-->
   ```

3. Run the `service ctxvda restart` command to restart the `ctxvda` service.

If there’s an error during connection build-up:

1. Check for any firewall limitation that stops session shadowing from opening the port.
2. Verify that you have named certificates and key files properly and put them under the correct path if it’s the SSL scenario.
3. Verify that there are enough ports left between 6001-6099 for new shadowing requests.

The monitor service daemon

January 23, 2023

The monitor service daemon monitors key services by performing periodical scans. When detecting exceptions, the daemon restarts or stops service processes and cleans up process residuals for releasing resources. The detected exceptions are recorded in the **/var/log/xdl/ms.log** file.

Configuration

The monitor service daemon starts automatically when you start the VDA.

You can configure the feature through the **scanningpolicy.conf**, **rulesets.conf**, and **whitelist.conf** files under **/opt/Citrix/VDA/sbin** with administrator privileges.

To make your changes in the **scanningpolicy.conf**, **rulesets.conf**, and **whitelist.conf** files take effect, run the following command to restart the monitor service daemon.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

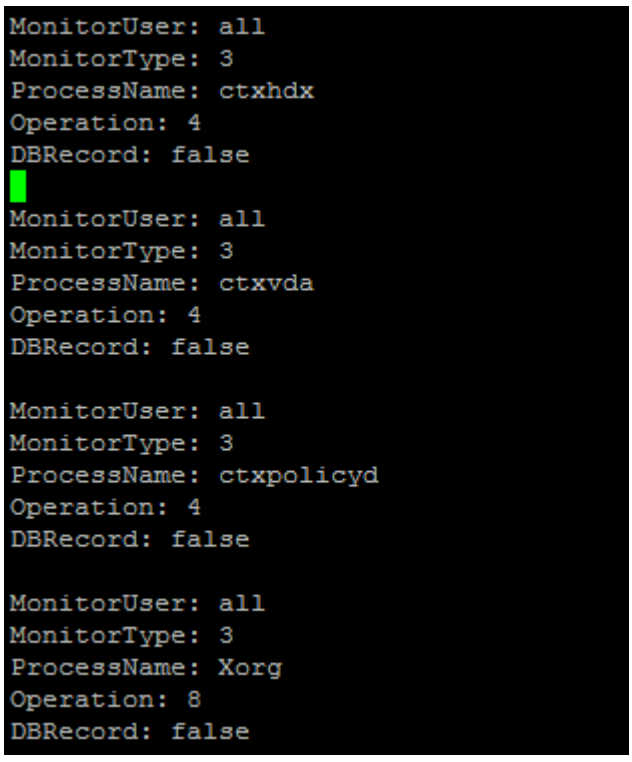
- **scanningpolicy.conf**

  This configuration file enables or disables the monitor service daemon. It sets the service detection interval and specifies whether to repair detected exceptions.

  - MonitorEnable: true/false (true by default)
  - DetectTime: 20 (unit: seconds, default value: 20, minimum value: 5)
  - AutoRepair: true/false (true by default)
  - MultBalance: false
  - ReportAlarm: false

- **rulesets.conf**

  This configuration file specifies the target services to monitor. There are four monitored services by default as shown in the following screen capture.



  To configure each service to monitor, set the following fields.

  - **MonitorUser**: all
  - **MonitorType**: 3

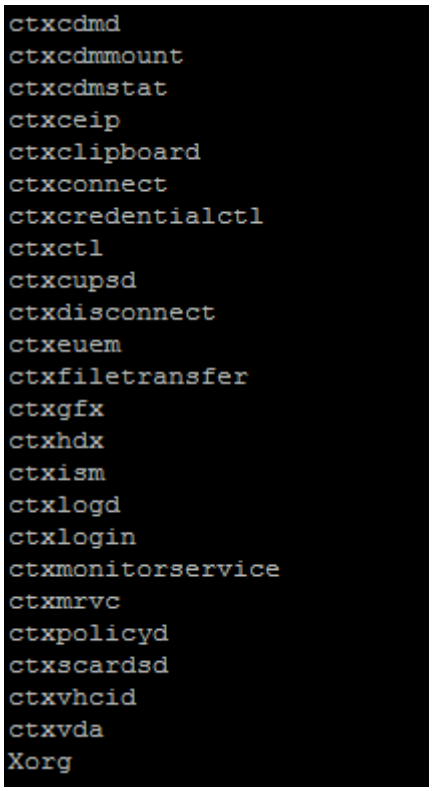
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **ProcessName**: <> (The process name cannot be left blank and must be exactly matched.)
- **Operation**: 1/2/4/8 (1 = stop the service when exceptions are detected. 2 = kill the service when exceptions are detected. 4 = restart the service. 8 = clear the Xorg process residuals.)
- **DBRecord**: false

- **whitelist.conf**

  The target services specified in the **rulesets.conf** file must also be configured in the **whitelist.conf** file. The white list configuration is a secondary filter for security.

  To configure the white list, include only the process names (which must be match exactly) in the **whitelist.conf** file. For an example, see the following screen capture.



> **Note:**
>
> Before you stop the `ctxvda`, `ctxhdx`, and `ctxpolicyd` services, run the `service ctxmonitorservice stop` command to stop the monitor service daemon. Otherwise, the monitor service daemon restarts the services you stopped.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Tools and utilities

April 3, 2023

Session data query utility

We provide a utility (`ctxsdcutil`) that you can use to query session data on each Linux VDA. To query the following data of all sessions or a specific session hosted on a VDA, run the `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]` command. The `[-c]` argument means to query data every second.

- **Input Session Bandwidth**
- **Output Session Bandwidth**
- **Output Session Line Speed**
- **Latency - Last Recorded**
- **Round Trip Time**
- **Output ThinWire Bandwidth**
- **Output Audio Bandwidth**
- **Output Printer Bandwidth**
- **Input Drive Bandwidth**
- **Output Drive Bandwidth**

The xdlcollect Bash script

The `xdlcollect` Bash script used to collect logs is integrated into the Linux VDA software and located under **/opt/Citrix/VDA/bin**. After you install the Linux VDA, you can run the `bash /opt/Citrix/VDA/bin/xdlcollect.sh` command to collect logs. After log collection completes, a compressed log file is generated in the same folder as the script. The `xdlcollect` Bash script can ask you whether to upload the compressed log file to Citrix Insight Services (CIS). If you agree, `xdlcollect` returns an upload_ID after the upload completes. The upload does not remove the compressed log file from your local machine. Other users can use the upload_ID to access the log file in CIS.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

XDPing

The Linux **XDPing** tool is a command-line application. It automates the process of checking for common configuration issues with a Linux VDA environment.

The Linux **XDPing** tool performs over 150 individual tests on the system, which are broadly categorized as follows:

- Check whether Linux VDA system requirements are met
- Identify and display machine information including the Linux distributions
- Check the Linux kernel compatibility
- Check for any known Linux distribution issues that can impact the Linux VDA operation
- Check the Security-Enhanced Linux (SELinux) mode and compatibility
- Identify network interfaces and check network settings
- Check storage partitioning and available disk space
- Check machine host and domain name configuration
- Check DNS configuration and perform lookup tests
- Identify underlying hypervisors and check virtual machine configuration. Support for:
  - Citrix Hypervisor
  - Microsoft HyperV
  - VMware vSphere
- Check time settings and check whether network time synchronization is operational
- Check whether PostgreSQL service is properly configured and operational
- Check whether the firewall is enabled and required ports are open
- Check Kerberos configuration and perform authentication tests
- Check the LDAP search environment for the group policy service engine
- Check whether Active Directory integration is set up properly and the current machine is joined to the domain. Support for:
  - Samba Winbind
  - Dell Quest Authentication Services
  - Centrify DirectControl
  - SSSD
- Check the integrity of the Linux computer object in Active Directory
- Check Pluggable Authentication Module (PAM) configuration
- Check the core dump pattern
- Check whether packages required by the Linux VDA are installed
- Identify the Linux VDA package and check the integrity of the installation
- Check the integrity of the PostgreSQL registry database
- Check whether the Linux VDA services are properly configured and operational

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Check the integrity of the VDA and HDX configuration
- Probe each configured Delivery Controller to test that the Broker Service is reachable, operational, and responsive
- Check whether the machine is registered with the Delivery Controller farm
- Check the state of each active or disconnected HDX session
- Scan log files for the Linux VDA related errors and warnings
- Check whether the version of Xorg is suitable

Use the Linux XDPing tool

> **Note:**
>
> Running ctxsetup.sh does not install **XDPing**. You can run `sudo /opt/Citrix/VDA/bin/xdping` to install **XDPing**.
> This command also creates a Python3 virtual environment that is required for **XDPing**. If this command fails to create a Python3 virtual environment, create it manually following the instructions at Create a Python3 virtual environment.
>
> To address SSL connection errors that you might encounter when using the pip tool, consider adding the following trusted hosts to the /etc/pip.conf file:
> `[global]`
> `trusted-host =`
> `pypi.org`
> `files.pythonhosted.org`

XDPing comes with the single executable named `xdping` that is run from the command shell.

To display the command-line options, use the `-h` option:

```
sudo /opt/Citrix/VDA/bin/xdping -h
<!--NeedCopy-->
```

To run the full suite of tests, run `xdping` without any command-line options:

```
sudo /opt/Citrix/VDA/bin/xdping
<!--NeedCopy-->
```

To check the environment before installing the Linux VDA package, run the `pre-flight` tests:

```
sudo /opt/Citrix/VDA/bin/xdping --preflight
<!--NeedCopy-->
```

To run specific test categories only, for example, the time and Kerberos tests, use the `-T` option:

```
sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To probe a particular XenDesktop Controller:

```
sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
<!--NeedCopy-->
```

Sample Output The following is a sample output from running the Kerberos test:

```
sudo xdping -T kerberos

Root User ------------------------------------------------------------------
    User:         root
    EUID:         0
      Verify user is root                                                [Pass]

Kerberos -------------------------------------------------------------------
    Kerberos version: 5
      Verify Kerberos available                                          [Pass]
      Verify Kerberos version 5                                          [Pass]
    KRB5CCNAME:   [Not set]
                  Distro default FILE:/tmp/krb5cc_%{uid}
    KRB5CCNAME type: [Supported]
    KRB5CCNAME format: [Default]
      Verify KRB5CCNAME cache type                                       [Pass]
      Verify KRB5CCNAME format                                           [Pass]
    Configuration file: /etc/krb5.conf [Exists]
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
  Verify Kerberos configuration file found                              [Pass]
Keytab file:  /etc/krb5.keytab [Exists]
Default realm: XD2.LOCAL
Default realm KDCs: [NONE SPECIFIED]
Default realm domains: [NONE SPECIFIED]
DNS lookup realm: [Enabled]
DNS lookup KDC: [Enabled]
Weak crypto:  [Disabled]
Clock skew limit:  300 s
  Verify system keytab file exists                                      [Pass]
  Verify default realm set                                              [Pass]
  Verify default realm in upper-case                                    [Pass]
  Verify default realm not EXAMPLE.COM                                  [Pass]
  Verify default realm domain mappings                                  [Pass]
  Verify default realm master KDC configured                            [Pass]
  Verify Kerberos weak crypto disabled                                  [Pass]
  Verify Kerberos clock skew setting                                    [Pass]
Default ccache: [Not set]
               Distro default FILE:/tmp/krb5cc_%{uid}
Default ccache type: [Supported]
Default ccache format: [Default]
  Verify default credential cache cache type                            [Pass]
  Verify default credential cache format                                [Pass]
UPN system key [MYVDA1$@          ]: [MISSING]
SPN system key [host/m                  l]: [Exists]
  Verify Kerberos system keys for UPN exist                            [ERROR]
  No system keys were found for the user principal name (UPN) of
  the machine account. For the Linux VDA to mutually authenticate
  with the Delivery Controller, the system keytab file must
  contain keys for both the UPN and host-based SPN of the machine
  account.

      Verify Kerberos system keys for SPN exist                          [Pass]
    Kerberos login: [FAILED AUTHENTICATION]
                    Keytab contains no suitable keys for MYVDA1$@
                    while getting initial credentials
      Verify KDC authentication                                         [ERROR]
      Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
      from the KDC authentication service for the machine account UPN
      MYVDA1$@          . Check that the Kerberos configuration is
      valid and the keys in the system keytab are current.


Summary ------------------------------------------------------------------------
  The following tests did not pass:
      Verify Kerberos system keys for UPN exist                         [ERROR]
      Verify KDC authentication                                         [ERROR]
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Others

January 23, 2023

This section contains the following topics:

- Citrix Workspace app for HTML5 support
- Create a Python3 virtual environment
- Integrate NIS with Active Directory
- IPv6
- LDAPS
- **Xauthority**

Citrix Workspace app for HTML5 support

January 23, 2023

You can use Citrix Workspace app for HTML5 to access Linux virtual apps and desktops directly without connecting your client to Citrix Gateway. For information about Citrix Workspace app for HTML5, see the Citrix documentation.

Enable this feature

This feature is disabled by default. To enable it, do the following:

1. In Citrix StoreFront, enable Citrix Workspace app for HTML5.

   For the detailed procedure, see Step 1 of the Knowledge Center article CTX208163.

2. Enable WebSocket connections.

   a) In Citrix Studio, set the **WebSockets connections** policy to **Allowed**.

   You can also set the other WebSocket policies. For a full list of the WebSocket policies, see WebSockets policy settings.

   b) On the VDA, restart the `ctxvda` service and the `ctxhdx` service, in this order, for your setting to take effect.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

c) On the VDA, run the following command to check whether the WebSocket listener is running.

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

When the WebSocket listener is running, the command output is similar to the following:

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

Note: You can also enable TLS encryption to secure WebSocket connections. For information about enabling TLS encryption, see Secure user sessions using TLS.

Create a Python3 virtual environment

October 18, 2023

If you are connecting to the network, running the `sudo /opt/Citrix/VDA/bin/xdping` or `/opt/Citrix/VDA/sbin/enable_ldaps.sh` command can create a Python3 virtual environment. However, if the commands fail to create a Python3 virtual environment, you can create it manually even without a network connection. This article details the prerequisites and steps to create a Python3 virtual environment without a network connection.

Prerequisites

- You must have administrative privileges to access the `/opt/Citrix/VDA/sbin/ctxpython3` directory.
- The wheel files of `Python3` packages are in place. You can download the wheel files from https://pypi.org/.

Create a Python3 virtual environment

Complete the following steps to create a Python3 virtual environment:

1. Install Python3 dependencies.

   For Amazon Linux 2:

   ```
   yum -y install python3 python3-devel krb5-devel gcc
   <!--NeedCopy-->
   ```

   For RHEL and Rocky Linux:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
yum -y install python3-devel krb5-devel gcc
<!--NeedCopy-->
```

> **Note:**
>
> You might have to enable a particular repository to install some dependencies. For RHEL 7, run the `subscription-manager repos --enable rhel-7-server-optional-rpms` command. For RHEL 8, run the `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms` command.

For Debian, Ubuntu:

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
<!--NeedCopy-->
```

For SUSE:

```
zypper -n install lsb-release python3-devel python3-setuptools krb5-devel gcc libffi-devel libopenssl-devel
<!--NeedCopy-->
```

2. Create a Python3 virtual environment.

> **Note:**
>
> To address SSL connection errors that you might encounter when using the pip tool, consider adding the following trusted hosts to the /etc/pip.conf file:
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

For Amazon Linux 2, Debian, RHEL, Rocky Linux, Ubuntu:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

For SUSE:

```
export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin

sudo mkdir -p /usr/lib/mit/include/gssapi/

sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/gssapi/gssapi_ext.h

sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Install LDAPS dependencies.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi==1.7.3 ldap3==2.9.1 pyasn1==0.4.8 pycparser==2.21 six==1.16.0
<!--NeedCopy-->
```

4. Install **XDPing** dependencies.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging==21.3 pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser==2.21 pyparsing==3.0.8 scramp==1.4.1 six==1.16.0 termcolor==1.1.0

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl<!--NeedCopy-->
```

Integrate NIS with Active Directory

January 23, 2023

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 Virtual Apps and Desktops. As a result, it fits tightly into the Windows AD environment.

Using NIS instead of AD as a UID and GID provider requires the account information (user name and password combinations) to be the same in 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 is used only for special use cases. For an RHEL/CentOS distribution, follow the instructions in Install the Linux VDA on Amazon Linux 2, CentOS, RHEL, and Rocky Linux manually. For an Ubuntu distribution, follow

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> the instructions in Install the Linux VDA on Ubuntu manually.

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 for the system. It provides both PAM and NSS modules, and in the future can support D-BUS based interfaces for extended user information. It also provides a better database to store local user accounts and extended user data.

Integrate NIS with AD

To integrate NIS with AD, complete the following steps:

Step 1: Add the Linux VDA as a NIS client

Configure the NIS client:

```
yum –y install ypbind rpcbind oddjob-mkhomedir
<!--NeedCopy-->
```

Set the NIS domain:

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

The **nis.domain** represents the domain name of the NIS server. The **server.nis.domain** is the host name 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
<!--NeedCopy-->
```

Ensure that the NIS configuration is correct:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

```
getent passwd nisaccount
<!--NeedCopy-->
```

> **Note:**
>
> The **nisaccount** represents the real NIS account on the NIS server. Ensure that the UID, GID, home directory, and login shell are configured correctly.

Step 2: Join the domain and create a host keytab using 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 the functions, 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 using 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
<!--NeedCopy-->
```

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

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 offline logon = no
```

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

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

REALM is the Kerberos realm name in uppercase and **user** is a domain user who has permissions to add computers to the domain.

Step 3: 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 (more options can be added as needed):

```
[sssd]
config_file_version = 2
domains = EXAMPLE
services = nss, pam

[domain/EXAMPLE]
# Uncomment if you need offline logins
# cache_credentials = true
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
id_provider = proxy
proxy_lib_name = nis
auth_provider = ad
access_provider = ad

# Should be specified as the long version of the Active Directory domain.
ad_domain = EXAMPLE.COM

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
21
22 # Uncomment if service discovery is not working
23 # ad_server = server.ad.example.com
24
25 # Comment out if the users have the shell and home dir set on the AD
      side
26 default_shell = /bin/bash
27 fallback_homedir = /home/%d/%u
28
29 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
      available
30 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
31 <!--NeedCopy-->
```

Replace **ad.domain.com**, **server.ad.example.com** with the corresponding value. For more details, see the **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
```

Step 4: Configure NSS/PAM

RHEL/CentOS:

Use **authconfig** to enable SSSD. Install **oddjob-mkhomedir** to ensure that the home directory creation is compatible with SELinux:

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo systemctl enable sssd
6 <!--NeedCopy-->
```

> **Tip:**
>
> When configuring Linux VDA settings, consider that for SSSD, there has no special settings for the Linux VDA client. For extra solutions in the **ctxsetup.sh** script, use the default value.

Step 5: Verify the Kerberos configuration

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

```
1 sudo klist -ke
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

This command displays 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
<!--NeedCopy-->
```

The machine and realm names must be specified in uppercase. 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 -ke
<!--NeedCopy-->
```

Step 6: 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
<!--NeedCopy-->
```

The **DOMAIN** parameter indicates the short version domain name. If another logon format 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, use a domain user account to log on to the Linux VDA. The domain user account has not been used before.

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

id -u
<!--NeedCopy-->
```

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

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
3
4 <!--NeedCopy-->
```

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

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

IPv6

January 23, 2023

The Linux VDA supports IPv6 to align with Citrix Virtual Apps and Desktops. When using this feature, consider the following:

- For dual stack environments, IPv4 is 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 must be IPv6, not only for the Linux VDA.
> - Centrify does not support pure IPv6.

No special setup tasks are required for IPv6 when you install 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:

```
1 " HKLM\Software\Policies\Citrix\VirtualDesktopAgent " -t " REG_DWORD "
    -v " OnlyUseIPv6ControllerRegistration "
2 " HKLM\Software\Policies\Citrix\VirtualDesktopAgent " -t " REG_DWORD "
    -v " ControllerRegistrationIPv6Netmask "
3 <!--NeedCopy-->
```

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

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
    OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
2 <!--NeedCopy-->
```

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

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

For more information about IPv6 deployment in Citrix Virtual Apps and Desktops, see IPv4/IPv6 support.

Troubleshooting

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

LDAPS

January 23, 2023

LDAPS is the secure version of the Lightweight Directory Access Protocol (LDAP) where LDAP communications are encrypted using TLS/SSL.

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

The following Linux VDA components have dependencies on LDAPS:

- Broker agent: Linux VDA registration with a Delivery Controller
- Policy service: Policy evaluation

Configuring LDAPS involves:

- Enable LDAPS on the Active Directory (AD)/LDAP server
- Export the root CA for client use
- Enable/disable LDAPS on the Linux VDA
- Configure LDAPS for third-party platforms
- Configure SSSD
- Configure Winbind
- Configure Centrify
- Configure Quest

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> You can run the following command to set a monitoring cycle for your LDAP servers. The default value is 15 minutes. Set it to 10 minutes at least.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "ListOfLDAPServersMonitorPeroid" -t "
     REG_DWORD" -d "0x0000000f" --force
2 <!--NeedCopy-->
```

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.

> **Tip:**
>
> LDAPS is enabled automatically when you install an Enterprise Root CA on a domain controller.

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.

When you have a multi-tier certificate authority hierarchy, you do not automatically have the appropriate certificate for LDAPS authentication on the domain controller.

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

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 a trusted keystore.

For more information about how to export Root CA, see How to export Root Certification Authority Certificate on the Microsoft Support website.

Enable or disable LDAPS on the Linux VDA

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

The syntax for this command includes the following:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```

- Enable LDAP over SSL/TLS with channel binding:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
<!--NeedCopy-->
```

> **Note:**
>
> The root CA certificate for channel binding must be in PEM format. If enabling LDAPS does not create a Python3 virtual environment successfully, create it manually following the instructions at Create a Python3 virtual environment.
>
> To address SSL connection errors that you might encounter when using the pip tool, consider adding the following trusted hosts to the /etc/pip.conf file:
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

- Fall back to LDAP without SSL/TLS

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

The Java keystore dedicated for LDAPS resides 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

HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
<!--NeedCopy-->
```

Configure LDAPS for third-party platform

Besides the Linux VDA components, several third-party software components that adhere to the VDA 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **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 port 389.

SSSD

Configure the SSSD secure LDAP traffic on port 636 or port 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 **/etc/samba/smb.conf** and **/etc/openldap/ldap.conf** (for RHEL) or **/etc/ldap/ldap.conf** (for Ubuntu). Change the files as follows:

- smb.conf

  ```
  ldap ssl = start tls
  ldap ssl ads = yes
  client ldap sasl wrapping = plain
  ```

- ldap.conf

  ```
  TLS_REQCERT never
  ```

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

```
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 port 389 using a different method.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Troubleshooting

The following issues might arise when you use 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 ports are configured correctly. Check the Root CA Certificate first and ensure that it matches the AD/LDAP server.

- **Incorrect registry change by accident**

  If you updated the LDAPS related keys 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 occur.

- **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 Certificate is the correct type. It is supposed to be compatible with most of the Java Keytool types supported. If it is not listed in the support list, you can convert the type first. We recommend 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 keystore.

Xauthority

January 23, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

The Linux VDA supports environments that use X11 display functionality (including `xterm` and `gvim`) for interactive remoting. 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 run 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. It is used to store credentials in cookies used by xauth for authentication of XServer. When an XServer instance (Xorg) is started, the cookie is used to authenticate connections to that specific display.

How it works

When Xorg starts up, a `.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:

```
# xauth -f ~/.Xauthority

# > list

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

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:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
   XauthEnabled" -d "0x00000001" --force
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
     CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
      -d "0x00000001" --force
4 <!--NeedCopy-->
```

After enabling **Xauthority**, pass the `.Xauthority` file to the **XClient** manually or by mounting a shared home directory:

- Pass the `.Xauthority` file to the XClient manually

  After launching an ICA session, the Linux VDA generates the `.Xauthority` file 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:

  ```
  1  export DISPLAY={
  2  Display number stored in the Xauthority file }
  3
  4
  5  export XAUTHORITY={
  6  the file path of .Xauthority }
  7
  8  <!--NeedCopy-->
  ```

  > **Note:**
  >
  > If the **XAUTHORITY** environment variable is not set, the `~/.Xauthority` file is used by default.

- Pass the `.Xauthority` file to the 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 the XClient, the user does not need to transmit this `.Xauthority` file to the XClient manually. After the **DISPLAY** and **XAUTHORITY** environment variables are set correctly, the GUI is displayed in the XServer desktop automatically.

Troubleshooting

If **Xauthority** does not work, follow the troubleshooting steps:

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

   ```
   1  ps aux | grep -i xorg
   2  <!--NeedCopy-->
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

```
/var/xdl/xauth/.Xauthority110
<!--NeedCopy-->
```

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

```
Xauth -f /var/xdl/xauth/.Xauthority110
<!--NeedCopy-->
```

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 by using the IP address of the Linux VDA and the published desktop display number.

   For example, run the following command on the XClient machine:

   ```
   telnet 10.158.11.11 6160
   <!--NeedCopy-->
   ```

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

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

Authentication

January 23, 2023

This section contains the following topics:

- Authentication with Azure Active Directory
- Double-hop single sign-on authentication
- Federated Authentication Service
- Non-SSO authentication
- Smart cards
- Unauthenticated sessions by anonymous users

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Authentication with Azure Active Directory

February 1, 2023

> **Note:**
>
> This feature is available only for Azure-hosted VDAs.

Based on your needs, you can deploy two types of Linux VDAs in Azure:

- Azure AD DS-joined VMs. The VMs are joined to an Azure Active Directory (AAD) Domain Services (DS) managed domain. Users use their domain credentials to log on to the VMs.
- Non-domain-joined VMs. The VMs integrate with the AAD identity service to provide user authentication. Users use their AAD credentials to log on to the VMs.

For more information about AAD DS and AAD, see this Microsoft article.

This article shows you how to enable and configure the AAD identity service on non-domain-joined VDAs.

Supported distributions

- Ubuntu 22.04, 20.04, 18.04
- RHEL 8.6, 8.4, 7.9
- SUSE 15.3

For more information, see this Microsoft article.

Known issues and workarounds

On Red Hat 8.3 and 7.9, PAM (Pluggable Authentication Module) `pam_loginuid.so` fails to set `loginuid` after AAD user authentication. This issue blocks AAD users from accessing VDA sessions.

To work around this issue, in `/etc/pam.d/remote`, comment out the line `Session required pam_loginuid.so`. See the following screenshot for an example.

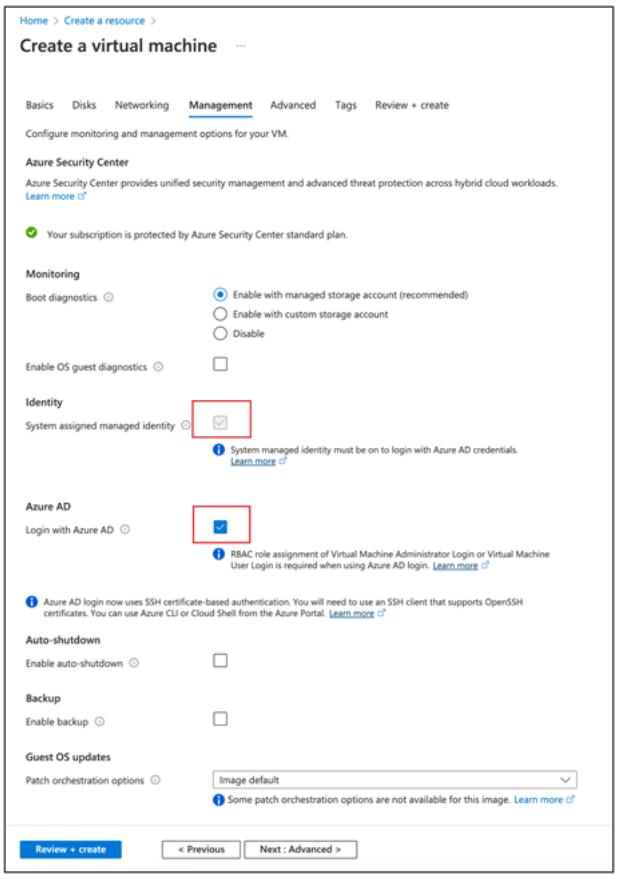
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
#%PAM-1.0
auth       substack     password-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
#session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    include      postlogin
```

Step 1: Create a template VM on the Azure portal

Create a template VM and install the Azure CLI on the VM.

1. On the Azure portal, create a template VM. Be sure to select **Login with Azure AD** on the **Management** tab before clicking **Review + create**.



2. Install the Azure CLI on the template VM.
   For more information, see this Microsoft article.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 2: Prepare a master image on the template VM

To prepare a master image, follow **Step 3: Prepare a master image** in Create Linux VDAs using Machine Creation Services (MCS).

Step 3: Set the template VM to non-domain-joined mode

After you create a master image, follow these steps to set the VM to non-domain-joined mode:

1. Run the following script from the command prompt.

```
Modify /var/xdl/mcs/mcs_util.sh
<!--NeedCopy-->
```

2. Locate `function read_non_domain_joined_info()`, and then change the value of `NonDomainJoined` to 2. See the following code block for an example.

```
function read_non_domain_joined_info()
{

log "Debug: Enter read_non_domain_joined_info"
# check if websocket enabled
TrustIdentity=`cat ${
 id_disk_mnt_point }
 ${
 ad_info_file_path }
  | grep '\[TrustIdentity\]' | sed 's/\s//g'`
if [ "$TrustIdentity" == "[TrustIdentity]" ]; then
NonDomainJoined=2
fi
...
 }

<!--NeedCopy-->
```

3. Save the change.
4. Shut down the template VM.

Step 4: Create the Linux VMs from the template VM

After you have the non-domain-joined template VM ready, follow these steps to create VMs:

1. Sign in to Citrix Cloud.
2. Double-click Citrix DaaS, and then access the Full Configuration management console.
3. In **Machine Catalogs**, choose to use Machine Creation Services to create the Linux VMs from the template VM. For more information, see Non-domain-joined VDAs in the Citrix DaaS document.

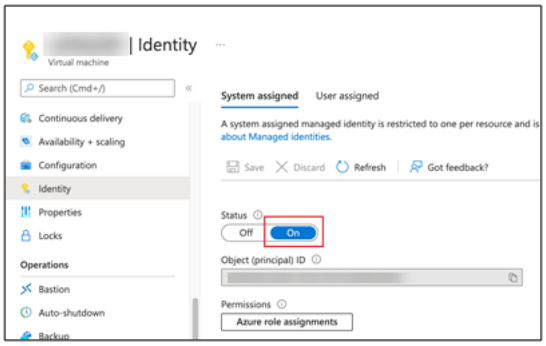
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Step 5: Assign AAD user accounts to the Linux VMs

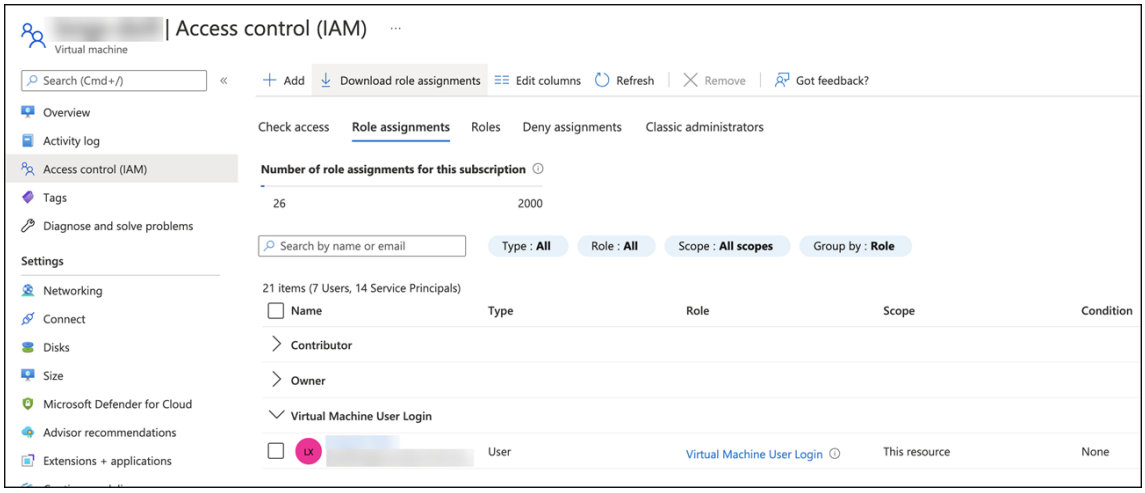
After you create the non-domain-joined VMs, assign AAD user accounts to them.

To assign AAD user accounts to a VM, follow these steps:

1. Access the VM using an administrator account.
2. On the **Identify > System assigned** tab, enable **System Identity**.



3. On the **Access control (IAM) > Role assignments** tab, locate the **Virtual Machine User Login** area, and then add the AAD user accounts as needed.



Log on to non-domain-joined VDAs

End users in your organization can log on to a non-domain-joined VDA in two ways. Detailed steps are as follows:

1. Start the Workspace app, and then log on to the workspace by entering the AAD user name and password. The Workspace page appears.
2. Double-click a non-domain-joined desktop. The AAD LOGIN page appears.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

The page varies depending on the login mode set on the VDA: Device Code or AAD account/password. By default, Linux VDAs authenticate AAD users using Device Code login mode as follows. As the administrator, you can change the login mode to AAD account/password if needed. See the following section for detailed steps.

3. Based on the onscreen instructions, log on to the desktop session in one of the following ways:

   - Scan the QR code and enter the code.
   - Enter the AAD user name and password.

Change to AAD account/password login mode

By default, Linux VDAs authenticate AAD users with device codes. See this Microsoft article for details. To change the login mode to *AAD account/password*, follow these steps:

Run the following command on the VDA, locate the key `AADAcctPwdAuthEnable`, and change its value to `0x00000001`.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Services\CitrixBrokerAgent\WebSocket" -t "REG_DWORD" -v "
   AADAcctPwdAuthEnable" -d "0x00000001" --force

<!--NeedCopy-->
```

> **Note:**
>
> This approach doesn't work with Microsoft accounts or accounts that have two-factor authentication enabled.

Double-hop single sign-on authentication

January 23, 2023

User credentials for accessing a StoreFront store can be injected to the AuthManager module of Citrix Workspace app for Linux and Citrix Receiver for Linux 13.10. After injection, you can use the client to access virtual desktops and applications from within a Linux virtual desktop session, without entering user credentials for a second time.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> This feature is supported on Citrix Workspace app for Linux and Citrix Receiver for Linux 13.10.

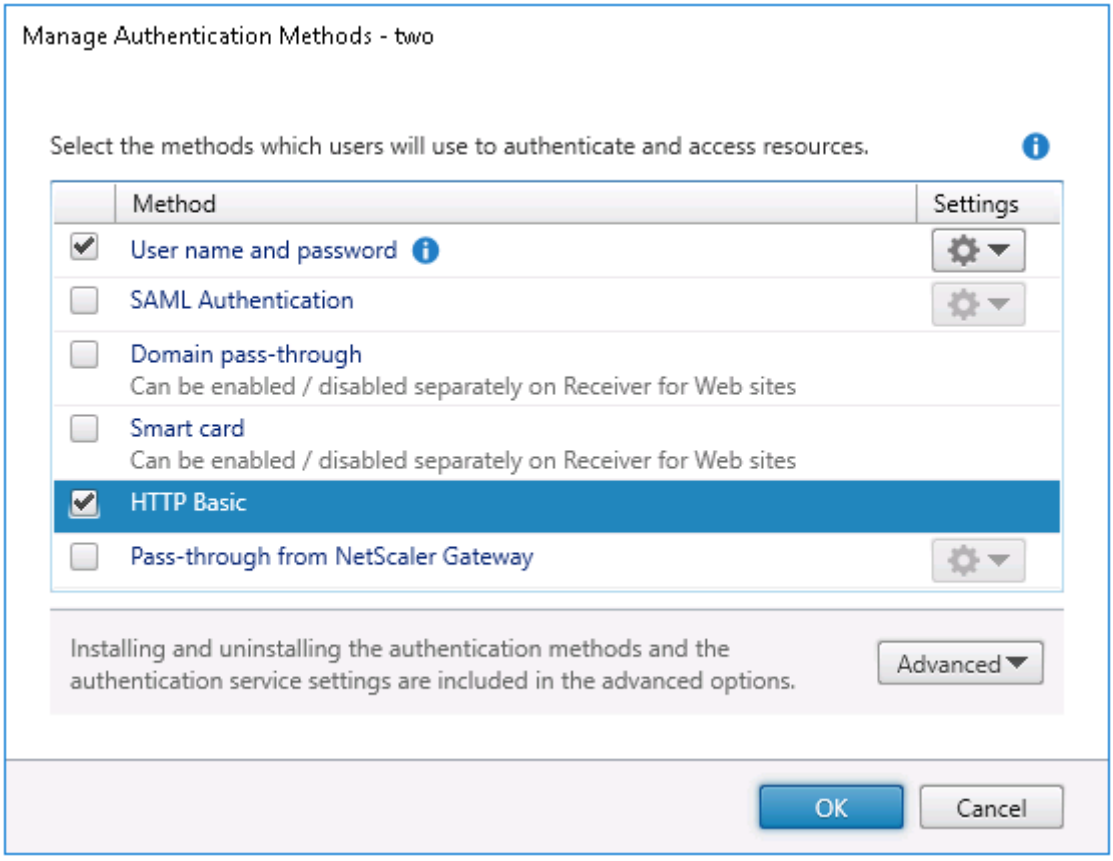
To enable the feature:

1. On the Linux VDA, install Citrix Workspace app for Linux or Citrix Receiver for Linux 13.10.

   Download the app from the Citrix download page for Citrix Workspace app or for Citrix Receiver.

   The default installation path is /opt/Citrix/ICAClient/. If you install the app to a different path, set the ICAROOT environment variable to point to the actual installation path.

2. In the Citrix StoreFront management console, add the **HTTP Basic** authentication method for the target store.



3. Add the following key to the AuthManager configuration file ($ICAROOT/config/AuthManConfig.xml) for allowing the HTTP Basic authentication:

```
<Protocols>
     <HTTPBasic>
         <Enabled>True</Enabled>
    </HTTPBasic>
</Protocols>
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Run the following commands to install the root certificate in the specified directory.

```
cp rootcert.pem $ICAROOT/keystore/cacerts/
$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
<!--NeedCopy-->
```

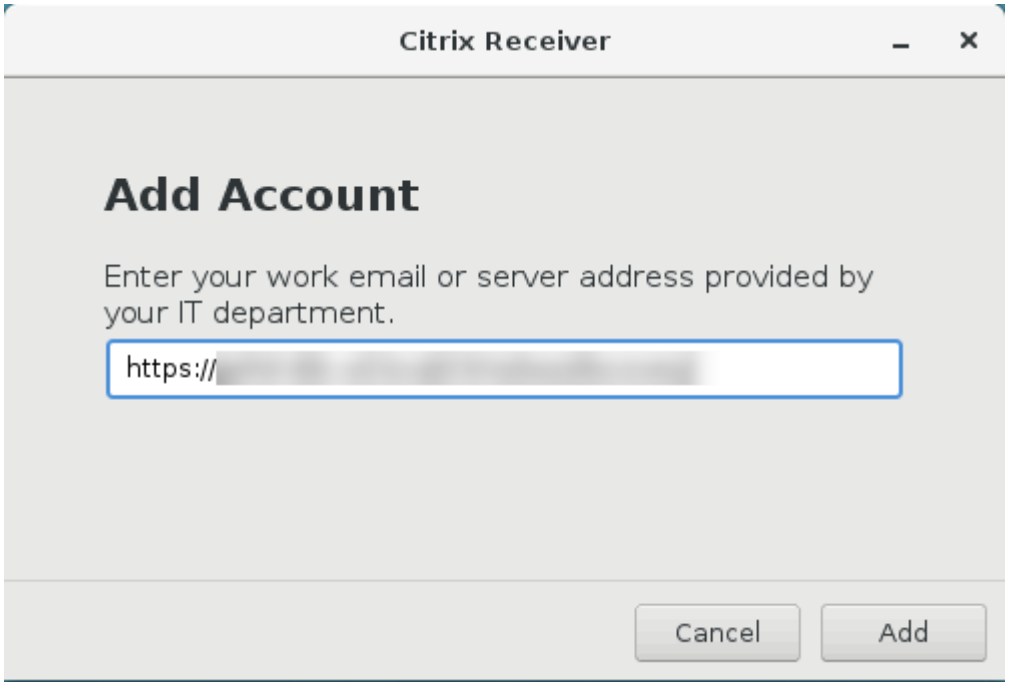
5. Run the following command to enable the feature:

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

6. Launch a Linux virtual desktop session and start Citrix Workspace app for Linux or Citrix Receiver for Linux 13.10 within that session.

   You are prompted for a store account when you start the Citrix Workspace app for the first time. Later on, you are logged on to the store you specified earlier automatically.

   > **Note:**
   >
   > Enter an HTTPS URL as your store account.



Federated Authentication Service

January 24, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

You can use Federated Authentication Service (FAS) to authenticate users logging on to a Linux VDA. The Linux VDA uses the same Windows environment as the Windows VDA for the FAS logon feature. For information about configuring the Windows environment for FAS, see Federated Authentication Service. This article provides extra information specific to the Linux VDA.

> **Note:**
>
> - The Linux VDA does not support the **In-session Behavior** policy.
> - The Linux VDA uses short connections to transmit data with FAS servers.
> - Starting with the 2206 release, you can customize the FAS port on the Linux VDA side through CTX_XDL_FAS_LIST in the ctxsetup.sh. For more information, see the Linux VDA installation article based on your distribution.

Configure FAS on the Linux VDA

FAS support on RHEL 8 and Rocky Linux 8

FAS depends on the pam_krb5 module, which is deprecated on RHEL 8 and Rocky Linux 8. The following steps are required if you want to use FAS on RHEL 8 and Rocky Linux 8 machines delivered in multi-session OS mode. For FAS on RHEL 8 and Rocky Linux 8 machines delivered in single-session OS (VDI) mode, you can skip the following steps.

1. Download the pam_krb5-2.4.8-6 source code from the following website:

   https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.

2. Build and install the pam_krb5 module on RHEL 8 and Rocky Linux 8.

```
yum install make gcc krb5-devel pam-devel autoconf libtool
rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
tar xvzf pam_krb5-2.4.8.tar.gz
cd pam_krb5-2.4.8
./configure --prefix=/usr
make
make install
<!--NeedCopy-->
```

3. Verify that pam_krb5.so exists under /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Set FAS servers

To use FAS in a fresh Linux VDA installation, type the FQDN of each FAS server when you run ctxinstall.sh or ctxsetup.sh. Because the Linux VDA does not support AD Group Policy, you can provide a semicolon-separated list of FAS servers instead. If any server address is removed, fill its blank with the **<none>** text string and do not modify the order of server addresses.

To upgrade an existing Linux VDA installation, you can rerun `ctxsetup.sh` to set the FAS servers. Or you can run the following commands to set the FAS servers and to restart the `ctxvda` service to make your setting take effect.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
    " -v "Addresses" -d "<Your-FAS-Server-List>" --force

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

To update the FAS servers through `ctxreg`, run the following commands:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -v "
    Addresses" -d "<Your-FAS-Server-List>"

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

Install certificates

For the verification of users' certificates, install the root CA certificate and all intermediate certificates on the VDA. For example, to install the root CA certificate, get the AD root certificate from the preceding **Retrieve the CA Certificate from the Microsoft CA (on AD)** step, or download its DER format from the root CA server `http://CA-SERVER/certsrv`.

> **Note:**
>
> The following commands also apply to configuring an intermediate certificate.

Convert a DER file (.crt, .cer, .der) to PEM by running the command similar to the following:

```
sudo openssl x509 -inform der -in root.cer -out root.pem
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Then, install the root CA certificate to the `openssl` directory by running the command similar to the following:

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

> **Note:**
>
> Do not put the root CA certificate under the **/root** path. Otherwise, FAS does not have the read permission to the root CA certificate.

Run ctxfascfg.sh

Run the ctxfascfg.sh script to configure FAS:

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

Environment variables are added so that `ctxfascfg.sh` can be run in silent mode:

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis**: Denotes the Active Directory integration method, which equals to `CTX_EASYINSTALL_ADINTEGRATIONWAY` when `CTX_EASYINSTALL_ADINTEGRATIONWAY` is specified. If `CTX_EASYINSTALL_ADINTEGRATIONWAY` is not specified, `CTX_FAS_ADINTEGRATIONWAY` uses its own value setting.
- **CTX_FAS_CERT_PATH =<certificate path>**: Specifies the full path that stores the root certificate and all intermediate certificates.
- **CTX_FAS_KDC_HOSTNAME**: Specifies the host name of the Key Distribution Center (KDC) when you select PBIS.
- **CTX_FAS_PKINIT_KDC_HOSTNAME**: Specifies the PKINIT KDC host name, which equals to CTX_FAS_KDC_HOSTNAME unless otherwise specified. If you have multiple Delivery Controllers, add the host names of all KDCs of the domain to pkinit_kdc_hostname in the **/etc/krb5.conf** file. For more information, see Knowledge Center article CTX322129.

Choose the correct Active Directory integration method and then type the correct path of certificates (for example, `/etc/pki/CA/certs/`).

The script then installs the krb5-pkinit and pam_krb5 packages and sets the relevant configuration files.

Disable FAS

To disable FAS on the Linux VDA, remove all FAS servers from ConfDB using the following commands:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
    " -v "Addresses" -d "" --force

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```

Limitation

- FAS supports limited Linux platforms and AD integration methods. See the following matrix:

	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	Yes	Yes	Yes	Yes
Debian 11.3	Yes	Yes	Yes	Yes
RHEL 9.0	Yes	Yes	No	No
RHEL 8.6, RHEL 8.4	Yes	Yes	Yes	Yes
RHEL 7.9 / CentOS 7.9	Yes	Yes	Yes	Yes
Rocky Linux 9.0	Yes	Yes	No	No
Rocky Linux 8	Yes	Yes	No	No
SLES 15.3	Yes	Yes	Yes	No
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Yes	Yes	Yes	Yes

- FAS doesn't support the lock screen yet. If you click the lock button in a session, you can't log back on to the session again by using FAS.
- This release supports only the common FAS deployments summarized in the Federated Authentication Service architectural overview article and doesn't include **Windows 10 Azure AD Join**.

Troubleshooting

Before troubleshooting FAS, make sure that the Linux VDA is installed and configured correctly and a non-FAS session can be launched successfully on the common store by using password authentication.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

If non-FAS sessions work properly, set the HDX log level of the **Login** class to VERBOSE and the VDA log level to TRACE. For information on enabling trace logging for the Linux VDA, see Knowledge Center article CTX220130.

FAS server configuration error

Launching a session from the FAS store fails.

Check **/var/log/xdl/hdx.log** and find the error log similar to the following:

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon Type] Federated Authentication Logon.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start connect to server 0

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed to connect: Connection refused.

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed to connect to server [0], please confirm if fas service list is well configurated in condb

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit, 43

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed to validate fas credential

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate: failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER

<!--NeedCopy-->
```

Solution Run the following command to verify that the Citrix registry value "HKEY_LOCAL_MACHINE\SOFTWARE\
is set to <Your-FAS-Server-List>.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
<!--NeedCopy-->
```

If the existing setting is incorrect, follow the preceding Set FAS servers step to set it again.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Incorrect CA certificate configuration

Launching a session from the FAS store fails. A gray window appears and disappears several seconds later.

Check **/var/log/xdl/hdx.log** and find the error log similar to the following:

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: entry

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller:
   current process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: entry

2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
    for response...

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query
   to server success

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: exit

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    input size 1888

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
    output size 1415

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: get logon certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
    cache certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: exit, 0

2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
      pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
<!--NeedCopy-->
```

Solution Verify that you have correctly set in `/etc/krb5.conf` the full path that stores the root CA certificate and all intermediate certificates. The full path is similar to the following:

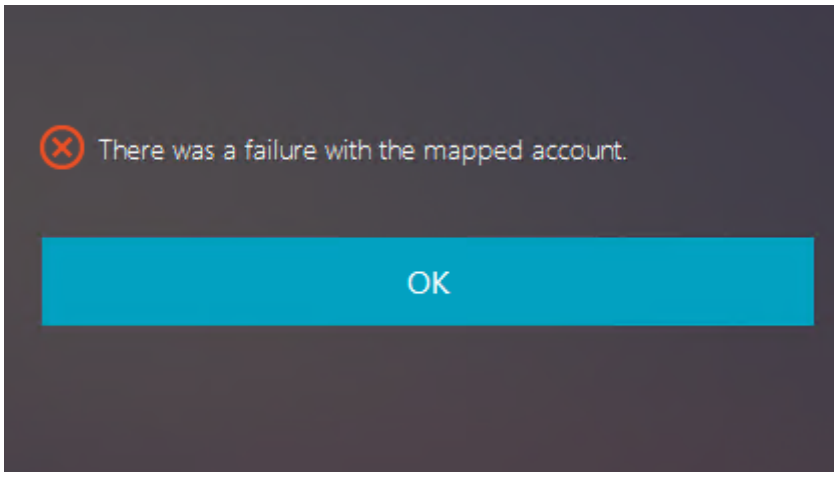
```
 [realms]

EXAMPLE.COM = {


    ......

    pkinit_anchors = DIR:/etc/pki/CA/certs/

    ......

 }

<!--NeedCopy-->
```

If the existing setting is incorrect, follow the preceding Install certificates step to set it again.

Alternatively, check whether the root CA certificate is valid.

Shadow account mapping error

FAS is configured by SAML authentication. The following error might occur after an ADFS user enters the user name and password on the ADFS logon page.



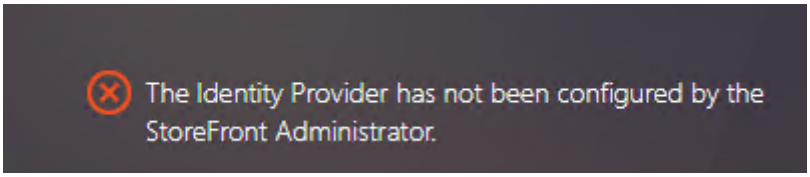
This error indicates that the ADFS user has been verified successfully, but there is no shadow user configured on AD.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Solution Set the Shadow Account on AD.

ADFS not configured

The following error occurs during a logon attempt to the FAS store:



The issue occurs when the FAS store is configured to use SAML authentication but the ADFS deployment is missing.

Solution Deploy the ADFS IdP for Federated Authentication Service. For more information, see Federated Authentication Service ADFS deployment.

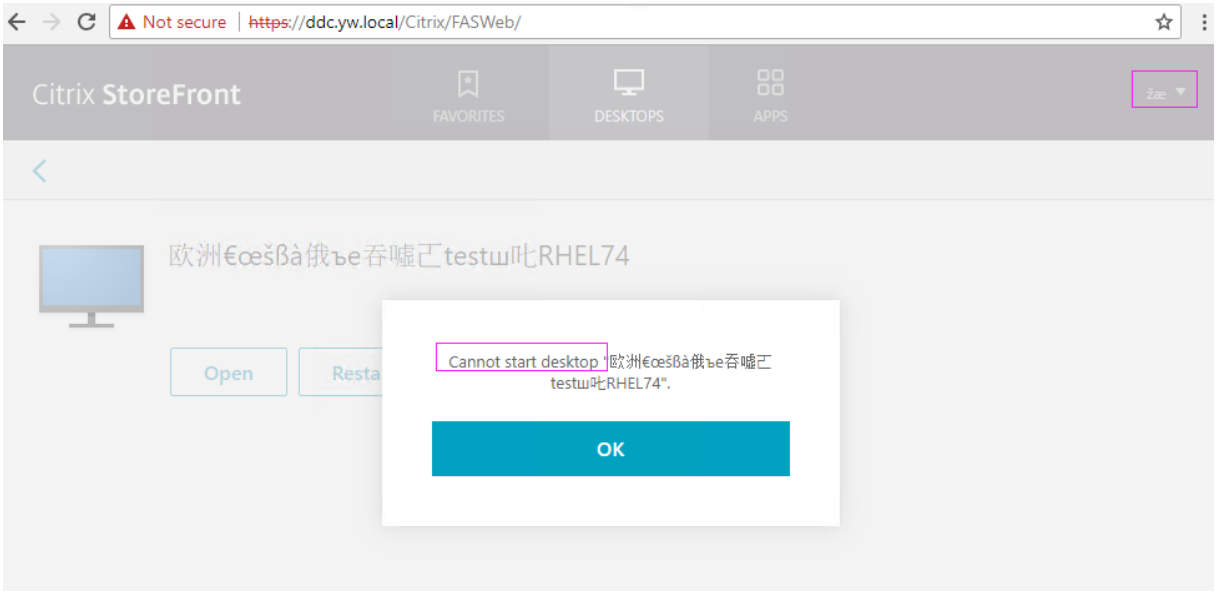
Related information

- The common FAS deployments are summarized in the Federated Authentication Service architectural overview article.
- "How-to"articles are introduced in the Federated Authentication Service advanced configuration chapter.

Known issue

When FAS is in use, you can fail when trying to launch a published desktop or app session with non-English characters.

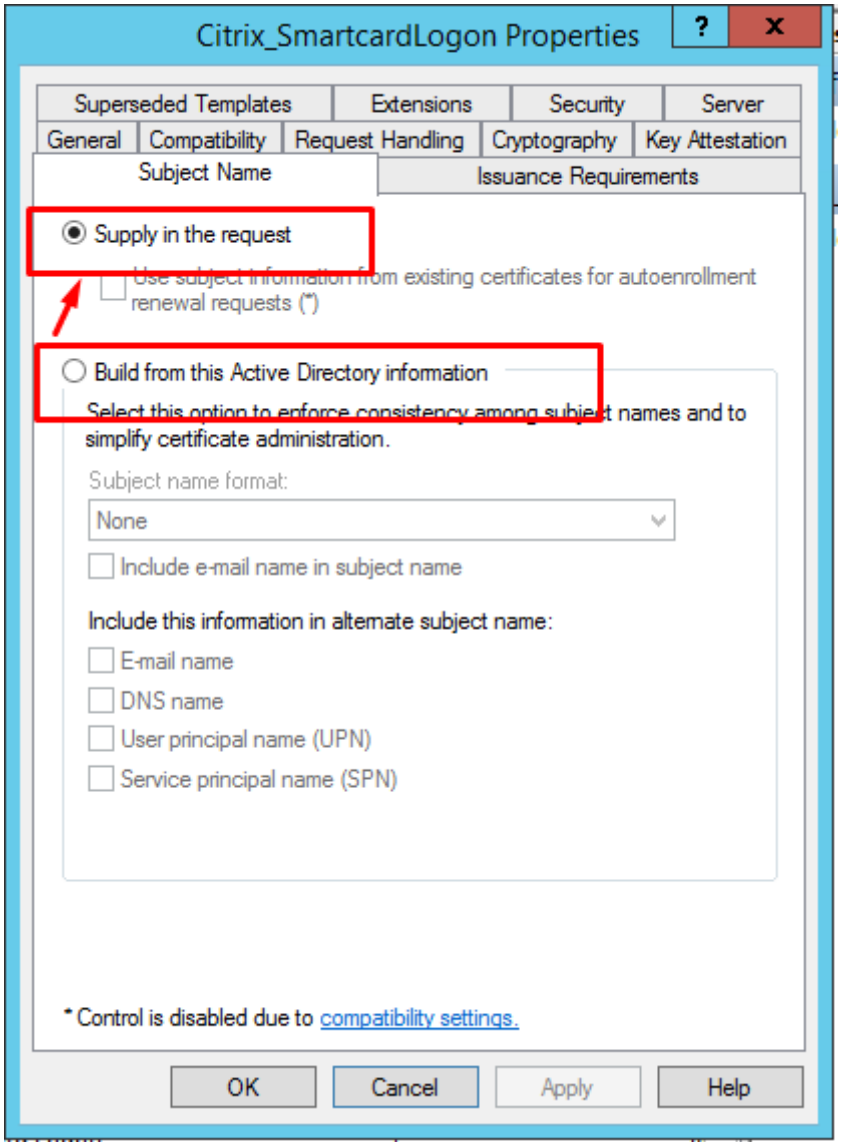
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Workaround

Right-click **Manage Templates** in the CA tool to change the **Citrix_SmartcardLogon** template from **Build from this Active Directory information** to **Supply in the request**:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Non-SSO authentication

January 23, 2023

This article provides guidance on how to enable non-SSO authentication on the Linux VDA.

Overview

By default, the Linux VDA has single sign-on (SSO) enabled. Users log on to Citrix Workspace app and to VDA sessions using one set of credentials.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To have users log on to VDA sessions using a different set of credentials, disable SSO on the Linux VDA. The following table lists combinations of user authentication methods supported in non-SSO scenarios.

Citrix Workspace app	VDA session
user name	user name
smart card	user name
user name	smart card

Disable SSO

Run the following command on your Linux VDA:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\WinStations\tcp" -t "REG_DWORD" -v "
   fPromptForDifferentUser" -d "0x00000001" --force
<!--NeedCopy-->
```

Smart cards

January 23, 2023

You can use a smart card connected to the client device for authentication when logging on to a Linux virtual desktop session. This feature is implemented through smart card redirection over the ICA smart card virtual channel. You can also use the smart card within the session. Use cases include:

- Adding a digital signature to a document
- Encrypting or decrypting an email
- Authenticating to a website

The Linux VDA uses the same configuration as the Windows VDA for this feature. For more information, see the Configure the smart card environment section in this article.

> **Note:**
>
> Using a mapped smart card within a Linux VDA session to sign on to Citrix Gateway isn't supported.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Prerequisites

The availability of smart card pass-through authentication is contingent on the following conditions:

- Your Linux VDA is installed on one of the following distributions:
  - RHEL 9.0
  - RHEL 8
  - RHEL 7/CentOS 7
  - Rocky Linux 9.0
  - Rocky Linux 8.6
  - Ubuntu 22.04
  - Ubuntu 20.04
  - Ubuntu 18.04
  - Debian 11.3

  After you complete installing the VDA, verify that your VDA can register with the Delivery Controller and you can open the published Linux desktop sessions using Windows credentials.
- Smart cards supported by OpenSC are used. For more information, see Ensure that OpenSC supports your smart card.
- Citrix Workspace app for Windows is used.

Ensure that OpenSC supports your smart card

OpenSC is a widely used smart card driver on RHEL 7.4+. As a fully compatible replacement of CoolKey, OpenSC supports many types of smart cards (see Smart Card Support in Red Hat Enterprise Linux).

In this article, the YubiKey smart card is used as an example to illustrate the configuration. YubiKey is an all-in-one USB CCID PIV device that can easily be purchased from Amazon or other retail vendors. The OpenSC driver supports YubiKey.

If your organization requires some other more advanced smart card, prepare a physical machine with a supported Linux distribution and the OpenSC package installed. For information about the OpenSC installation, see Install the smart card driver. Insert your smart card, and run the following command to verify that OpenSC supports your smart card:

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configuration

Prepare a root certificate

A root certificate is used to verify the certificate on the smart card. Complete the following steps to download and install a root certificate.

1. Get a root certificate in PEM format, typically from your CA server.

   You can run a command similar to the following to convert a DER file (*.crt, *.cer, *.der) to PEM. In the following command example, **certnew.cer** is a DER file.

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

2. Install the root certificate to the `openssl` directory. The **certnew.pem** file is used as an example.

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

   To create a path for installing the root certificate, run `sudo mdkir -p <path where you install the root certificate>`.

Build the pam_krb5 module on RHEL 8 and Rocky Linux 8

Smart card authentication depends on the pam_krb5 module, which is deprecated on RHEL 8 and Rocky Linux 8. The following steps are required if you want to use smart card authentication on RHEL 8 and Rocky Linux 8 machines delivered in multi-session OS mode. For smart card authentication on RHEL 8 and Rocky Linux 8 machines delivered in single-session OS (VDI) mode, you can skip the following steps.

1. Download the pam_krb5-2.4.8-6 source code from https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.
2. Build and install the pam_krb5 module on RHEL 8 and Rocky Linux 8.

   ```
   yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-
       tools
   yum install gcc krb5-devel pam-devel autoconf libtool
   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
   tar xvzf pam_krb5-2.4.8.tar.gz
   cd pam_krb5-2.4.8
   ./configure --prefix=/usr
   make
   make install
   <!--NeedCopy-->
   ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Verify that pam_krb5.so exists under /usr/lib64/security/.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

Configure the smart card environment

You can use the ctxsmartlogon.sh script to configure the smart card environment or complete the configuration manually.

(Option 1) Use the ctxsmartlogon.sh script to configure the smart card environment

> **Note:**
>
> The ctxsmartlogon.sh script adds PKINIT information to the default realm. You can change this setting through the **/etc/krb5.conf** configuration file.

Before using smart cards for the first time, run the ctxsmartlogon.sh script to configure the smart card environment.

> **Tip:**
>
> If you have used SSSD for domain joining, restart the SSSD service after you run ctxsmartlogon.sh.

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

The results resemble the following:

```
#*********************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*********************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
  Please select which Active Directory integration method to use:
     1: Winbind
     2: SSSD
     3: Centrify
  Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
  Installing, please wait...
    [krb5-pkinit][pam_krb5] already installed.
    [pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
  Packages installed. [Success]
Step 4:Configure krb5.conf.
  Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
  /etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
  Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
  /etc/pam.d/ctxfsc configure successfully.
  /etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

You can also disable smart cards by running the ctxsmartlogon.sh script:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

The results resemble the following:

```
#*******************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*******************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.
```

(Option 2) configure the smart card environment manually The Linux VDA uses the same smart card environment with the Windows VDA. In the environment, multiple components must be configured, including the Domain Controller, Microsoft Certificate Authority (CA), Internet Information Services, Citrix StoreFront, and Citrix Workspace app. For information about the configuration based on the YubiKey smart card, see Knowledge Center article CTX206156.

Before moving to the next step, make sure that:

- You have configured all components correctly.
- You have downloaded the private key and user certificate to the smart card.
- You can successfully log on to the VDA using the smart card.

Install the PC/SC Lite packages PCSC Lite is an implementation of the Personal Computer/Smart Card (PC/SC) specification in Linux. It provides a Windows smart card interface for communicating to smart cards and readers. Smart card redirection in the Linux VDA is implemented on the PC/SC level.

Run the following command to install the PC/SC Lite packages:

RHEL 9.0/8.x, Rocky Linux 9.0/8.6, RHEL 7/CentOS 7:

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

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04, Debian 11.3:

```
apt-get install -y libpcsclite1 libccid
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Install the smart card driver OpenSC is a widely used smart card driver. If OpenSC is not installed, run the following command to install it:

RHEL 9.0/8.x, Rocky Linux 9.0/8.6, RHEL 7/CentOS 7:

```
yum install opensc
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04, Debian 11.3:

```
apt-get install -y opensc
<!--NeedCopy-->
```

Install the PAM modules for smart card authentication Run the following command to install the pam_krb5 and krb5-pkinit modules.

RHEL 7/CentOS 7:

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

RHEL 9.0/8.x, Rocky Linux 9.0/8.6:

```
yum install krb5-pkinit
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04:

```
apt-get install libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

Debian 11.3:

```
apt-get install -y libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

The pam_krb5 module is a pluggable authentication module. PAM-aware applications can use pam_krb5 to check passwords and obtain ticket-granting tickets from the Key Distribution Center (KDC). The krb5-pkinit module contains the PKINIT plug-in that allows clients to obtain initial credentials from the KDC using a private key and a certificate.

Configure the pam_krb5 module The pam_krb5 module interacts with the KDC to get Kerberos tickets using certificates in the smart card. To enable pam_krb5 authentication in PAM, run the following command:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

In the **/etc/krb5.conf** configuration file, add PKINIT information according to the actual realm.

> **Note:**
>
> The **pkinit_cert_match** option specifies matching rules that the client certificate must match before it is used to attempt PKINIT authentication. The syntax of the matching rules is:
>
> **[relation-operator] component-rule ...**
>
> where **relation-operator** can be either **&&**, meaning all component rules must match, or **||**, meaning only one component rule must match.

Here is an example of a generic krb5.conf file:

```
EXAMPLE.COM = {


    kdc = KDC.EXAMPLE.COM

    auth_to_local = RULE:[1:$1@$0]

    pkinit_anchors = FILE:<path where you install the root certificate
       >/certnew.pem

    pkinit_kdc_hostname = KDC.EXAMPLE.COM

    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature

    pkinit_eku_checking = kpServerAuth

  }

<!--NeedCopy-->
```

The configuration file resembles the following after you add the PKINIT information.

```
CTXDEV.LOCAL = {
    kdc = [redacted]
    auth_to_local = RULE:[1:$1@$0]
    pkinit_kdc_hostname = ctx-ad.ctxdev.local
    pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
    pkinit_eku_checking = kpServerAuth
    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
}
```

Configure PAM authentication PAM configuration files tell what modules are used for PAM authentication. To add pam_krb5 as an authentication module, add the following line to the **/etc/pam.d/smartcard-auth** file:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options
=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.
so
```

The configuration file resembles the following after modification if SSSD is used.

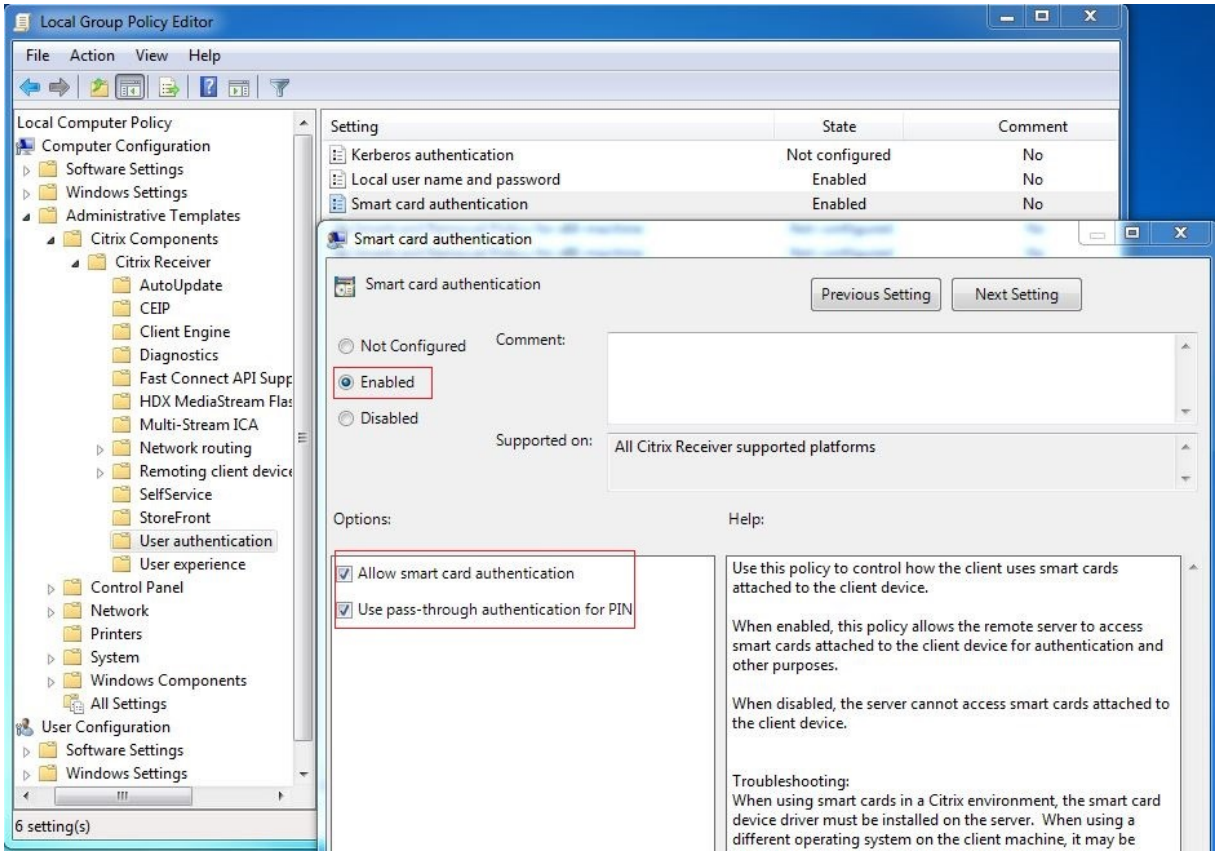
```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die]  pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
account     required      pam_permit.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
#session     optional      pam_oddjob_mkhomedir.so umask=0077
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
session     optional      pam_krb5.so
```

(Optional) Single sign-on by using smart cards

Single sign-on (SSO) is a Citrix feature that implements pass-through authentication with virtual desktop and application launches. This feature reduces the number of times that users type their PIN. To use SSO with the Linux VDA, configure Citrix Workspace app. The configuration is the same with the Windows VDA. For more information, see Knowledge Center article CTX133982.

Enable the smart card authentication as follows when configuring the group policy in Citrix Workspace app.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Fast smart card logon

Fast smart card is an improvement over the existing HDX PC/SC-based smart card redirection. It improves performance when smart cards are used in high-latency WAN environments. For more information, see Smart cards.

The Linux VDA supports fast smart card on the following versions of Citrix Workspace app:

- Citrix Receiver for Windows 4.12
- Citrix Workspace app 1808 for Windows and later

Enable fast smart card logon on the client Fast smart card logon is enabled by default on the VDA and disabled by default on the client. On the client, to enable fast smart card logon, include the following parameter in the default.ica file of the associated StoreFront site:

```
1 [WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Disable fast smart card logon on the client To disable fast smart card logon on the client, remove the **SmartCardCryptographicRedirection** parameter from the default.ica file of the associated StoreFront site.

Usage

Log on to the Linux VDA by using a smart card

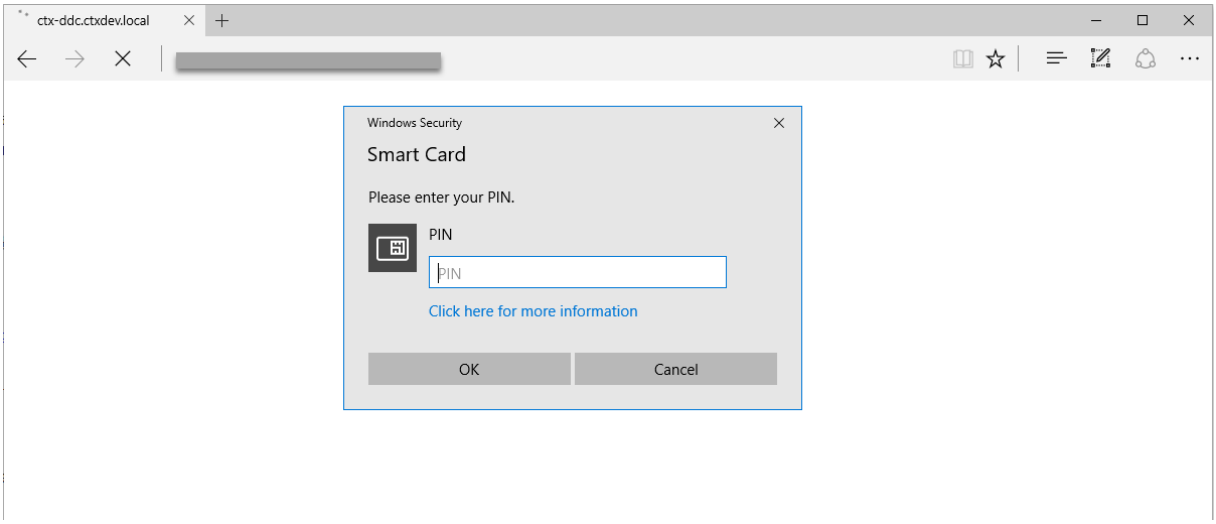
You can use a smart card to log on to the Linux VDA in both SSO and non-SSO scenarios.

- In the SSO scenario, you are logged on to StoreFront automatically by using the cached smart card certificate and PIN. When you launch a Linux virtual desktop session in StoreFront, the PIN is passed to the Linux VDA for smart card authentication.
- In the non-SSO scenario, you are prompted to select a certificate and type a PIN to log on to StoreFront.

When you launch a Linux virtual desktop session in StoreFront, a dialog box for logon to the Linux VDA appears as follows. The user name is extracted from the certificate in the smart card and you must type the PIN again for logon authentication.

This behavior is the same with the Windows VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Reconnect to a session by using a smart card

To reconnect to a session, ensure that the smart card is connected to the client device. Otherwise, a gray caching window appears on the Linux VDA side and exits quickly because reauthentication fails without the smart card connected. No other prompt is provided in this case to remind you to connect the smart card.

On the StoreFront side, however, if a smart card is not connected when you reconnect to a session, the StoreFront web might give an alert as follows:

Limitation

Support for limited Linux distributions and AD integration methods

- Smart card pass-through authentication supports limited Linux distributions and AD integration methods. See the following matrix:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	Winbind	SSSD	Centrify
Debian 11.3	Yes	Yes	Yes
RHEL 9.0	Yes	Yes	No
RHEL 8.6, RHEL 8.4	Yes	Yes	Yes
RHEL 7.9 / CentOS 7.9	Yes	Yes	Yes
Rocky Linux 9.0	Yes	Yes	No
Rocky Linux 8	Yes	Yes	No
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	Yes	Yes	Yes

Smart card removal policy

Now, the Linux VDA uses only the default behavior for smart card removal. When you remove the smart card after logging on to the Linux VDA successfully, the session remains connected and the session screen is not locked.

Support for other smartcards and the PKCS#11 library

Citrix provides a generic smart card redirection solution. Although only the OpenSC smart card is listed on our support list, you can try using other smart cards and the PKCS#11 library. To switch to your specific smart card or the PKCS#11 library:

1. Replace all the `opensc-pkcs11.so` instances with your PKCS#11 library.
2. To set the path of your PKCS#11 library to the registry, run the following command:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
   PKCS11LibPath" -d "PATH"
<!--NeedCopy-->
```

   where **PATH** points to your PKCS#11 library such as /usr/lib64/pkcs11/opensc-pkcs11.so

3. Disable fast smart card logon on the client.

Unauthenticated sessions by anonymous users

January 23, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

> **Note:**
>
> When configuring unauthenticated sessions, consider that session prelaunch is not supported. Session prelaunch is also not supported on Citrix Workspace app for Android.

Create an unauthenticated store

To support an unauthenticated session on the Linux VDA, create an unauthenticated store using StoreFront.

Enable unauthenticated users in a Delivery Group

After creating an unauthenticated store, enable unauthenticated users in a Delivery Group to support an unauthenticated session. To enable unauthenticated users in a Delivery Group, follow the instructions in the Citrix Virtual Apps and Desktops documentation.

Set the unauthenticated session idle time

An unauthenticated session has a default idle timeout 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 five minutes:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v AnonymousUserIdleTime -d 0
    x00000005
<!--NeedCopy-->
```

Set the maximum number of unauthenticated users

To set the maximum number of unauthenticated users, use the registry key **MaxAnonymousUserNumber**. This setting limits the number of unauthenticated sessions running on a single Linux VDA concurrently. Use the **ctxreg** tool to configure this registry setting. For example, to set the value to 32:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
    x00000020
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important:**
>
> Limit the number of unauthenticated sessions. Too many sessions being launched concurrently can cause problems on the VDA, including running out of available memory.

Troubleshooting

Consider the following when configuring unauthenticated sessions:

- **Failed to log on to an unauthenticated session**.

Verify that the registry was updated to include the following (set to 0):

```
sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet
    \Control\Citrix" -v MaxAnonymousUserNumber
<!--NeedCopy-->
```

Verify that the **ncsd** service is running and configured to enable **passwd** cache:

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
<!--NeedCopy-->
```

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 unauthenticated session with KDE**.

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

```
[KDE Action Restrictions]
action/lock_screen=false
<!--NeedCopy-->
```

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, modify the system-wide `kdeglobals` file to remove the `[$i]` 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.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

File

January 23, 2023

This section contains the following topics:

- File copy and paste
- File transfer

File copy and paste

January 23, 2023

Users can copy and paste files between a session and a local client by using the right-click menu or keyboard shortcuts. This feature requires Citrix Virtual Apps and Desktops 2006 or later and Citrix Workspace app 1903 or later for Windows.

To copy and paste files successfully, ensure that:

- The maximum number of files does not exceed 20.
- The maximum file size does not exceed 200 MB.
- The Nautilus file manager is available on the machine where you installed the Linux VDA.

Supported Linux distributions

The **file copy and paste feature** is available for all Linux distributions that the Linux VDA supports.

Relevant policies

The following clipboard policies are relevant to configuring the feature. For more information about the clipboard policies, see Policy support list.

- Client clipboard redirection
- Clipboard selection update mode
- Primary selection update mode

> **Note:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> To disable the file copy and paste feature, set the **Client clipboard redirection** policy to **Prohibited** in Citrix Studio.

Limitations

- Cut is not supported. Requests to cut a file are treated as copy.
- Drag and drop is not supported.
- Copying directories is not supported.
- File copy and paste must be performed sequentially. Only after the previous file is copied and pasted successfully can the next file be copied.

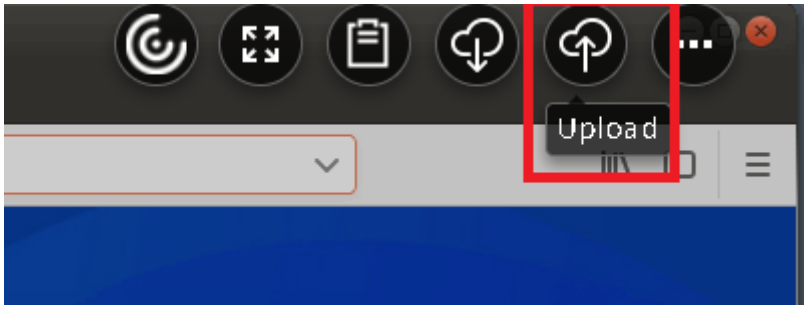
File transfer

January 23, 2023

File transfer is supported between the Linux VDA and the client device. This feature is available when the client device runs a web browser that supports the HTML5 sandbox attribute. The HTML5 sandbox attribute allows users to access virtual desktops and apps using Citrix Workspace app for HTML5 and for Chrome.

> **Note:**
>
> File transfer is available for Citrix Workspace app for HTML5 and for Chrome.

Within published app and desktop sessions, file transfer allows file uploads and downloads between the Linux VDA and the client device. To upload files from the client device to the Linux VDA, click the **Upload** icon on the toolbar of Citrix Workspace app and select the file you want from the file dialogs. To download files from the Linux VDA to the client device, click the **Download** icon. You can add files during uploading or downloading. You can transfer up to 100 files at any one time.



> **Note:**
>
> To upload and download files between the Linux VDA and the client device, enable the toolbar

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> of Citrix Workspace app.
> You can use a version of Citrix Workspace app that lets you drag and drop files.

Autodownload is an enhancement for file transfer. Files you download or move to the **Save to My Device** directory on the VDA are transferred to the client device automatically.

> **Note:**
>
> Autodownload requires the **Allow file transfer between desktop and client** and **Download file from desktop** policies to be set to **Allowed**.

Here are some use cases for auto-download:

- Download files to **Save to My Device**

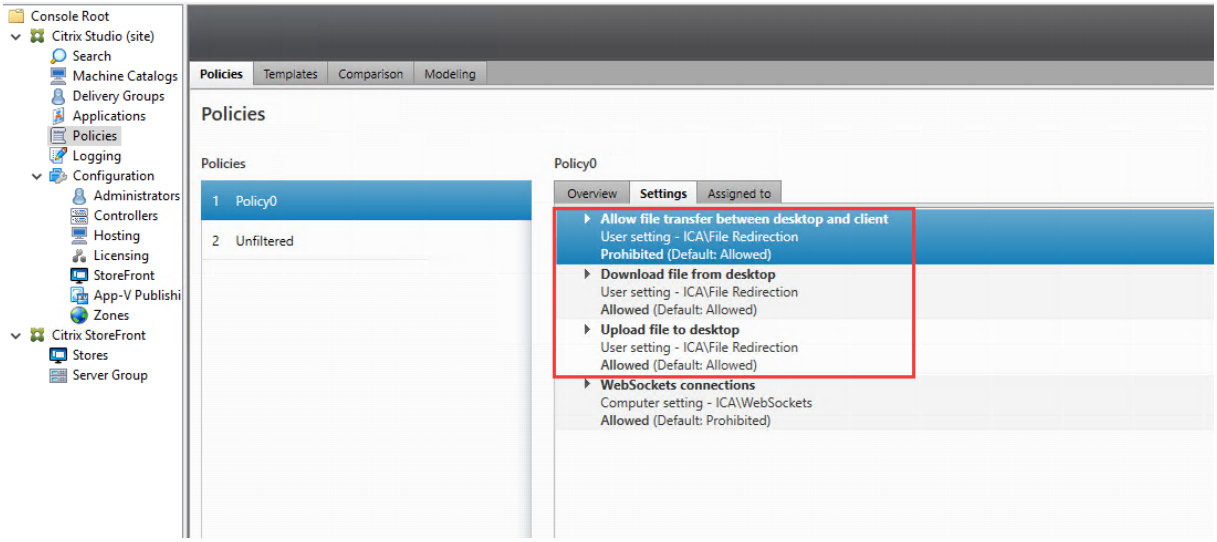
  Within published desktop and web browser app sessions, files you download from websites can be saved to the **Save to My Device** directory on the VDA for automatic transfer to the client device. To achieve auto-download, set the default download directory of the in-session web browser to **Save to My Device** and set a local download directory in the web browser that runs your Citrix Workspace app for HTML5 or for Chrome.

- Move or copy files to **Save to My Device**

  Within published desktop sessions, choose the target files and move or copy them to the **Save to My Device** directory for availability on the client device.

File transfer policies

You can use Citrix Studio to set the file transfer policies. By default, file transfer is enabled.



Policy descriptions:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

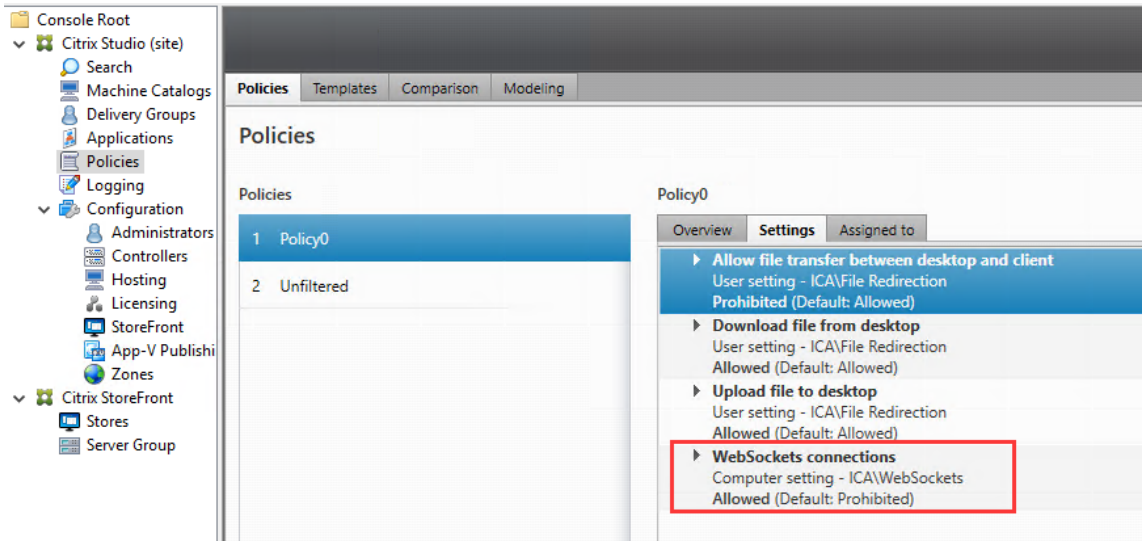
- **Allow file transfer between desktop and client.** Allows or prevents users from transferring files between a Citrix Virtual Apps and Desktops session and their devices.
- **Download file from desktop.** Allows or prevents users from downloading files from a Citrix Virtual Apps and Desktops session to their device.
- **Upload file to desktop.** Allows or prevents users from uploading files from their device to a Citrix Virtual Apps and Desktops session.

> **Note:**
>
> To ensure that the **Download file from desktop** and **Upload file to desktop** policies take effect, set the **Allow file transfer between desktop and client** policy to **Allowed**.

Usage

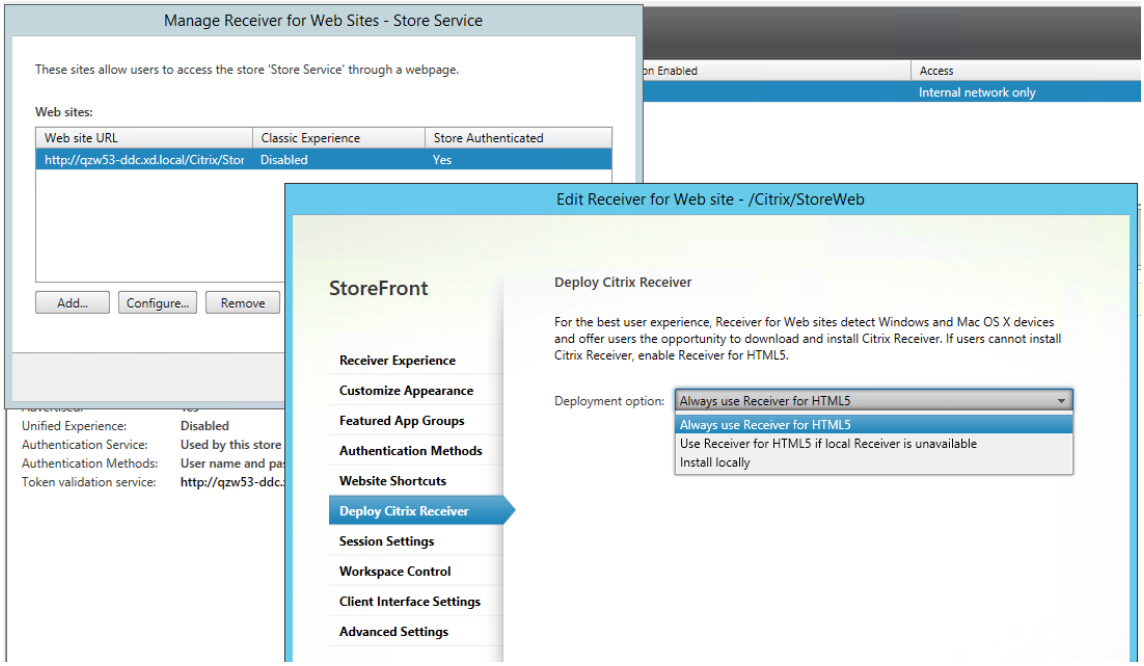
To use the file transfer feature through Citrix Workspace app for HTML5:

1. In Citrix Studio, set the **WebSockets connections** policy to **Allowed**.



2. In Citrix Studio, enable file transfer through the file transfer policies described earlier.
3. In the Citrix StoreFront management console, click **Stores**, select the **Manage Receiver for Web Sites** node, and enable Citrix Receiver for HTML5 by selecting the **Always use Receiver for HTML5** option.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Launch a virtual desktop or web browser app session. Perform one or more file transfers between the Linux VDA and your client device.

To use the file transfer feature through Citrix Workspace app for Chrome:

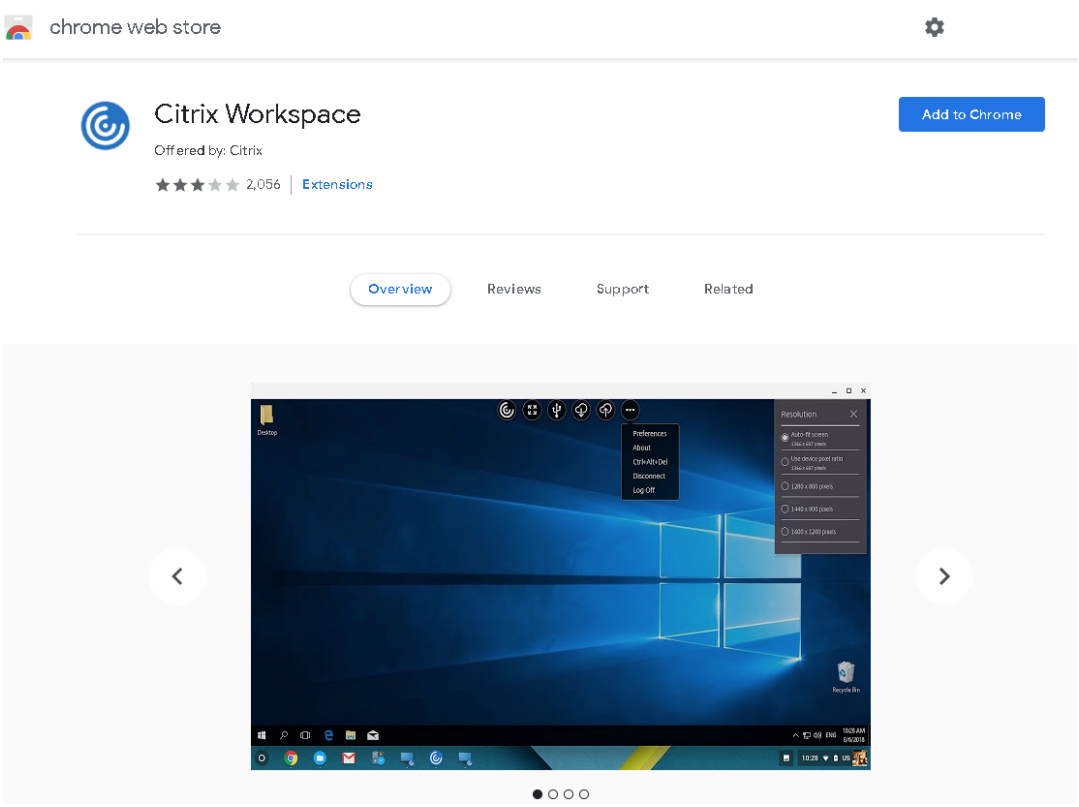
1. Enable file transfer through the file transfer policies described earlier.
2. Obtain Citrix Workspace app from the Chrome Web Store.

   Skip this step if you already added Citrix Workspace app for Chrome to the Chrome Apps page.

   a) Type **Citrix Workspace for Chrome** in the search box of Google Chrome. Click the search icon.

   b) Among the search results, click the URL to the Chrome Web Store where Citrix Workspace app is available.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



c) Click **Add to Chrome** to add Citrix Workspace app to Google Chrome.

3. Click Citrix Workspace app for Chrome on the Chrome Apps page.
4. Type the URL of your StoreFront store to connect.

   Skip this step if you typed the URL before.
5. Launch a virtual desktop or app session. Perform one or more file transfers between the Linux VDA and your client device.

Graphics

February 1, 2023

This section contains the following topics:

- Automatic DPI scaling
- Client battery status display
- Graphics configuration and fine-tuning
- HDX screen sharing

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Non-virtualized GPUs
- Session watermark
- Thinwire progressive display

Automatic DPI scaling

January 23, 2023

The Linux VDA supports automatic DPI scaling. When a user opens a virtual desktop or application session, the DPI value in the session automatically changes to match the DPI setting on the client side.

The following are considerations related to this feature:

- The feature requires that you enable DPI matching for Citrix Workspace. In the case of Citrix Workspace app for Windows, make sure that the **No, use the native resolution** option is selected. For more information about configuring DPI scaling for Citrix Workspace app for Windows, see DPI scaling.
- For the feature to work in multi-monitor scenarios, each monitor must be configured with the same DPI setting. Mixed DPI scenarios are not supported. If monitors are configured with different DPI settings, the Linux VDA applies the smallest DPI value for all screens.
- The feature is enabled for MATE, GNOME, GNOME Classic, and KDE. When using KDE or MATE, consider the following:
  - For Linux virtual desktops running in a KDE desktop environment:
    - We recommend using KDE Plasma 5 or later.
    - Changing DPI settings on the client side while sessions are running requires users to log off and log back on.
  - For Linux virtual desktops running in a MATE desktop environment:
    - Only scale factors of 1 and 2 are supported.
    - Changing DPI settings on the client side while sessions are running requires users to log off and log back on.
- The DPI value in the virtual session automatically changes according to the DPI setting on the client side. Currently, the feature supports only scale factors of type integer, for example, 100% and 200%. If the scale factor configured on the client side is of type fractional, the virtual session DPI changes to an integer scale factor according to the following table. Example: If the scale factor is 125%, the DPI value changes to 100%.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Client-side scale factor	Remote session DPI
Less than or equal to 174%	96 (1 x 96)
175%–274%	192 (2 x 96)
275%–399%	288 (3 x 96)
Greater than or equal to 400%	384 (4 x 96)

Client battery status display

January 23, 2023

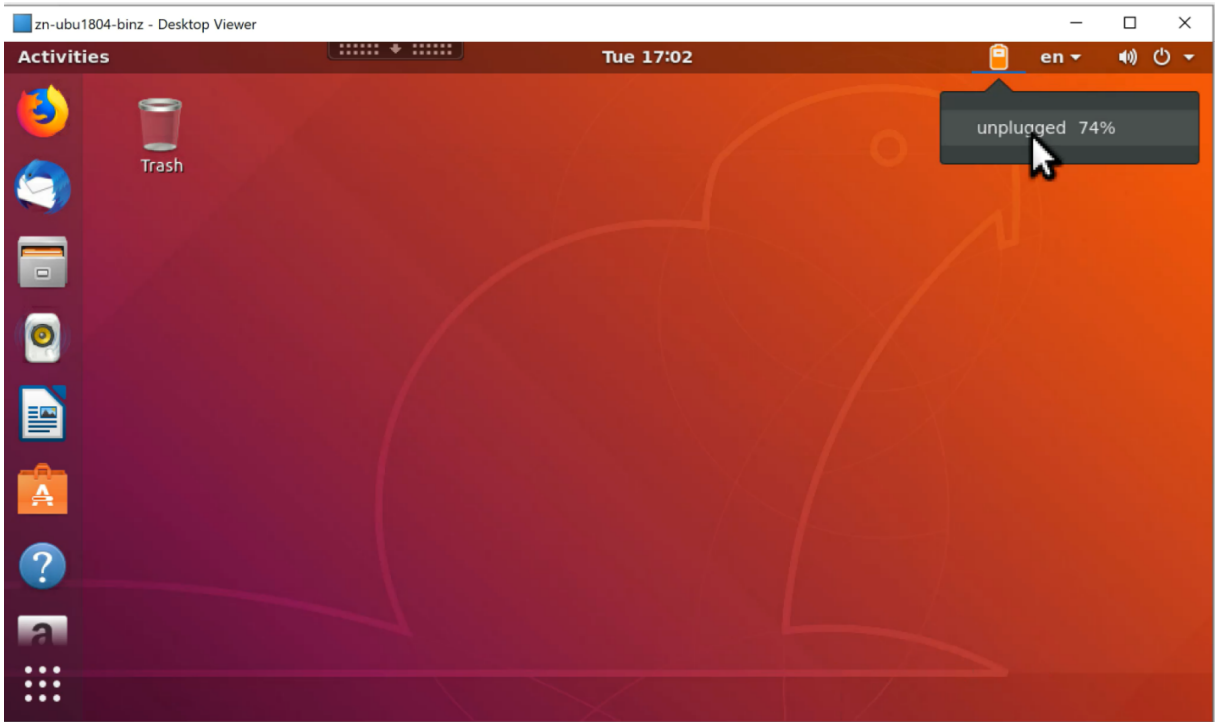
The Linux VDA can redirect and display the battery status of client devices in virtual desktops. This feature is enabled by default and available for the following versions of Citrix Workspace app:

- Citrix Workspace app for iOS
- Citrix Workspace app for Linux
- Citrix Workspace app for Mac (version 2204.1 is not supported)
- Citrix Workspace app for Windows (version 2204.1 is not supported)

Overview

When users open a virtual desktop, they can see a battery icon in the Linux system tray. The battery icon indicates the battery status of their client devices. To check for the percentage of remaining battery life, click the battery icon. For example, see the following screen capture:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Different battery icons indicate different battery statuses. For an overview, see the following table:

Battery icon	Charging status	Level of remaining battery life	Percentage of remaining battery life
	Charging, indicated with a “+”symbol	High, indicated with a green color	=80%
	Charging, indicated with a “+”symbol	Medium, indicated with an amber color	=20% and <80%
	Charging, indicated with a “+”symbol	Low, indicated with a red color	< 20%
	Not charging, indicated with a “-“symbol	High, indicated with a green color	=80%
	Not charging, indicated with a “-“symbol	Medium, indicated with an amber color	=20% and <80%

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Battery icon	Charging status	Level of remaining battery life	Percentage of remaining battery life
	Not charging, indicated with a "-"symbol	Low, indicated with a red color	< 20%
	Unknown	Unknown	Unknown

Configuration

Client battery status display is enabled by default.

To disable the feature, run the following command:

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

To enable the feature, run the following command:

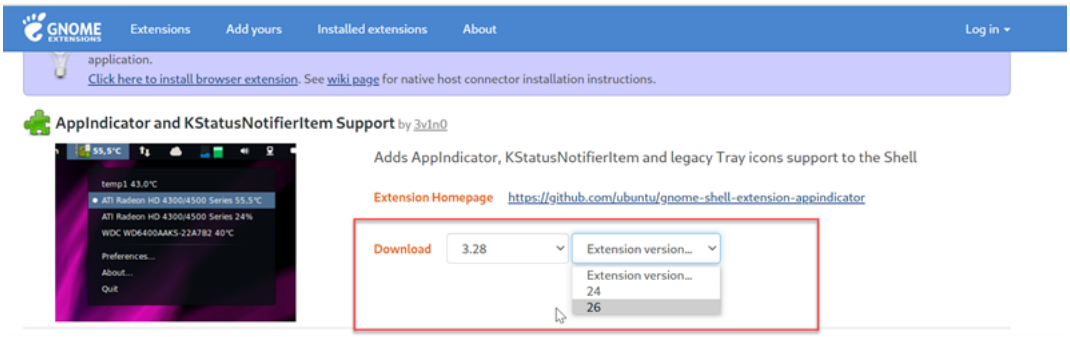
```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
   Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000001"
<!--NeedCopy-->
```

> **Note:**
>
> The preceding commands impact the soft keyboard feature, which shares the Mobile Receiver Virtual Channel (MRVC) with client battery status display.

Based on your distribution, complete the following extra steps:

1. If you are using RHEL 8.x or SUSE 15.x installed with GNOME, install a compatible extension for your GNOME shell to enable AppIndicator support:
   a) Run the `gnome-shell --version` command to check your GNOME shell version.
   b) Download a compatible extension for your GNOME shell from https://extensions.gnome.org/extension/615/appindicator-support. For example, if your shell version is 3.28, you can select 24 or 26 for the extension version.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



c) Untar the downloaded package. Verify that the **"uuid"** value in the **metadata.json** file in the package is set to **appindicatorsupport@rgcjonas.gmail.com**.

d) Run the `mv` command to move the **appindicatorsupport@rgcjonas.gmail.com** directory to the location under `/usr/share/gnome-shell/extensions/`.

e) Run the `chmod a+r metadata.json` command to make the **metadata.json** file readable to other users.

> **Tip:**
>
> By default, the **metadata.json** file in the **appindicatorsupport@rgcjonas.gmail.com** directory is readable only to the root user. To support screen sharing, make the **metadata.json** file readable to other users as well.

f) Install GNOME Tweaks.

g) In the desktop environment, reload your GNOME shell by pressing the `Alt+F2`, `r`, and `Enter` keys in sequence or by running the `killall -SIGQUIT gnome-shell` command.

h) In the desktop environment, run GNOME Tweaks and then enable **KStatusNotifierItem/AppIndicator Support** in the Tweaks tool.

2. If you are using Debian 11.3 installed with GNOME, complete the following steps to install and enable GNOME system tray icons:

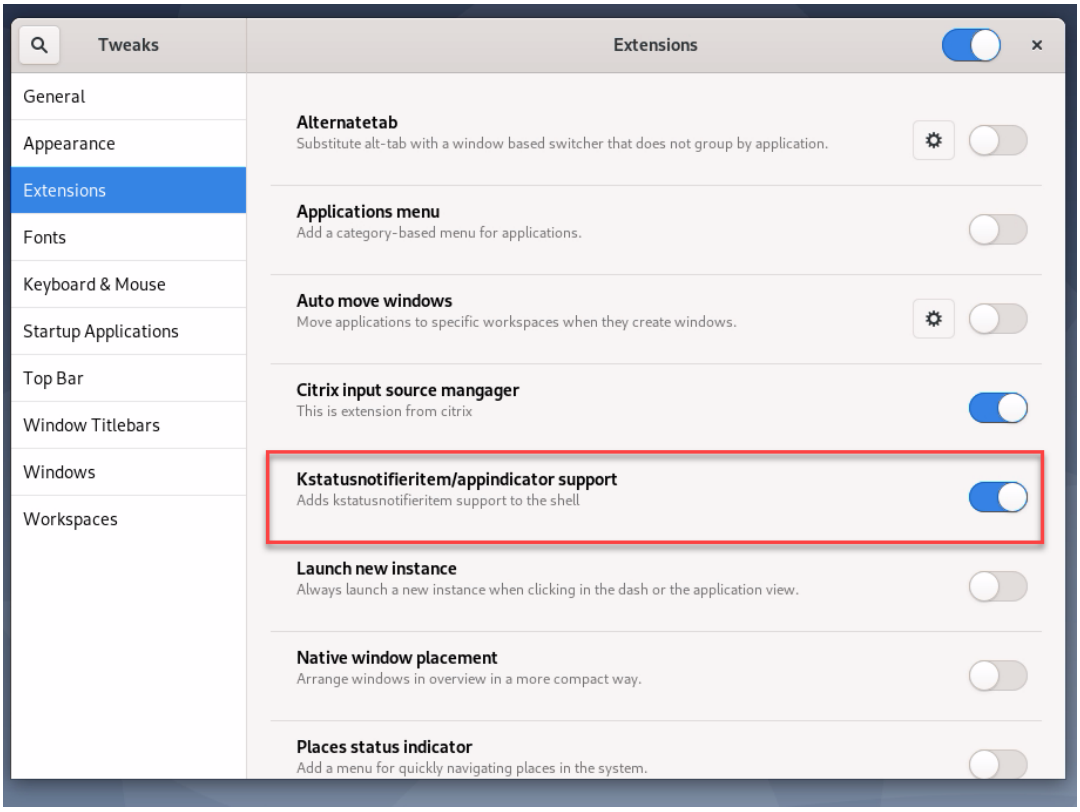
a) Run the `sudo apt install gnome-shell-extension-appindicator` command. You might have to log out and then back in again for GNOME to see the extension.

b) Search for Tweaks in your **Activities** screen.

c) Select **Extensions** in the Tweaks tool.

d) Enable **Kstatusnotifieritem/appindicator support**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Graphics configuration and fine-tuning

February 21, 2023

This article provides guidance for the Linux VDA graphics configuration and fine-tuning.

For more information, see System requirements and the Installation overview section.

Configuration

Optimize for 3D graphics workload

This setting configures the appropriate default values that best suit graphics-intensive workloads. Enable this setting for users whose workload focuses on graphics-intensive applications. Apply this policy only in cases where a GPU is available to the session. Any other settings that explicitly override the default settings set by this policy take precedence.

By default, **Optimize for 3D graphics workload** is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

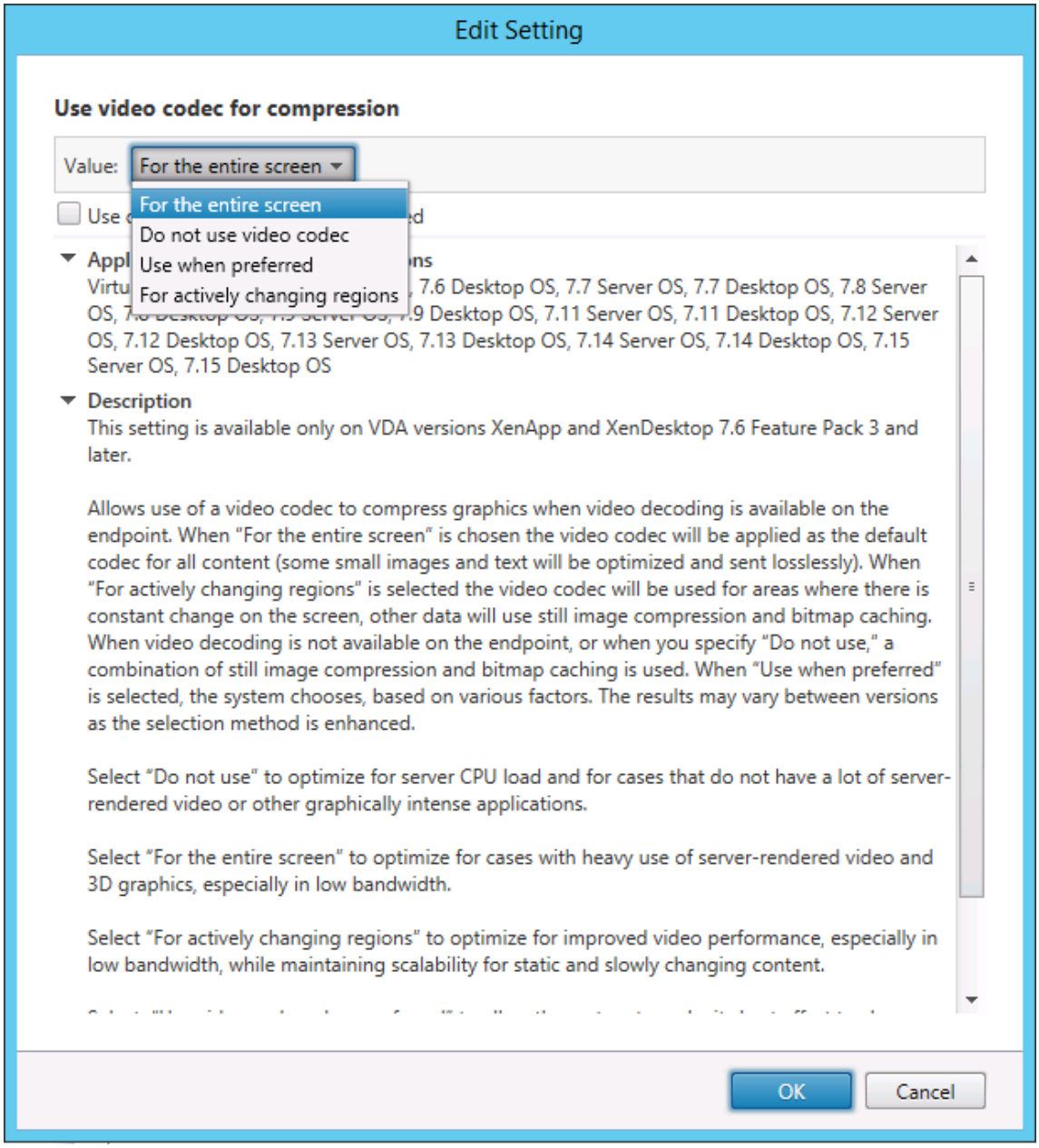
Video codec for compression

Thinwire is the display remoting technology used in the Linux VDA. The technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display.

The **Use video codec for compression** graphics policy sets the default graphics mode and provides the following options for different use cases:

- **Use when preferred**. This setting is the default. No additional configuration is required. It ensures that Thinwire is selected for all Citrix connections, and optimized for scalability, bandwidth, and superior image quality for typical desktop workloads.
- **For the entire screen**. Delivers Thinwire with full-screen H.264 or H.265 to optimize for improved user experience and bandwidth, especially in cases with heavy use of 3D graphics. Session watermark is supported when **For the entire screen** is selected, or when **Use when preferred** is selected and Optimize for 3D graphics workload is enabled.
- **For actively changing regions**. The adaptive display technology in Thinwire identifies moving images (video, 3D in motion). It uses H.264 only in the part of the screen where the image is moving. The selective use of the H.264 video codec enables HDX Thinwire to detect and encode parts of the screen that are frequently updated using the H.264 video codec. Still image compression (JPEG, RLE) and bitmap caching continue to be used for the rest of the screen, including text and photographic imagery. Users get the benefit of lower bandwidth consumption and better quality for video content combined with lossless text or high quality imagery elsewhere. To enable this feature, set the **Use video codec for compression** policy to **Use when preferred** (default) or **For actively changing regions**. For more information, see Graphics policy settings.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Some other policy settings, including the following visual display policy settings can be used to fine-tune the performance of display remoting:

- **Preferred color depth for simple graphics**
- **Target frame rate**
- **Visual quality**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

H.264 hardware encoding

The **Use hardware encoding for video codec** policy allows the use of GPU hardware acceleration, if available, to compress screen elements with the video codec. If GPU hardware is not available, the VDA falls back to CPU-based encoding using the software video codec.

GPU hardware acceleration optimizes hardware resource utilization and highly improves the performance of frames per second (FPS).

Starting with Version 2210, GPU hardware acceleration covers the following graphics modes:

- Use when preferred
- For the entire screen
- For actively changing regions

Allow visually lossless compression

The **Allow visually lossless compression** policy allows visually lossless compression to be used instead of true lossless compression for graphics. Visually lossless improves performance over true lossless, but has minor loss that is unnoticeable by sight. This setting changes the way the values of the **Visual quality** setting are used.

The **Allow visually lossless compression** policy is disabled by default. To enable visually lossless compression, set **Allow visually lossless compression** to **Enabled** and the **Visual quality** policy to **Build to Lossless**.

If the **Use video codec for compression** policy is set to **Do not use video codec**, visually lossless compression applies to static image encoding. If the **Use video codec for compression** policy is set to a graphics mode other than **Do not use video codec**, visually lossless compression applies to H.264 encoding.

The following clients support Selective H.264:

- Citrix Receiver for Windows 4.9 through 4.12
- Citrix Receiver for Linux 13.5 through 13.10
- Citrix Workspace app 1808 for Windows and later
- Citrix Workspace app 1808 for Linux and later

For more information about the **Visual quality** and **Use video codec for compression** policy settings, see Visual display policy settings and Graphics policy settings.

Support for H.265 video codec

Starting with the 7.18 release, the Linux VDA supports the H.265 video codec for hardware acceleration of remote graphics and videos.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

You can use this feature on:

- Citrix Receiver for Windows 4.10 through 4.12
- Citrix Workspace app 1808 for Windows and later

To benefit from this feature, enable it on both the Linux VDA and on your client. If the GPU of your client doesn't support H.265 decoding using the DXVA interface, the **H.265 decoding for graphics** policy setting is ignored and sessions fall back to using the H.264 video codec. For more information, see H.265 video encoding.

To enable H.265 hardware encoding on the VDA:

1. Enable the **Use hardware encoding for video codec** policy.
2. Enable the **Optimize for 3D graphics workload** policy
3. Ensure that the **Use video codec for compression** policy is default or set to **For the entire screen**.
4. Ensure that the **Visual quality** policy is **NOT** set to **Build to Lossless** or **Always Lossless**.

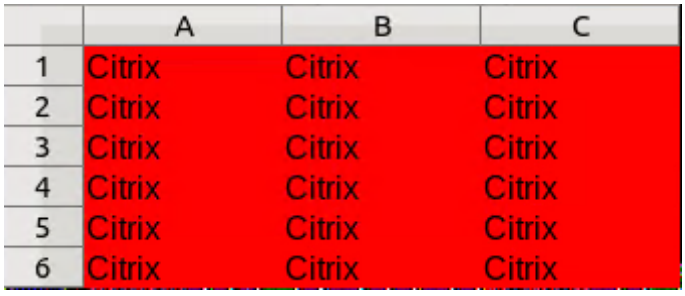
To enable H.265 hardware encoding on your client, see H.265 video encoding.

Support for YUV444 software encoding

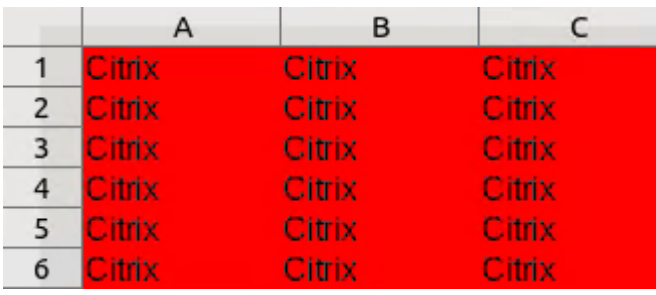
The Linux VDA supports YUV444 software encoding. The YUV encoding scheme assigns both brightness and color values to each pixel. In YUV, 'Y'represents the brightness or 'luma'value, and 'UV' represents the color or 'chroma'values. You can use this feature on Citrix Receiver for Windows 4.10 through 4.12 and on Citrix Workspace app 1808 for Windows and later.

Each unique Y, U, or V value comprises 8 bits, or one byte, of data. The YUV444 data format transmits 24 bits per pixel. The YUV422 data format shares U and V values between two pixels, which results in an average transmission rate of 16 bits per pixel. The following table shows an intuitive comparison between YUV444 and YUV420.

YUV444	YUV420



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



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

To enable YUV444 software encoding on the VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

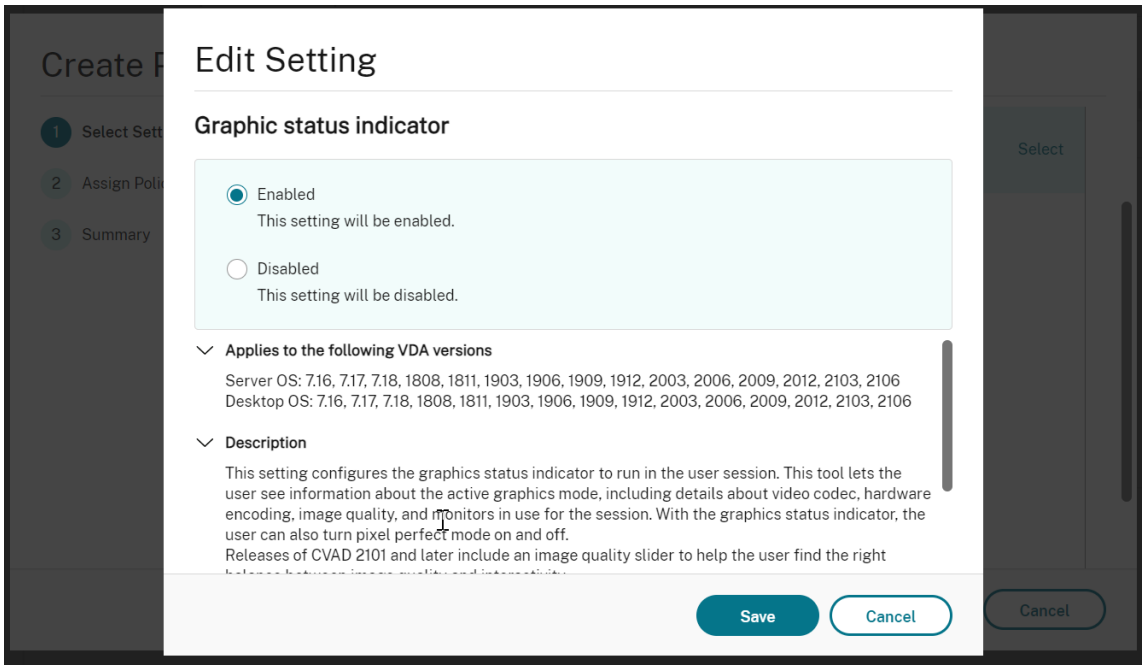
1. Ensure that the **Use video codec for compression** policy is set to **For the entire screen**.
2. Ensure that the **Visual quality** policy is set to **Always Lossless** or **Build to Lossless**.

Graphics quality slider

We have included a graphics quality slider in the graphics status indicator tool that runs in your virtual Linux sessions. The slider helps to find the right balance between image quality and interactivity.

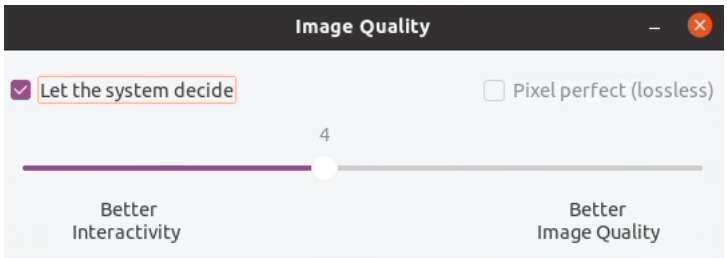
To use the slider, complete the following steps:

1. Enable the **Graphic status indicator** policy in Citrix Studio.



2. Open the Terminal and run the `ctxslider` command. The slider UI appears.

> **Note:**
>
> If you have set the **Visual Quality** policy to **Always Lossless** or **Build to Lossless**, the slider UI is not showing.



The following choices are now available:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- To change the image quality, move the slider. The slider supports a range of 0–9.
- To use system-defined settings, select **Let the system decide**.
- To switch to lossless mode, select **Pixel perfect**.

Adjust average bit rates based on bandwidth estimates

Citrix enhances HDX 3D Pro hardware encoding by adjusting average bit rates based on bandwidth estimates.

When HDX 3D Pro hardware encoding is in use, the VDA can intermittently estimate the bandwidth of the network and adjust the bit rates of encoded frames accordingly. This new feature provides a mechanism to balance between sharpness and fluency.

This feature is enabled by default. To disable it, run the following command:

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

In addition to using this feature, you can also run the following commands to adjust between sharpness and fluency. The **AverageBitRatePercent** and **MaxBitRatePercent** parameters set the percentage of bandwidth usage. The higher values you set, the sharper graphics and lower fluency you get. The recommended setting range is 50–100.

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

In the average bit rate adjustment, when your screen holds still, the most recent frame stays in a low-quality state because no new frames are sent. Sharpening support can address this issue by reconfiguring and immediately sending the most recent frame at the highest quality.

For a full list of the policies supported by the Linux VDA Thinwire, see Policy support list.

For information on the configuration of multi-monitor support on the Linux VDA, see CTX220128.

Parallel processing

Thinwire can improve the number of Frames Per Second (FPS) by parallelizing certain tasks, with the overhead of slightly higher overall CPU consumption. This feature is disabled by default. To enable the feature, run the following command on your VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ParallelProcessing" -d "0x00000001" --force
<!--NeedCopy-->
```

Troubleshooting

Check which graphics mode is in use

Run the following command to check which graphics mode is in use (**0** means TW+. **1** means full-screen video codec):

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

The result resembles:

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

Verify that H.264 is in use

Run the following command to verify that H.264 is in use (**0** means not in use. **1** means in use):

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

For example, the result can resemble:

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

Verify that H.265 is in use

Run the following command to verify that full-screen H.265 is in use (**0** means not in use. **1** means in use):

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

For example, the result can resemble:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Check which YUV encoding scheme is in use

Run the following command to check which YUV encoding scheme is in use (**0** means YUV420. **1** means YUV422. **2** means YUV444):

> **Note:**
>
> The value of **YUVFormat** is meaningful only when a video codec is in use.

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

For example, the result can resemble:

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

Verify that YUV444 software encoding is in use

Run the following command to verify that YUV444 software encoding is in use:

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

When YUV444 is in use, the result resembles:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000001"--force

create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force

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

create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000002"--force
```

Verify that HDX 3D Pro is enabled

Run the following commands to verify that HDX 3D Pro is enabled:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep ProductEdition

sudo /opt/Citrix/VDA/bin/ctxreg dump | grep StackSessionMode

sudo /opt/Citrix/VDA/bin/ctxreg dump | grep 3DPro
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

When HDX 3D Pro is enabled, the result resembles:

```
create -k "HKLM\Software\Citrix\VirtualDesktopAgent\State"-t "REG_SZ"
-v "ProductEdition"-d "<PLT or ENT>"--force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\
tcp"-t "REG_DWORD"-v "StackSessionMode"-d "0x00000000"--force

create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD
"-v "3DPro"-d "0x00000000"--force
```

To verify that the required NVIDIA libraries are loaded for HDX 3D Pro, run the **nvidia-smi** command on the Linux VDA. The result resembles:

```
Tue Apr 12 10:42:03 2016
+-----------------------------------------------------+
| NVIDIA-SMI 361.28     Driver Version: 361.28         |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
                     N/A |
| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
   Default |
+-------------------------------+----------------------+----------------------+


+-----------------------------------------------------------------------------+

| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|

|    0      2164  C+G   /usr/local/bin/ctxgfx
   106MiB |
|    0      2187    G   Xorg
    85MiB |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Verify that hardware encoding is in use for 3D Pro

Run the following command (**0** means not in use. **1** means in use):

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

When 3D Pro is in use, the result resembles:

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

Verify that the NVIDIA GRID graphics driver is installed correctly

To verify that the NVIDIA GRID graphics driver is installed correctly, run **nvidia-smi**. The result resembles:

```
+-----------------------------------------------------+
| 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
                                 |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Set the correct configuration for the card:

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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.

Known issues and limitations

For vGPU, the Citrix Hypervisor local console shows the ICA desktop session screen

Workaround: Disable the VM's local VGA console by running the following commands:

For Citrix Hypervisor 8.1 and later:

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

For Citrix Hypervisor earlier than 8.1:

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

Gnome 3 desktop popups slow when logging on

It is a limitation of Gnome 3 desktop session startup.

Some OpenGL/WebGL applications do not render well upon resizing the Citrix Workspace app window

Resizing the window of Citrix Workspace app changes the 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** might spawn an error saying that 'Rendering to **this** texture is not supported (incomplete frame buffer)'.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX screen sharing

January 23, 2023

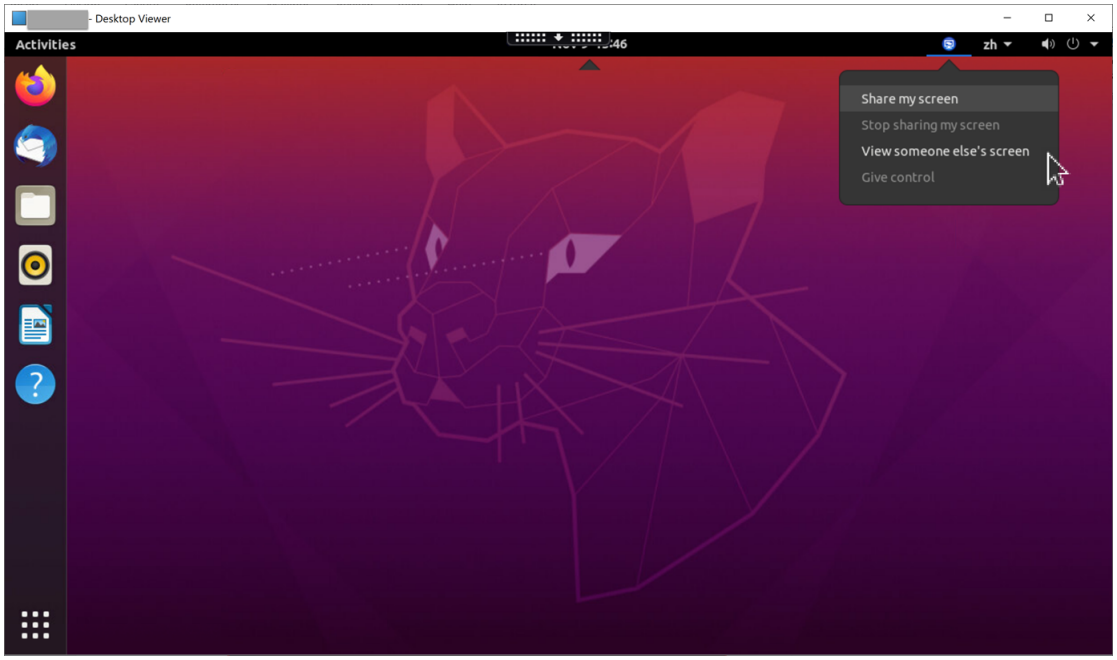
Overview

The Linux VDA lets you share the screen of your virtual desktop with session users on other virtual desktops.

The following example walks you through the procedure of sharing a screen and viewing some else's screen.

To share a screen:

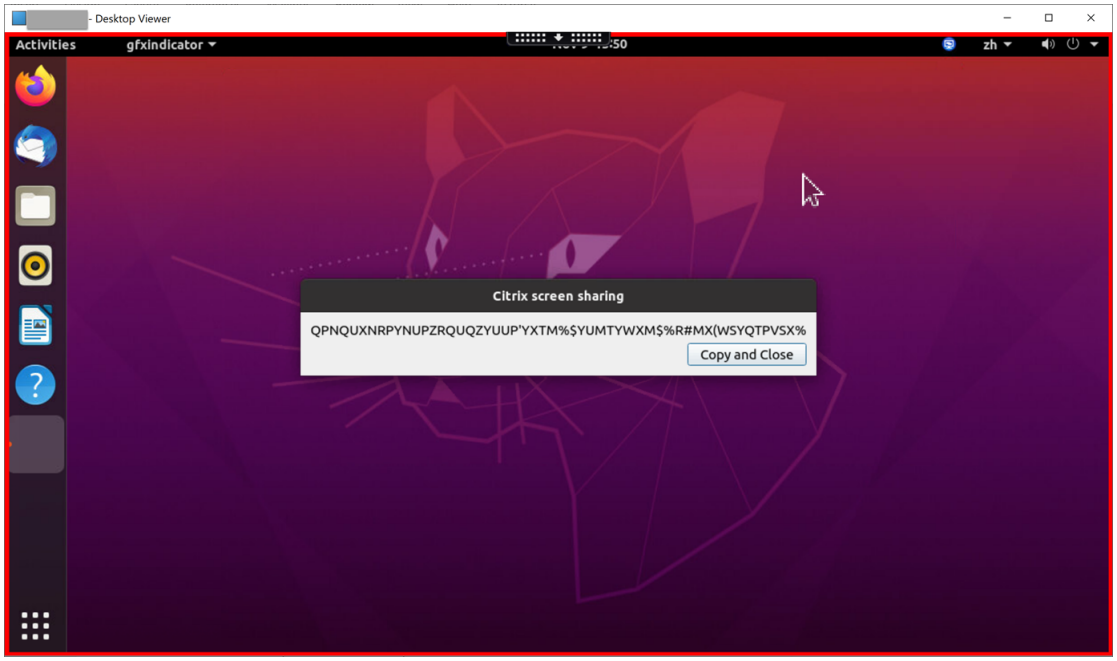
1. In the notification area of your virtual desktop, click the **screen sharing** icon and select **Share my screen**.



2. Click **Copy and Close**.

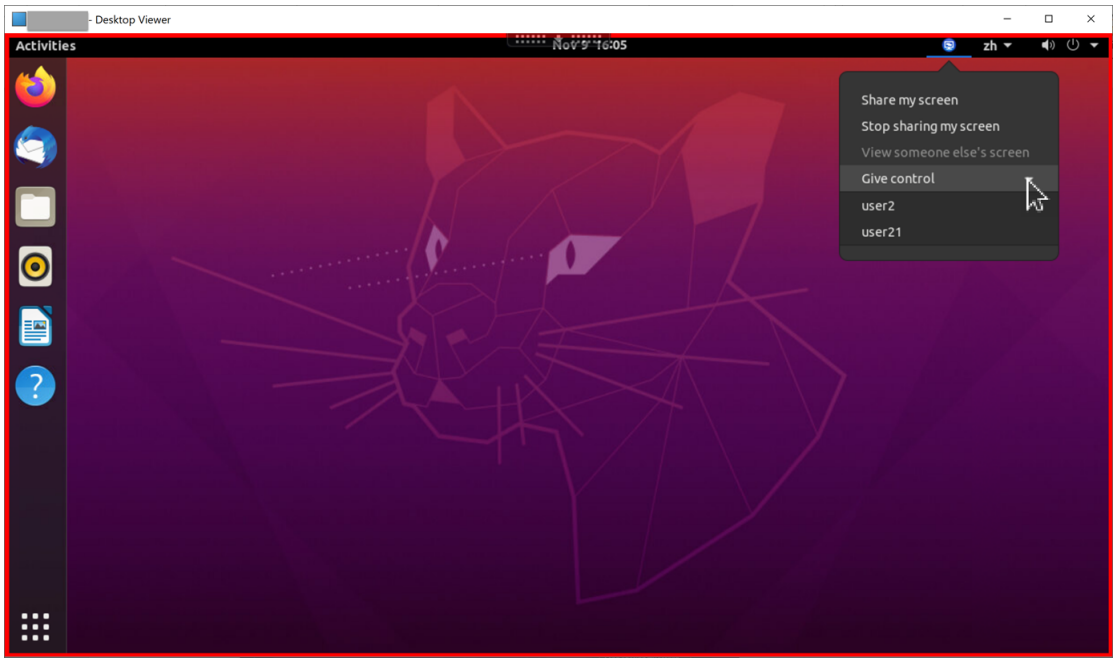
   The current screen sharing code persists until you stop and restart sharing your screen.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



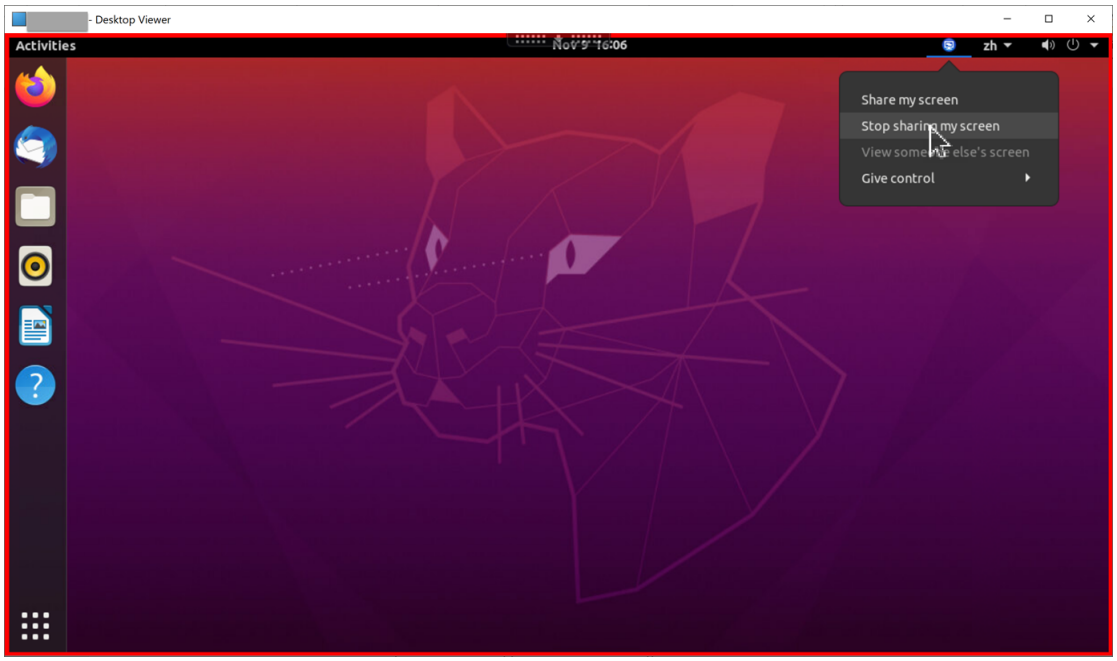
> **Tip:**
>
> While you are sharing your screen, there is a red border around it, indicating that sharing is in progress.

3. Share the copied code with session users on other virtual desktops that you want to share your screen with.
4. To let a viewer control your screen, select **Give control** and then the viewer's name. To stop giving control, clear the viewer's name.



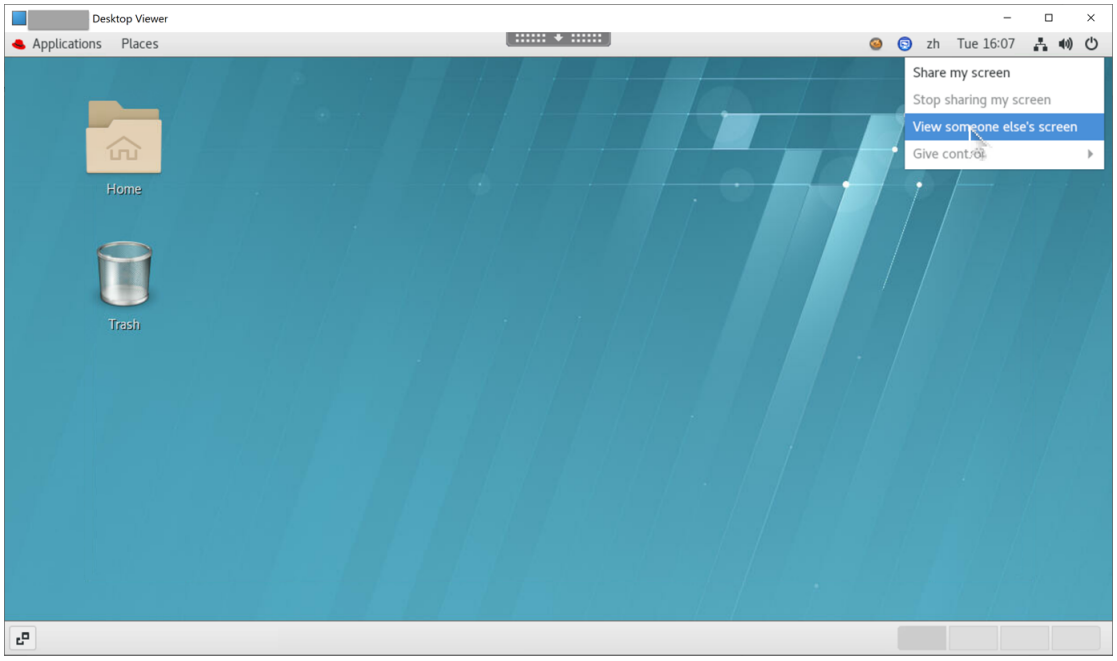
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. To stop sharing your screen, select **Stop sharing my screen**.



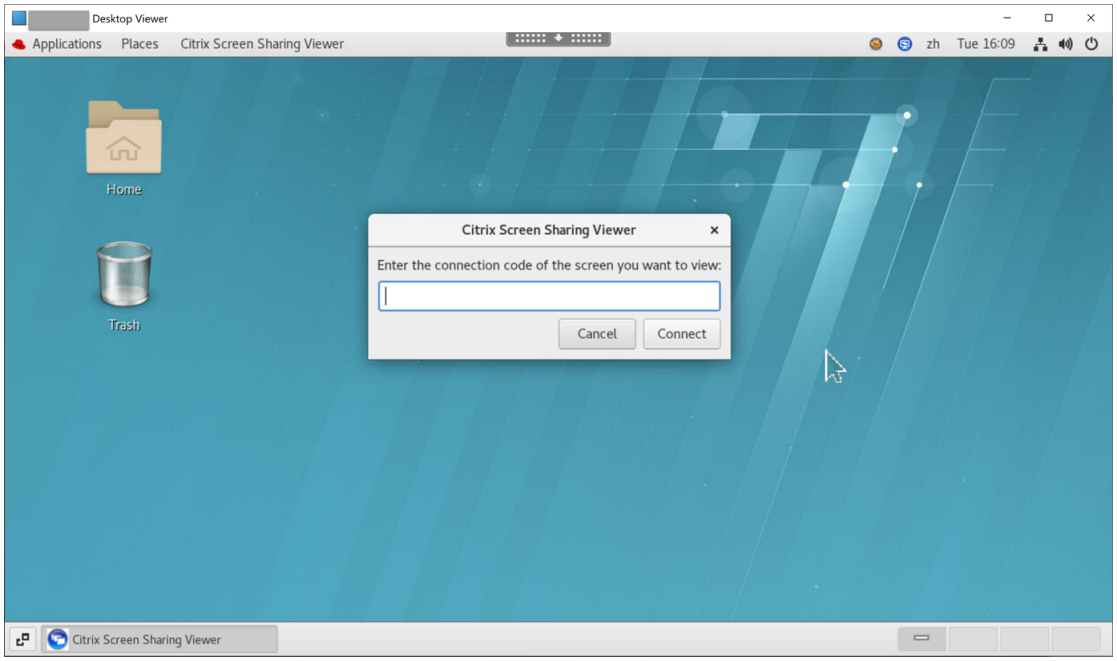
To view someone else's screen:

1. In the notification area of your virtual desktop, click the **screen sharing** icon and select **View someone else's screen**.

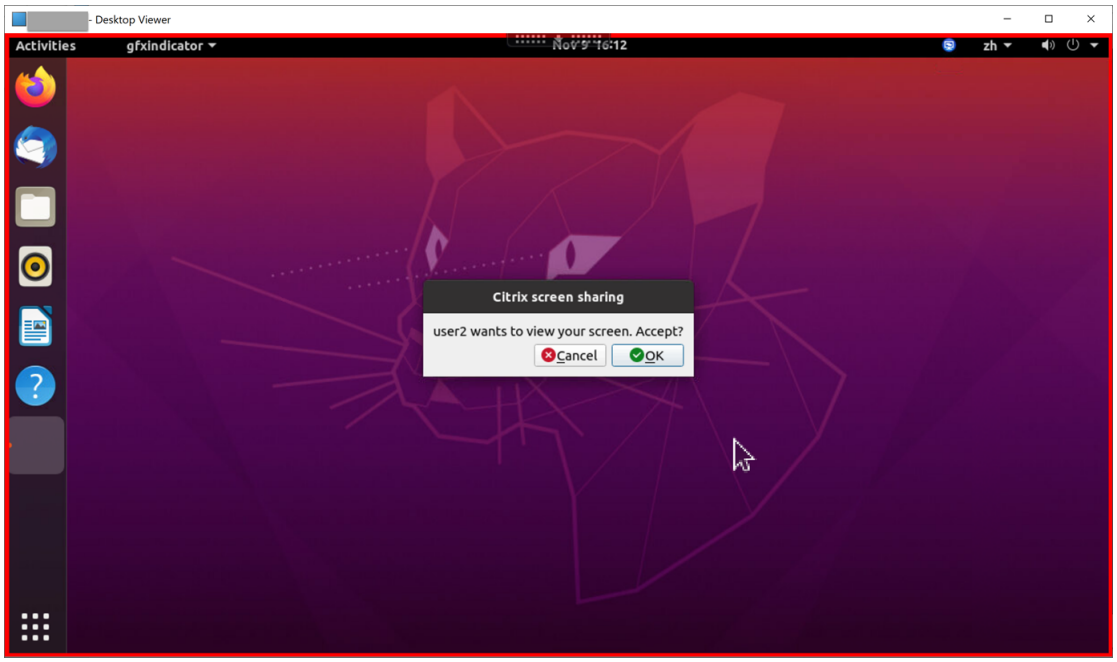


2. Enter the connection code of the screen that you want to view and then click **Connect**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



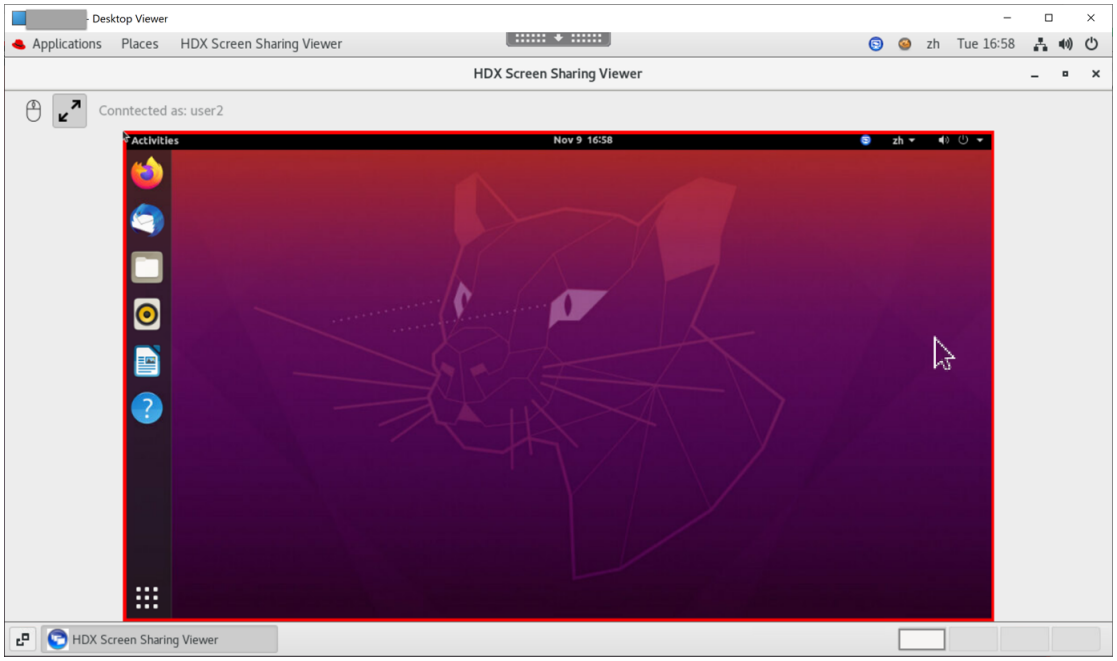
3. Wait for the screen sharer to accept your request. For example:



> **Tip:**
>
> - On the sharer side, the Linux system issues a notification of your request.
> - If the sharer does not accept your request within 30 seconds, your request expires and a prompt appears.

4. After the screen sharer accepts your request by clicking **OK**, the shared screen appears in your Desktop Viewer. You are connected as a viewer with an automatically assigned user name.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

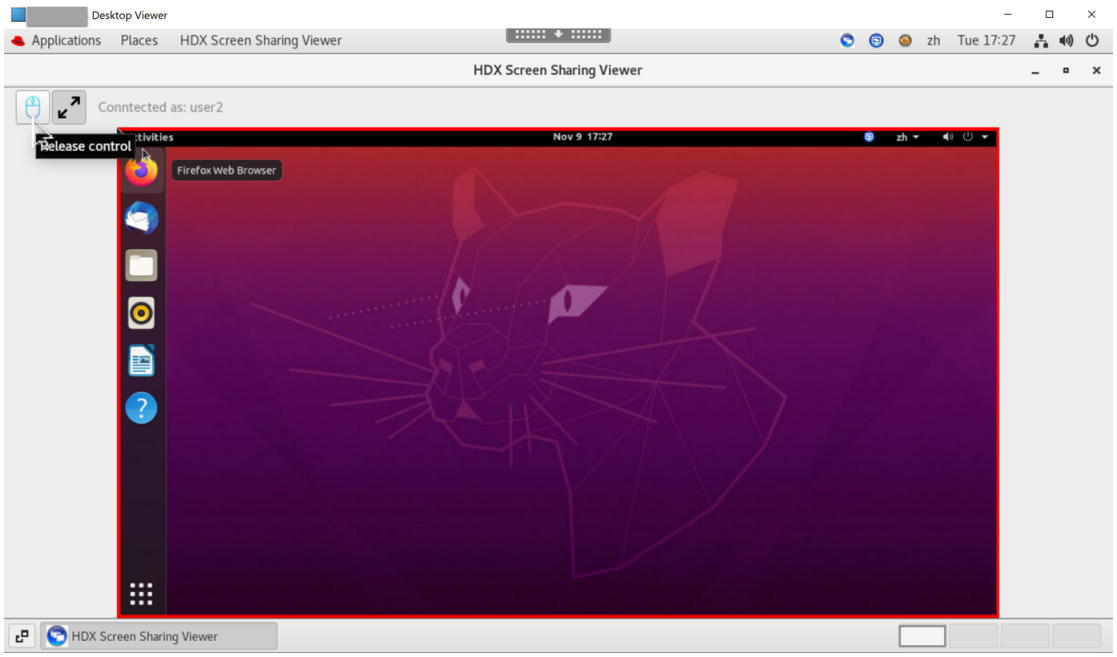


5. To request control over the shared screen, click the mouse icon in the upper left corner.

   Tip:

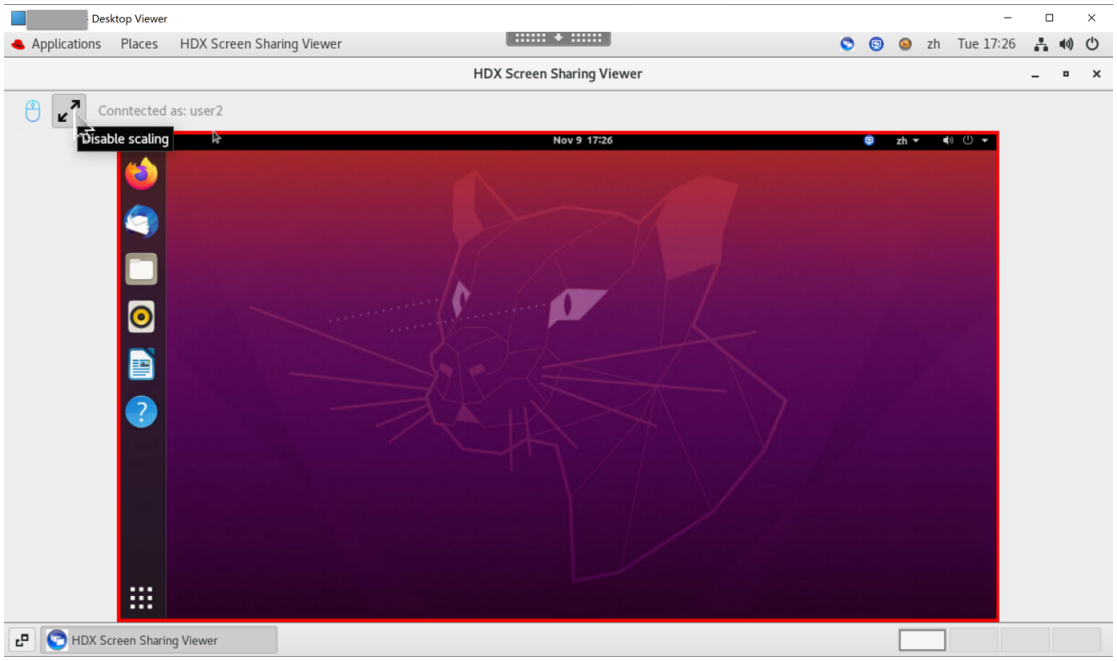
   - If the sharer does not accept your request within 30 seconds, your request expires.
   - Only one viewer is allowed to control a shared screen at a time.

   Click the mouse icon again to release control over the shared screen.



6. To disable display scaling or scale to the window size, click the icon next to the mouse icon.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Configuration

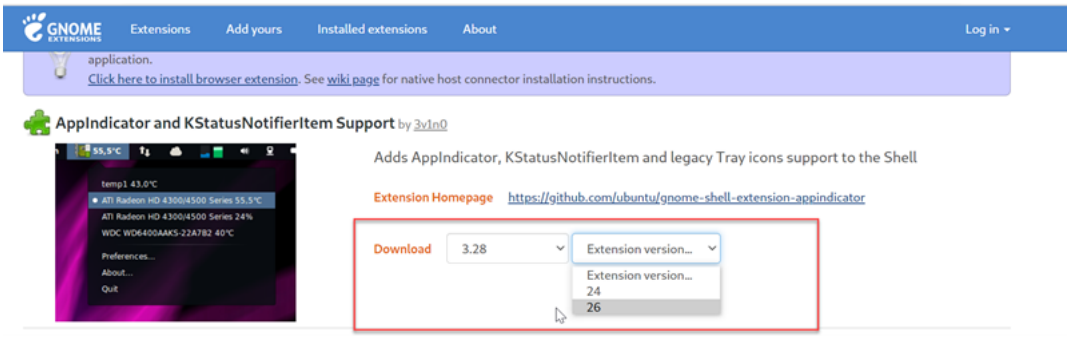
The screen sharing feature is disabled by default. To enable it, complete the following settings:

1. Enable the graphics status indicator policy in Citrix Studio.
2. For Citrix Virtual Apps and Desktops 2112 and later, enable the **ScreenSharing** policy in Citrix Studio.
3. (Optional) For Citrix Virtual Apps and Desktops 2109 and earlier, enable screen sharing on the Linux VDA by running the following command:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Thinwire" -v "
    EnableScreenSharing" -d "0x00000001"
<!--NeedCopy-->
```

4. Allow ports 52525–52625 in your firewall.
5. (Optional) If you are using RHEL 8.x, Debian 11, or SUSE 15.x installed with GNOME, install a compatible extension for your GNOME shell to enable AppIndicator support:
   a) Run the `gnome-shell --version` command to check your GNOME shell version.
   b) Download a compatible extension for your GNOME shell from https://extensions.gnome.org/extension/615/appindicator-support. For example, if your shell version is 3.28, you can select 24 or 26 for the extension version.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



c) Untar the downloaded package. Verify that the **"uuid"** value in the **metadata.json** file in the package is set to **appindicatorsupport@rgcjonas.gmail.com**.

d) Run the `mv` command to move the **appindicatorsupport@rgcjonas.gmail.com** directory to the location under `/usr/share/gnome-shell/extensions/`.

e) Run the `chmod a+r metadata.json` command to make the **metadata.json** file readable to other users.

> **Tip:**
>
> By default, the **metadata.json** file in the **appindicatorsupport@rgcjonas.gmail.com** directory is readable only to the root user. To support screen sharing, make the **metadata.json** file readable to other users as well.

f) Install GNOME Tweaks.

g) In the desktop environment, reload your GNOME shell by pressing the `Alt+F2`, `r`, and `Enter` keys in sequence or by running the `killall -SIGQUIT gnome-shell` command.

h) In the desktop environment, run GNOME Tweaks and then enable **KStatusNotifierItem/AppIndicator Support** in the Tweaks tool.

6. (Optional) If you are using Debian 11.3 installed with GNOME, complete the following steps to install and enable GNOME system tray icons:

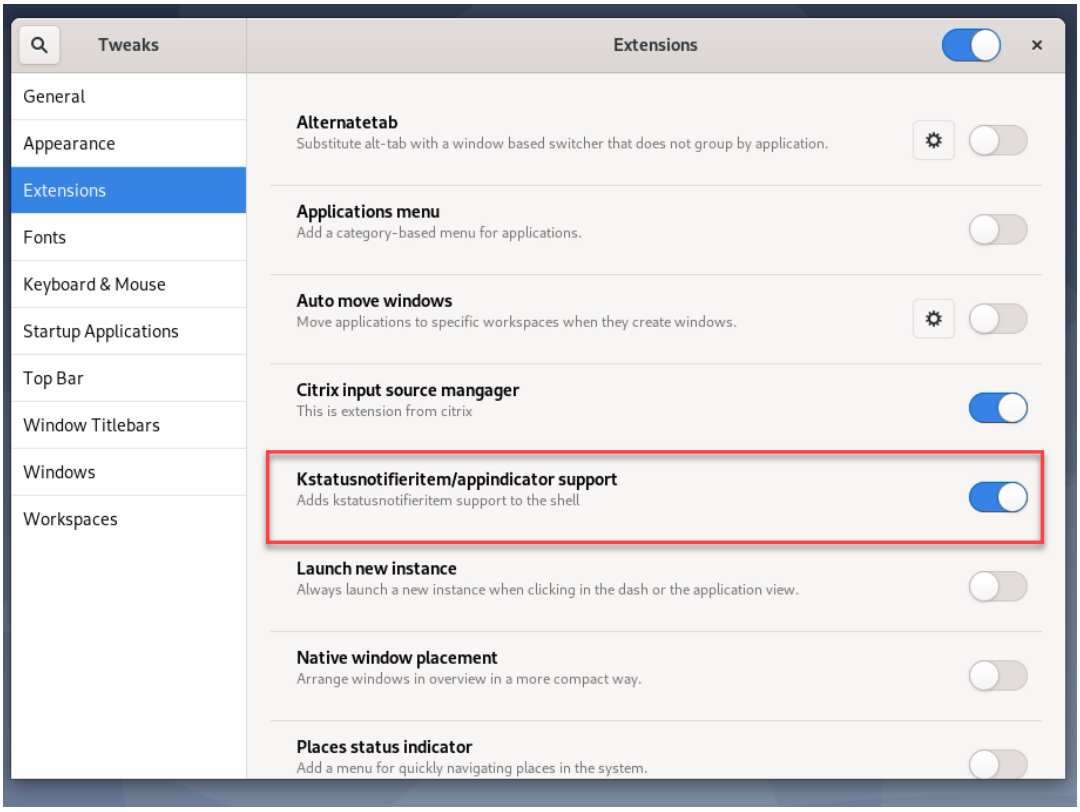
a) Run the `sudo apt install gnome-shell-extension-appindicator` command. You might have to log out and then back in again for GNOME to see the extension.

b) Search for Tweaks in your **Activities** screen.

c) Select **Extensions** in the Tweaks tool.

d) Enable **Kstatusnotifieritem/appindicator support**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Considerations

- The screen sharing feature does not support the H.265 video codec.
- The screen sharing feature is not available for app sessions.
- Users of desktop sessions can share their session screens with up to 10 viewers by default. The maximum number of viewers is configurable through `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-v "ScreenSharingViewerMaxNum"-d <hex_value>`. When the maximum number is reached, a prompt appears when users try to accept extra connection requests.

Non-virtualized GPUs

February 20, 2024

In the Linux VDA documentation, non-virtualized GPUs refers to:

- GPUs used in Remote PC Access scenarios
- GPUs passed through from a hypervisor

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

This article provides information on enabling HDX 3D Pro for non-virtualized GPUs.

Prerequisites

- Enable HDX 3D Pro. To do so, set `CTX_XDL_HDX_3D_PRO` to `Y` when installing the Linux VDA. For information about environment variables, see Step 8: Set up the runtime environment to complete the installation.
- For GPUs that the NVIDIA Linux Capture SDK supports, hardware acceleration is enabled by default after you enable HDX 3D Pro. No additional configuration is required.
- For GPUs that the NVIDIA Linux Capture SDK does not support, install `XDamage`. For example, you can run `sudo apt-get install -y libxdamage1` to install XDamage on Ubuntu 20.04. Typically, XDamage exists as an extension of XServer.

Configuration

Modify Xorg configuration files

For NVIDIA non-virtualized GPUs The configuration files are installed and set automatically.

For other GPUs You must modify the four template configuration files installed under `/etc/X11/`:

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf
- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

Using **ctx-driver_name-1.conf** as an example, do the following to modify the template configuration files:

1. Replace ***driver_name*** with your actual driver name.

   For example, if your driver name is `intel`, you can change the configuration file name to `ctx-intel-1.conf`.

2. Add the video driver information.

   Each template configuration file contains a section named "Device,"which is commented out. This section describes the video driver information. Enable this section before adding your video driver information. To enable this section:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) See the guide provided by the GPU manufacturer for configuration information. A native configuration file can be generated. Verify that your GPU can work in a local environment with the native configuration file.

b) Copy the "Device"section of the native configuration file to **ctx-driver_name-1.conf**.

3. Run the following command to set the registry key so that the Linux VDA can recognize the configuration file name set in Step 1.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
     DriverName" -d "intel" --force
2 <!--NeedCopy-->
```

Enable XDamage

If you are using a GPU that is not listed in the supported hardware section of the release notes for NVIDIA Linux Capture SDK, enable XDamage using:

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

Monitor blanking for Remote PC Access VDAs

The Linux VDA supports physical monitor blanking for Remote PC Access VDAs that use non-virtualized GPUs.

Fully tested Linux distributions that support the feature include Ubuntu 20.04 and Debian 11.3.

The feature is disabled by default. To enable it, complete the following two steps:

1. Install the evdi-dkms package based on your Linux distribution:

```
1 sudo apt install evdi-dkms
2 <!--NeedCopy-->
```

2. Enable graphics display offloading to EVDI:

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

3. If you are using an Intel GPU, disable the display manager. Otherwise, the Intel GPU is occupied by the display manager and not available for Citrix remote sessions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
sudo systemctl disable --now gdm
<!--NeedCopy-->
```

Troubleshooting

No or garbled graphic output

If you can run 3D applications locally and all configurations are correct, missing or garbled graphic output is the result of a bug. Use /opt/Citrix/VDA/bin/setlog and set GFX_X11 to verbose to collect the trace information for debugging.

Hardware encoding does not work

If you use `Xdamage`, only software encoding is supported.

Session watermark

January 23, 2023

Session watermark helps to deter and enable tracking of data theft. Traceable information appears on session desktops as a deterrent to users who employ photographs and screen captures to steal data. You can specify a watermark as a layer of text or a PNG image with alpha channel. The watermark displays over the entire session screen without changing the content of the original document.

> **Important:**
>
> Session watermark is not a security feature. It does not prevent data theft completely, but it provides some level of deterrent and traceability. We do not guarantee complete information traceability when using this feature. Instead, we recommend that you combine this feature with other security solutions as applicable.

The session watermark carries information for tracking data theft. The most important data is the identity of the user, as tracked by their logon credentials, of the session where the screen image was taken. To trace data leakage more effectively, include other information such as the server or client Internet protocol address and a connect time.

To adjust the user experience, use the following session watermark policy settings to configure the placement and watermark appearance on the screen:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Session watermark policy settings

Enable session watermark

When you enable this setting, the session display has an opaque watermark displaying session-specific information. The other watermark settings depend on this one being enabled.

By default, the session watermark is disabled.

Include client IP address

When you enable this setting, the session displays the current client IP address as a watermark.

By default, **Include client IP address** is disabled.

Include connection time

When you enable this setting, the session watermark displays a connect time. The format is yyyy/mm/dd hh:mm. The time displayed is based on the system clock and time zone.

By default, **Include connection time** is disabled.

Include logon user name

When you enable this setting, the session displays the current logon user name as a watermark. The display format is USERNAME@DOMAINNAME. We recommend that the user name is a maximum of 20 characters. When a user name is longer than 20 characters, smaller font sizes or truncation might occur, which lessens the effectiveness of the watermark.

By default, **Include logon user name** is enabled.

Include VDA host name

When you enable this setting, the session displays the VDA host name of the current ICA session as a watermark.

By default, **Include VDA host name** is enabled.

Include VDA IP address

When you enable this setting, the session displays the VDA IP address of the current ICA session as a watermark.

By default, **Include VDA IP address** is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Session watermark style

This setting controls whether you display a single watermark text label or multiple labels. Choose **Multiple** or **Single** from the **Value** drop-down menu.
For additional style options, see the **Watermark custom text** section in this article.

Multiple displays five watermark labels in the session. One in the center and four in the corners.

Single displays a single watermark label in the center of the session.

By default, the **Session watermark style** is **Multiple**.

Watermark transparency

You can specify watermark opacity from 0 through 100. The larger the value specified, the more opaque the watermark.

By default, the value is 17.

Watermark custom text

The value is empty by default. You can type a non-empty string, set a syntax to form a string, or use the combination to display in the session watermark. Non-empty strings support up to 25 Unicode characters per line. Longer strings are truncated to 25 characters.

For example, you can set the policy to the following value:

```
<date> <time><newline><username><style=single><fontsize=40><font=
Ubuntu><position=center><rotation=0><newline><serverip><newline><
clientip><newline>Citrix Linux VDA<newline>Version 2207
```

For a description of all syntax options, see the following table:

Syntax option	Description	Valid setting (case-sensitive)	Default value	Remarks
`<style>`	Watermark layout style	`xstyle`, `single`, `tile`, `horizontal`	`xstyle`	-
`<position>`	Watermark position	`center`, `topleft`, `topright`, `bottomleft`, `bottomright`	`center`	Valid only when the layout style is set to **single**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Syntax option	Description	Valid setting (case-sensitive)	Default value	Remarks
<rotation>	Watermark rotation to a certain angle	-180–180	0	-
<transparency>	Watermark opacity	0–100	17	-
<font>	-	A system supported font	Sans	-
<fontsize>	-	20–50	0 (auto calculated)	-
<fontzoom>	Percentage of the font and image sizes you set through <fontsize> and <image>	0 –	100	-
<image>	PNG watermark	Path to a PNG image on the VDA	N/A	This syntax configures a PNG watermark. Only PNG with an alpha channel is supported. With a PNG watermark in use, only the <style>, <position>, <rotation>, <transparency>, and <fontzoom> syntax options can be effective.
<date>	Placeholder for the session connection date (YYYY/MM/DD)	N/A	N/A	-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Syntax option	Description	Valid setting (case-sensitive)	Default value	Remarks
<time>	Placeholder for the session connection time (HH:MM)	N/A	N/A	-
<domain>	Placeholder for the user account domain	N/A	N/A	-
<username>	Placeholder for the current logon user name (excluding the user account domain)	N/A	N/A	-
<hostname>	Placeholder for the host name of the VDA	N/A	N/A	-
<clientip>	Placeholder for the IP address of the client	N/A	N/A	-
<serverip>	Placeholder for the IP address of the VDA	N/A	N/A	-

> **Note:**
>
> If **Watermark custom text** is specified with a valid syntax setting, all other session watermark policies - except **Enable session watermark** - are ignored.
>
> If you leave a syntax option unspecified or set it to an unsupported value, their default value is used.

Limitations

- Session watermark is supported in either of the following cases:
  - When **Use video codec for compression** is set to **For the entire screen**.
  - When **Use video codec for compression** is set to **Use when preferred** and Optimize for 3D graphics workload is enabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Session watermark is not supported in sessions where browser content redirection is used. To use the session watermark feature, ensure that browser content redirection is disabled.
- Session watermark is not supported and does not appear if the session is running in full-screen hardware accelerated H.264 or H.265 encoding mode with legacy NVIDIA drivers. (In this case, NvCaptureType is set to 2 in the registry.)
- Watermark is not visible for session shadowing.
- If you press the Print Screen key to capture a screen, the screen captured at the VDA side does not include the watermark. We recommend that you take measures to avoid screen captures being copied.

Thinwire progressive display

January 23, 2023

Session interactivity can degrade on low bandwidth or high latency connections. For example, scrolling on a webpage can become slow, unresponsive, or choppy. Keyboard and mouse operations can lag behind graphics updates.

Through version 7.17, you were able to use policy settings to reduce bandwidth consumption by configuring the session to **Low** visual quality, or setting a lower color depth (16-bit or 8-bit graphics). However, you had to know that a user was on a weak connection. HDX Thinwire did not dynamically adjust static image quality based on network conditions.

Starting with version 7.18, HDX Thinwire switches to a progressive update mode by default in either of the following cases:

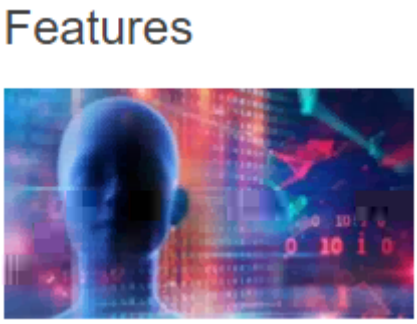
- Available bandwidth falls below 2 Mbps.
- Network latency exceeds 200 ms.

In this mode:

For example, in the following graphic where progressive update mode is active, the letters **F** and **e** have blue artifacts, and the image is heavily compressed. This approach significantly reduces bandwidth consumption, which allows images and text to be received more quickly, and session interactivity improves.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

When you stop interacting with the session, the degraded images and text are progressively sharpened to lossless. For example, in the following graphic, the letters no longer contain blue artifacts, and the image appears at source quality.



For images, sharpening uses a random block-like method. For text, individual letters or parts of words are sharpened. The sharpening process occurs over several frames. This approach avoids introducing a delay with a single large sharpening frame.

Transient imagery (video) is still managed with adaptive display or Selective H.264.

How progressive mode is used

By default, progressive mode is on standby for the **Visual quality** policy settings: **High**, **Medium** (default), and **Low**.

Progressive mode is forced off (not used) when:

- **Visual quality** = **Always Lossless** or **Build to Lossless**
- **Preferred color depth for simple graphics** = 8-bit
- **Use video codec for compression** = **For the entire screen** (when full-screen H.264 is desired)

When progressive mode is on standby, by default it is enabled when either of the following conditions occurs:

- Available bandwidth drops below 2 Mbps
- Network latency increases above 200 ms

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

After a mode switch occurs, a minimum of 10 s is spent in that mode, even if the adverse network conditions are momentary.

Change progressive mode behavior

You can change the progressive mode behavior by running the following command:

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

Where <value>:

0 = Always off (do not use under any circumstances)

1 = Automatic (toggle based on network conditions, default value)

2 = Always on

When in automatic mode (1), you can run either of the following commands to change the thresholds at which progressive mode is toggled:

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

Where <value> is <threshold in Kbps> (default = 2,048)

Example: 4096 = toggle progressive mode on if bandwidth falls below 4 Mbps

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

Where <value> is <threshold in ms> (default = 200)

Example: 100 = toggle progressive mode on if network latency drops below 100 ms.

Keyboard

January 23, 2023

This section contains the following topics:

- Client IME

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Client IME user interface synchronization
- Dynamic keyboard layout synchronization
- Soft keyboard
- Support for multiple language inputs

Client Input Method Editor (IME)

January 23, 2023

Overview

Double-byte characters such as Chinese, Japanese, and Korean characters must be typed through an IME. Type such characters with any IME that is compatible with Citrix Workspace app on the client side, such as the Windows native CJK IME.

Installation

This feature is installed automatically when you install the Linux VDA.

Usage

Open a Citrix Virtual Apps or Citrix Virtual Desktops session as per usual.

Change your input method as required on the client side to start using the client IME feature.

Known issues

- Double-clicking a cell in a Google spreadsheet is a must before you can use the client IME feature to type characters in the cell.
- The client IME feature is not disabled automatically in Password fields.
- The IME user interface does not follow the cursor in the input area.

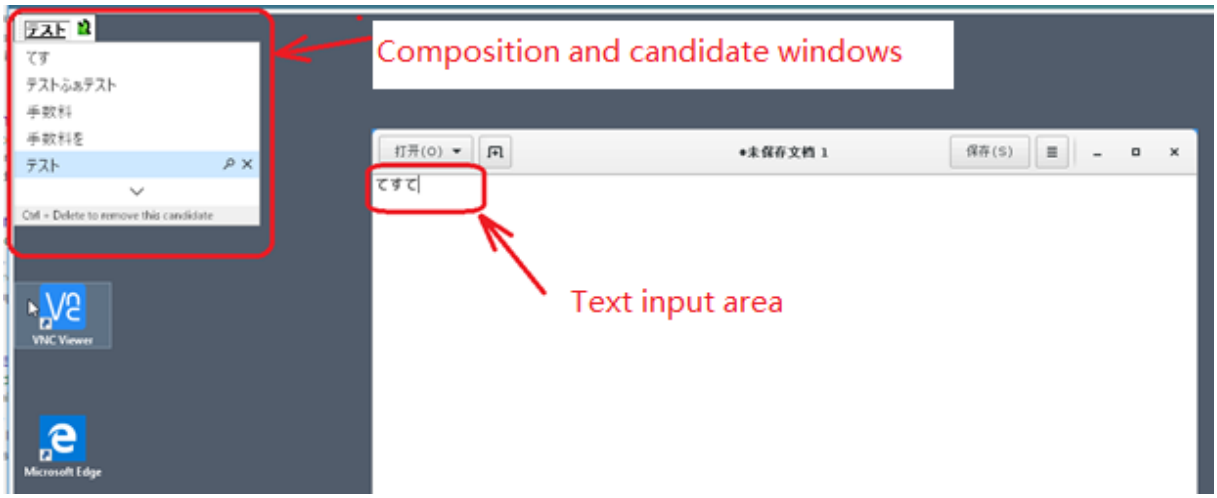
Client IME user interface synchronization

January 23, 2023

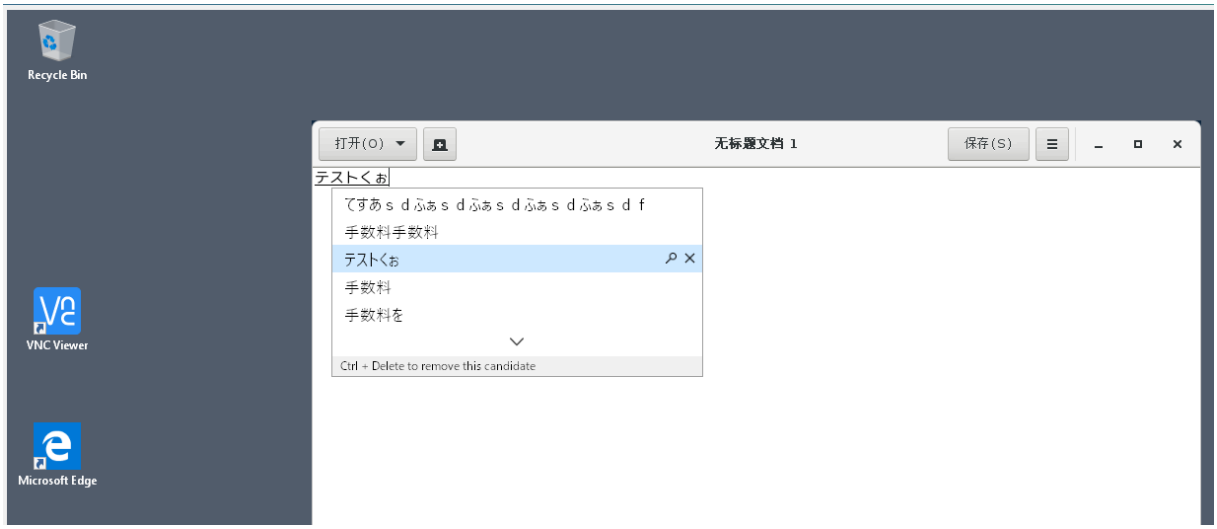
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Overview

To date, the client IME user interface (including the composition window and candidate window) was positioned in the upper left corner of the screen. It did not follow the cursor and sometimes was located far from the cursor in the text input area:



Citrix enhances usability and further improves the user experience with the client IME as follows:



Prerequisites for using the feature

1. Enable Intelligent Input Bus (`IBus`) on your Linux VDA. For information on how to enable `IBus` on a Linux OS, see the OS vendor's documentation. For example:
   - Ubuntu: https://help.ubuntu.com/community/ibus
   - CentOS, RHEL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Debian: https://wiki.debian.org/I18n/ibus
- SUSE: https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang

2. The feature installs automatically but you must enable it before you can use it.

Enable and disable the feature

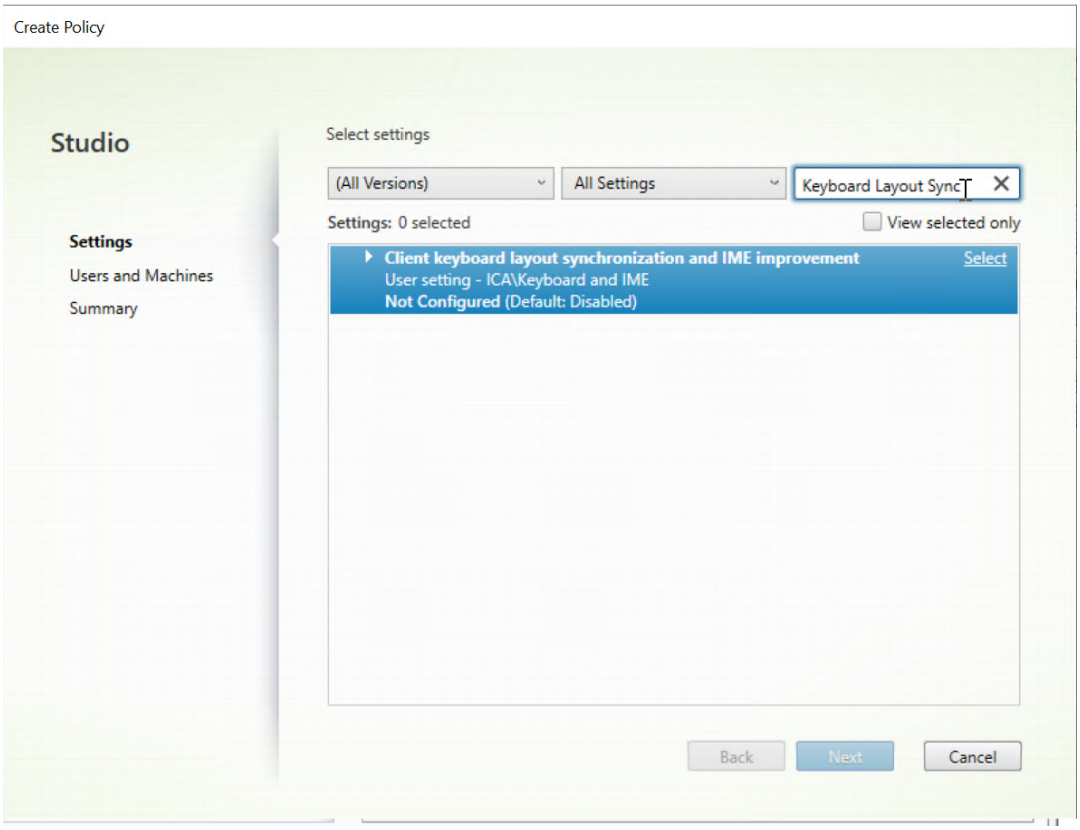
The client IME user interface synchronization feature is disabled by default. To enable or disable the feature, set the **Client Keyboard Layout Sync and IME Improvement** policy or edit the registry through the `ctxreg` utility.

> **Note:**
>
> The **Client Keyboard Layout Sync and IME Improvement** policy takes priority over registry settings and can be applied to user and machine objects you specify or all objects in your site. Registry settings on a given Linux VDA apply to all sessions on that VDA.

- Set the **Client Keyboard Layout Sync and IME Improvement** policy to enable or disable the client IME user interface synchronization feature:

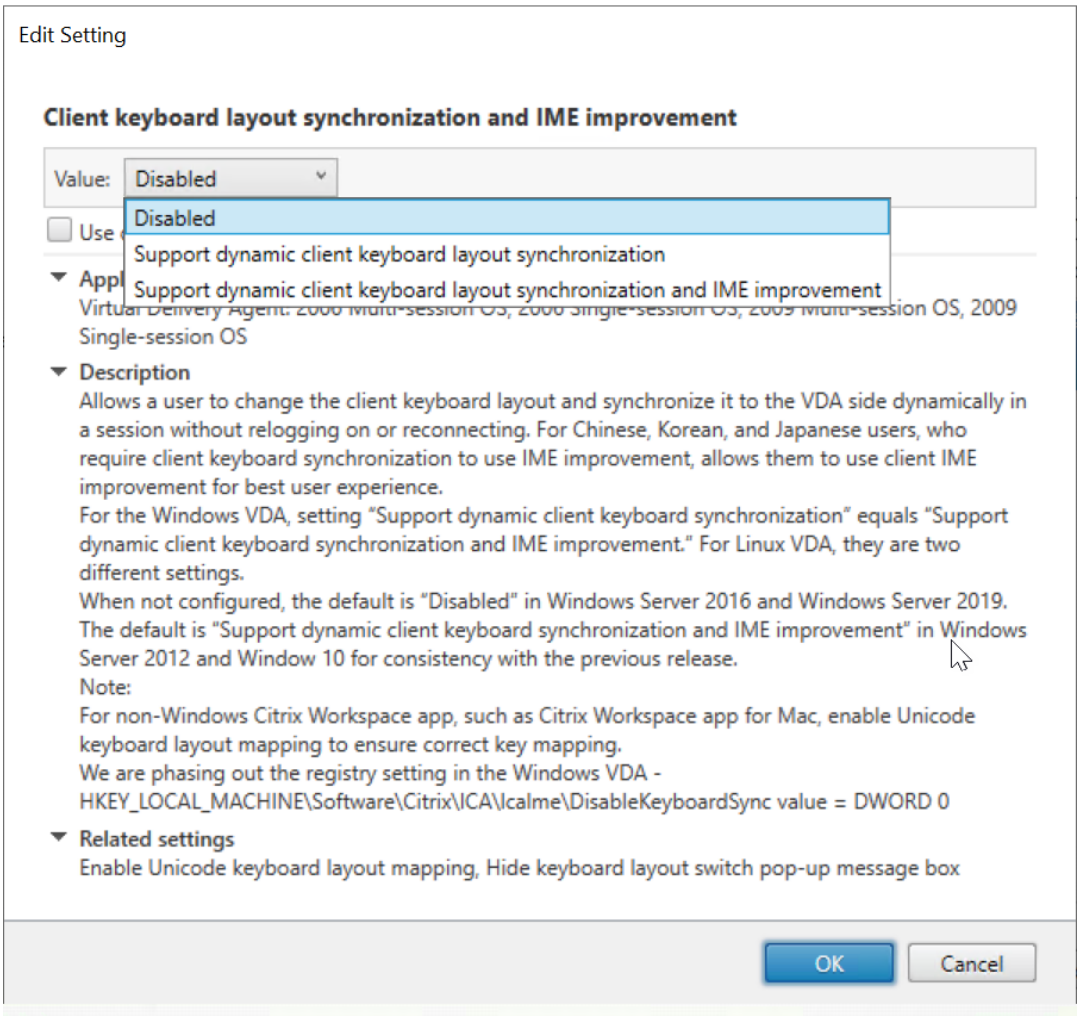
  1. In Studio, right-click **Policies** and select **Create Policy**.
  2. Search for the **Client Keyboard Layout Sync and IME Improvement** policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Click **Select** next to the policy name.
4. Set the policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



There are three options available:

- **Disabled**: disables dynamic keyboard layout synchronization and client IME user interface synchronization.
- **Support dynamic client keyboard layout synchronization**: enables dynamic keyboard layout synchronization regardless of the DWORD value of the **SyncKeyboardLayout** registry key at `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Support dynamic client keyboard layout synchronization and IME improvement**: enables both dynamic keyboard layout synchronization and client IME user interface synchronization regardless of the DWORD values of the **SyncKeyboardLayout** and **SyncClientIME** registry keys at `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Edit the registry through the `ctxreg` utility to enable or disable the client IME user interface synchronization feature:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To enable the feature, run the command:

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

To disable the feature, run the command:

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

Dynamic keyboard layout synchronization

January 23, 2023

Previously, the keyboard layouts on the Linux VDA and on the client device had to be the same. Key mapping issues might occur, for example, when the keyboard layout changed from English to French on the client device but not on the VDA.

Citrix addresses the issue by synchronizing the keyboard layout of the VDA with the keyboard layout of the client device automatically. Anytime the keyboard layout on the client device changes, the layout on the VDA follows suit.

> **Note:**
>
> Citrix Workspace app for HTML5 does not support the dynamic keyboard layout synchronization feature.

Configuration

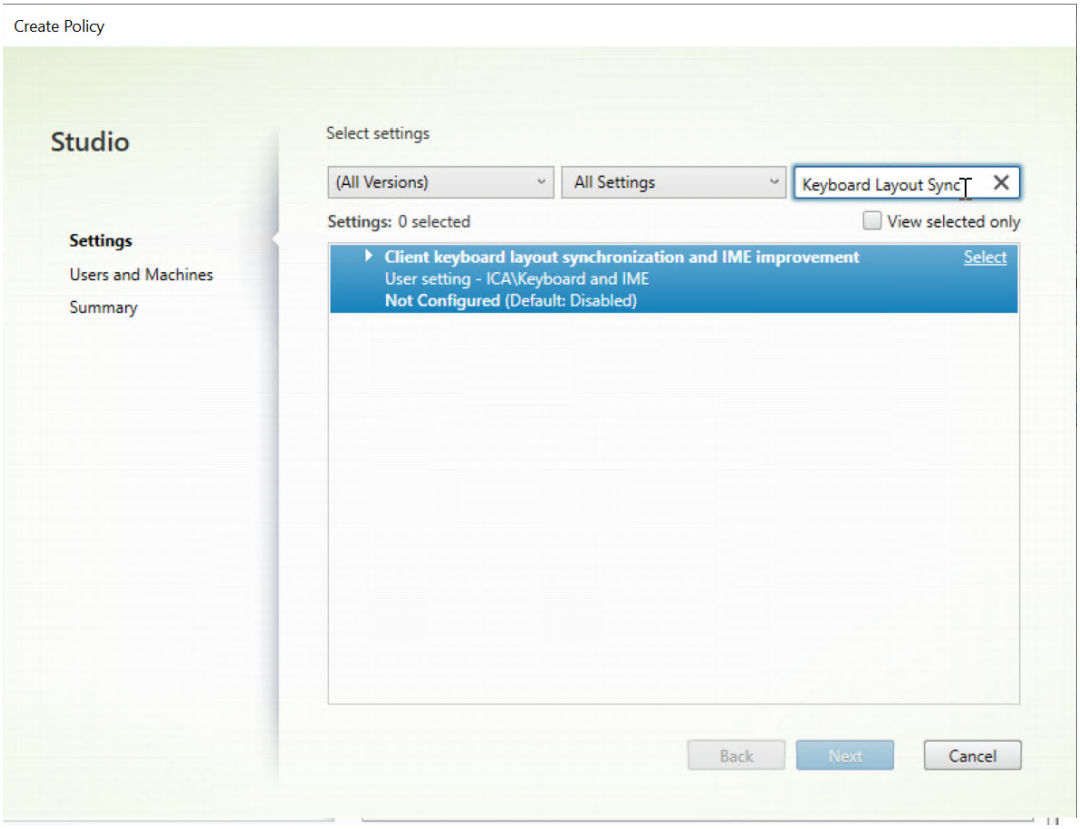
The dynamic keyboard layout synchronization feature is disabled by default. To enable or disable the feature, set the **Client Keyboard Layout Sync and IME Improvement** policy or edit the registry through the `ctxreg` utility.

> **Note:**
>
> The **Client Keyboard Layout Sync and IME Improvement** policy takes priority over registry settings and can be applied to user and machine objects you specify or all objects in your site. Registry settings on a given Linux VDA apply to all sessions on that VDA.

- Set the **Client Keyboard Layout Sync and IME Improvement** policy to enable or disable the dynamic keyboard layout synchronization feature:

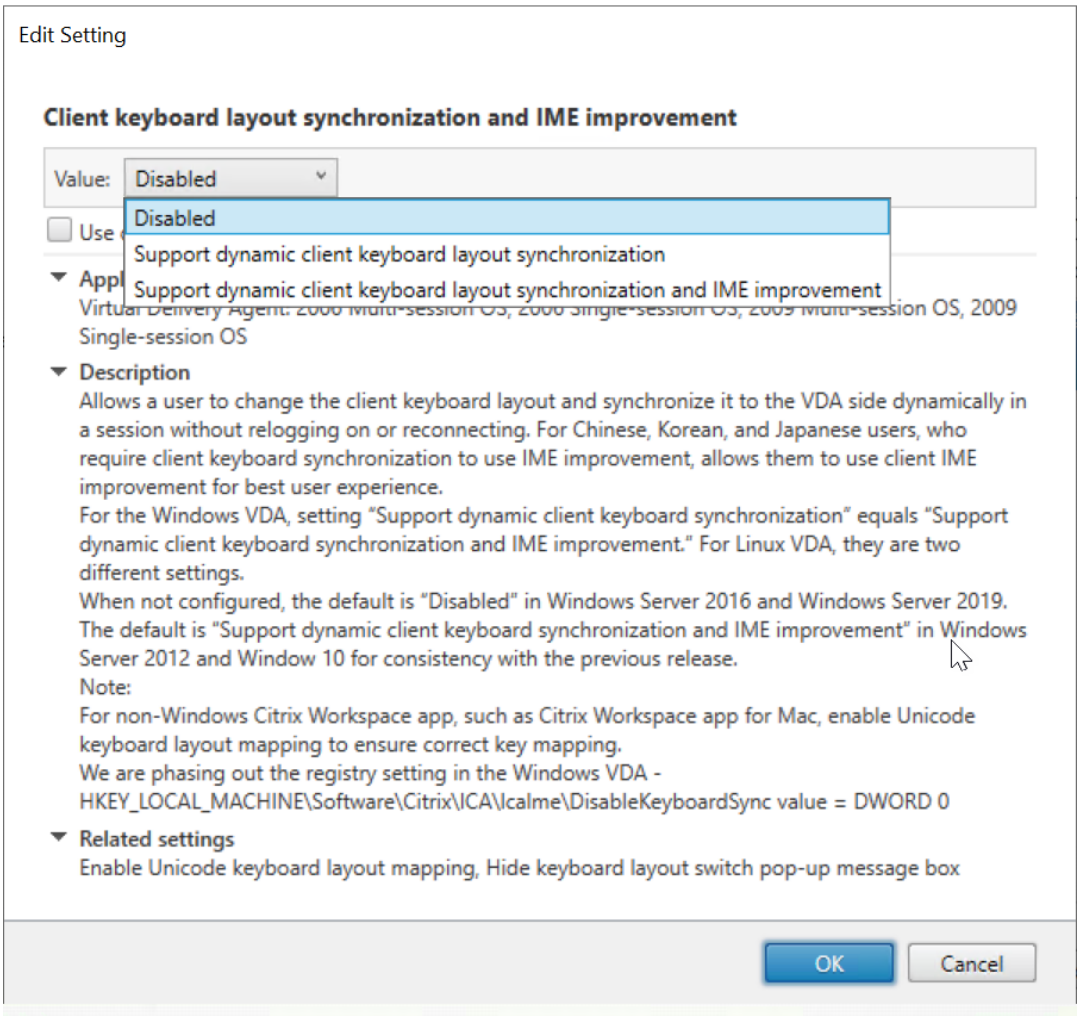
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. In Studio, right-click **Policies** and select **Create Policy**.
2. Search for the **Client Keyboard Layout Sync and IME Improvement** policy.



3. Click **Select** next to the policy name.
4. Set the policy.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



There are three options available:

- **Disabled**: disables dynamic keyboard layout synchronization and client IME user interface synchronization.
- **Support dynamic client keyboard layout synchronization**: enables dynamic keyboard layout synchronization regardless of the DWORD value of the **SyncKeyboardLayout** registry key at `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Support dynamic client keyboard layout synchronization and IME improvement**: enables both dynamic keyboard layout synchronization and client IME user interface synchronization regardless of the DWORD values of the **SyncKeyboardLayout** and **SyncClientIME** registry keys at `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Edit the registry through the `ctxreg` utility to enable or disable the dynamic keyboard layout synchronization feature:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

To enable this feature, run the command:

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

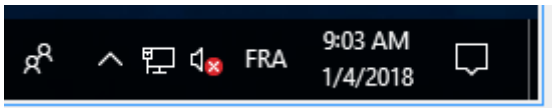
To disable this feature, run the command:

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

Usage

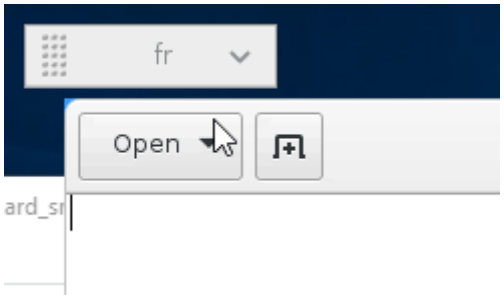
With this feature enabled, when the keyboard layout changes on the client device during a session, the keyboard layout of the session changes accordingly.

For example, if you change the keyboard layout on a client device to French (FR):

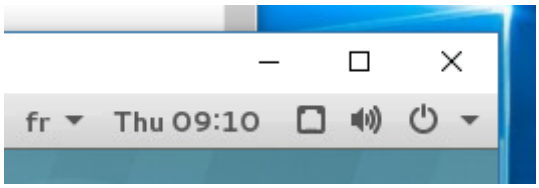


Then the keyboard layout of the Linux VDA session also changes to “fr.”

In an application session, you can see this automatic change if you have enabled the language bar:



In a desktop session, you can see this automatic change in the task bar:



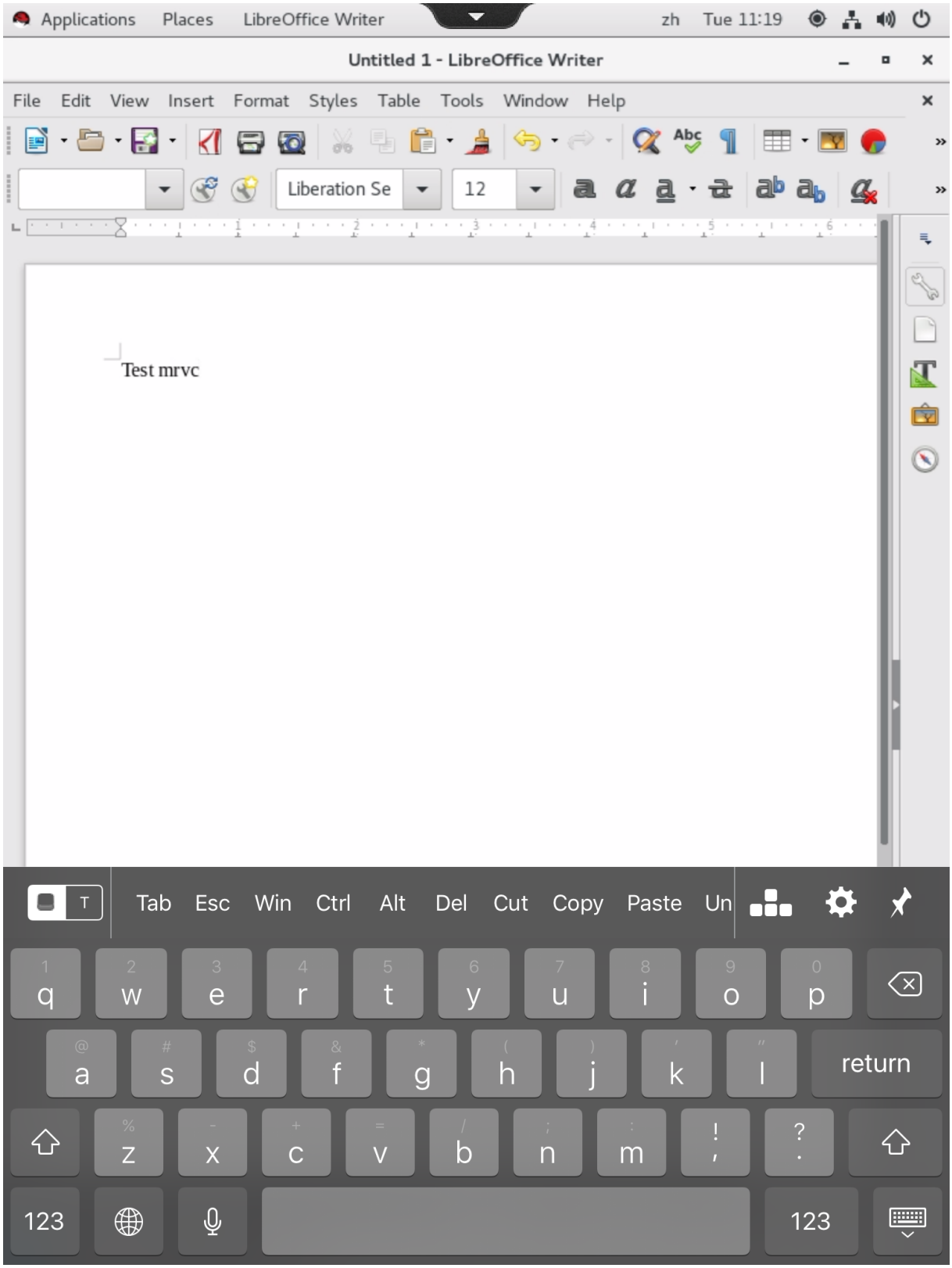
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Soft keyboard

January 23, 2023

The soft keyboard feature is available in a Linux virtual desktop or application session. The soft keyboard shows or hides automatically when you enter or leave an input field.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> The feature is supported on Citrix Workspace app for iOS and for Android.

Enable and disable the feature

The feature is disabled by default. Use the **ctxreg** utility to enable or disable the feature. The feature configuration on a given Linux VDA applies to all sessions on that VDA.

To enable the feature:

1. Run the command:

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

2. In Citrix Studio, set the **Automatic keyboard display** policy to **Allowed**.
3. (Optional) For RHEL 7 and CentOS 7, run the following command to configure the Intelligent Input Bus (IBus) as the default IM service:

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

To disable the feature, run the command:

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

> **Note:**
>
> The preceding settings take effect when you log on to a new session or log off and back on to the current session.

Limitations

- The feature might not work as expected with Google Chrome, LibreOffice, and other apps.
- To display the soft keyboard again after hiding it manually, click a non-input field and then the current input field again.
- The soft keyboard might not appear when you click from one input field to another in a web browser. To work around this issue, click a non-input field and then the target input field.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- The feature does not support Unicode characters and double-byte characters (such as Chinese, Japanese, and Korean characters).
- The soft keyboard is not available for password input fields.
- The soft keyboard might overlap the current input field. In this case, move the app window or scroll up your screen to move the input field to an accessible position.
- Due to compatibility issues between Citrix Workspace app and Huawei tablets, the soft keyboard appears on Huawei tablets even with a physical keyboard connected.

Support for multiple language inputs

January 23, 2023

As of the Linux VDA Version 1.4, Citrix has added support for published applications. Users can access a desired Linux application without the Linux desktop environment.

However, the native language bar on the Linux VDA was unavailable to the published application because the language bar is highly integrated with the Linux desktop environment. As a result, users were unable to input text in a language that requires IME such as Chinese, Japanese, or Korean. It was also not possible for users to switch between keyboard layouts during an application session.

To address those issues, this feature provides a language bar for published applications that accept text input. The language bar enables users to select a server-side IME and to switch between keyboard layouts during an application session.

Configuration

You can use the **ctxreg** utility to enable or disable this feature (disabled by default). The feature configuration on a given Linux VDA server applies to all applications published on that VDA.

The configuration key is "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar" and the type is DWORD.

To enable this feature, run the command:

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

To disable this feature, run the command:

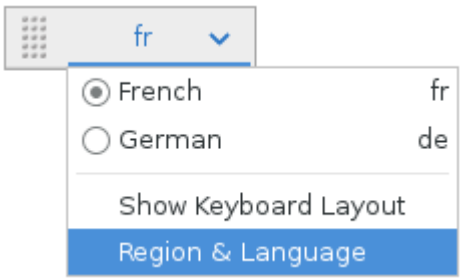
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

Usage

The usage is straightforward.

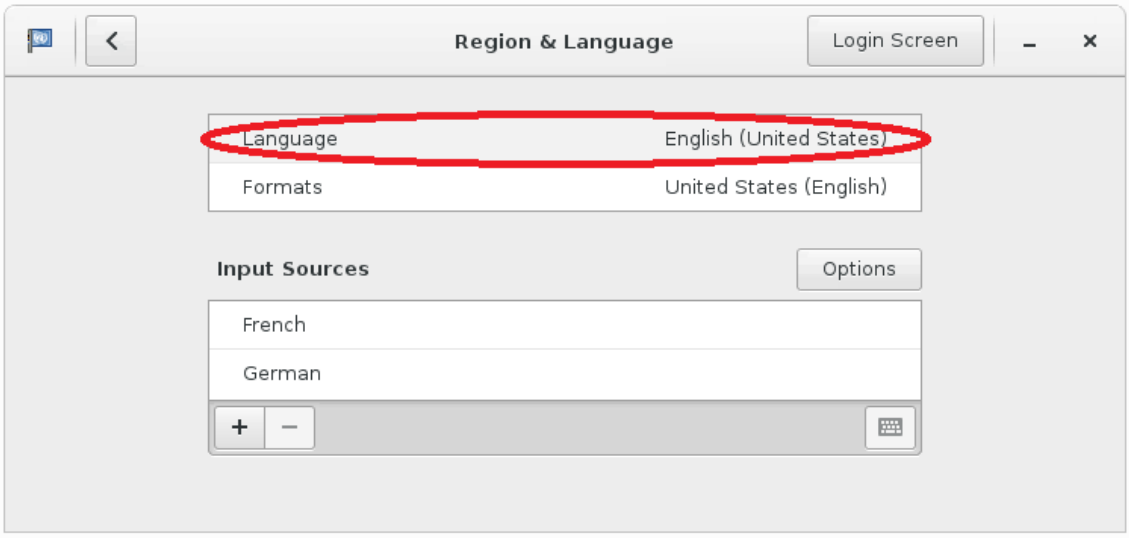
1. Enable the feature.
2. Access a published application that can accept text input. A language bar appears in the session, alongside the application.
3. From the drop-down menu, select **Region & Language** to add the desired language (input source).



4. Select the IME or keyboard layout from the drop-down menu.
5. Type a language using the selected IME or keyboard layout.

> **Note:**
>
> - When you change a keyboard layout on the VDA-side language bar, ensure that the same keyboard layout is used on the client side (running Citrix Workspace app).
> - The **accountsservice** package must be upgraded to Version 0.6.37 or later before you can perform settings in the **Region & Language** dialog box.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Multimedia

January 23, 2023

This section contains the following topics:

- Audio features
- Browser content redirection
- HDX webcam video compression

Audio features

July 25, 2023

Adaptive audio

Adaptive audio is enabled by default. It supports the following Citrix Workspace app clients:

- Citrix Workspace app for Windows –2109 and later versions
- Citrix Workspace app for Linux –2109 and later versions
- Citrix Workspace app for Mac –2109 and later versions

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Adaptive audio falls back to legacy audio when you use a client not on the list.

With adaptive audio, you don't need to manually configure the audio quality policies on the VDA. Adaptive audio dynamically adjusts audio sampling bitrates based on network conditions to provide a premium audio experience.

The following table shows a comparison between adaptive audio and legacy audio:

Adaptive audio	Legacy audio
Max. audio sample rate: 48 kHz	Max. audio sample rate: 8 kHz
Stereo channel	Mono channel

> **Tip:**
>
> Use PulseAudio 13.99 or later on RHEL 8.x.
>
> Use PulseAudio 14.2 or later on SUSE 15.3.

Browser content redirection

January 23, 2023

Overview

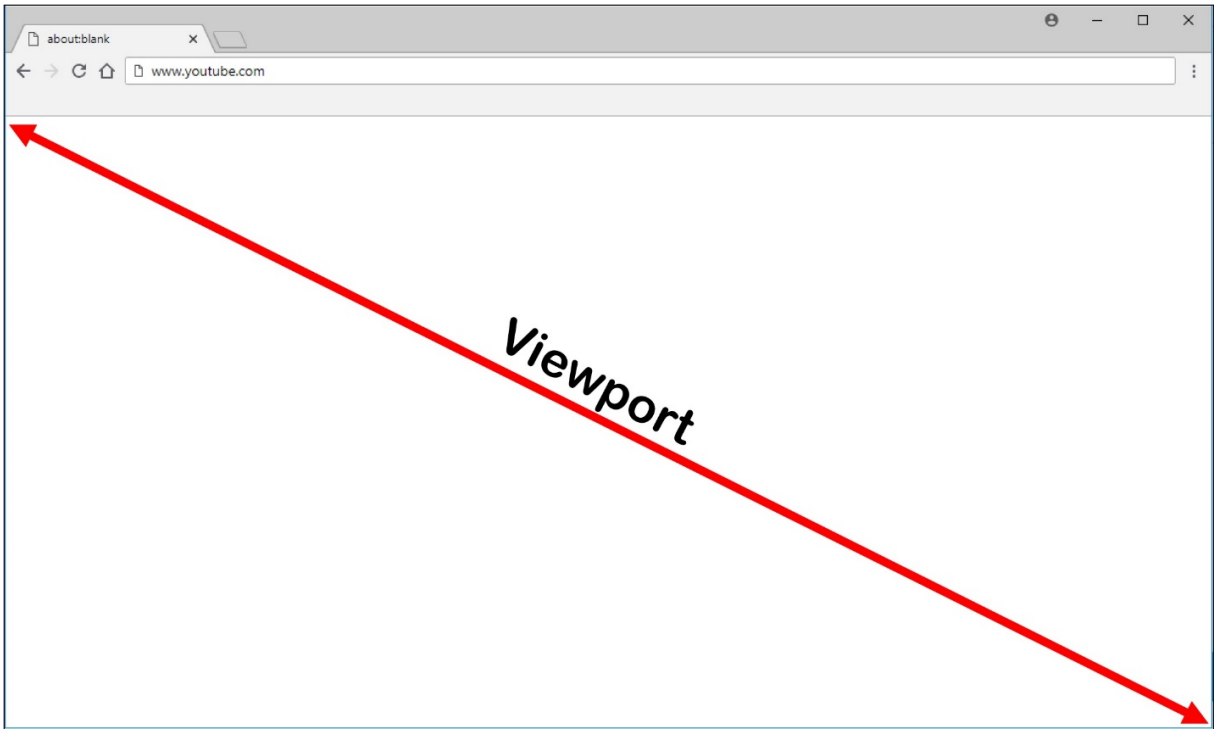
The Linux VDA supports browser content redirection in Google Chrome. Browser content redirection provides the ability of rendering webpages in the allow list on the client side. This feature uses Citrix Workspace app to instantiate a corresponding rendering engine on the client side, which fetches the HTTP and HTTPS content from the URL.

> **Note:**
>
> You can specify which webpages are redirected to the client side by using an allow list. Conversely, you can specify which webpages are not redirected to the client side by using a block list.

This overlay web layout engine runs on the client instead of on the VDA and uses the client CPU, GPU, RAM, and network.

Only the browser viewport is redirected. The viewport is the rectangular area in your browser where content displays. The viewport does not include items such as the address bar, favorites bar, and status bar. Those items are still running in the browser on the VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



System requirements

Windows client:

- Citrix Workspace app 1809 for Windows or later

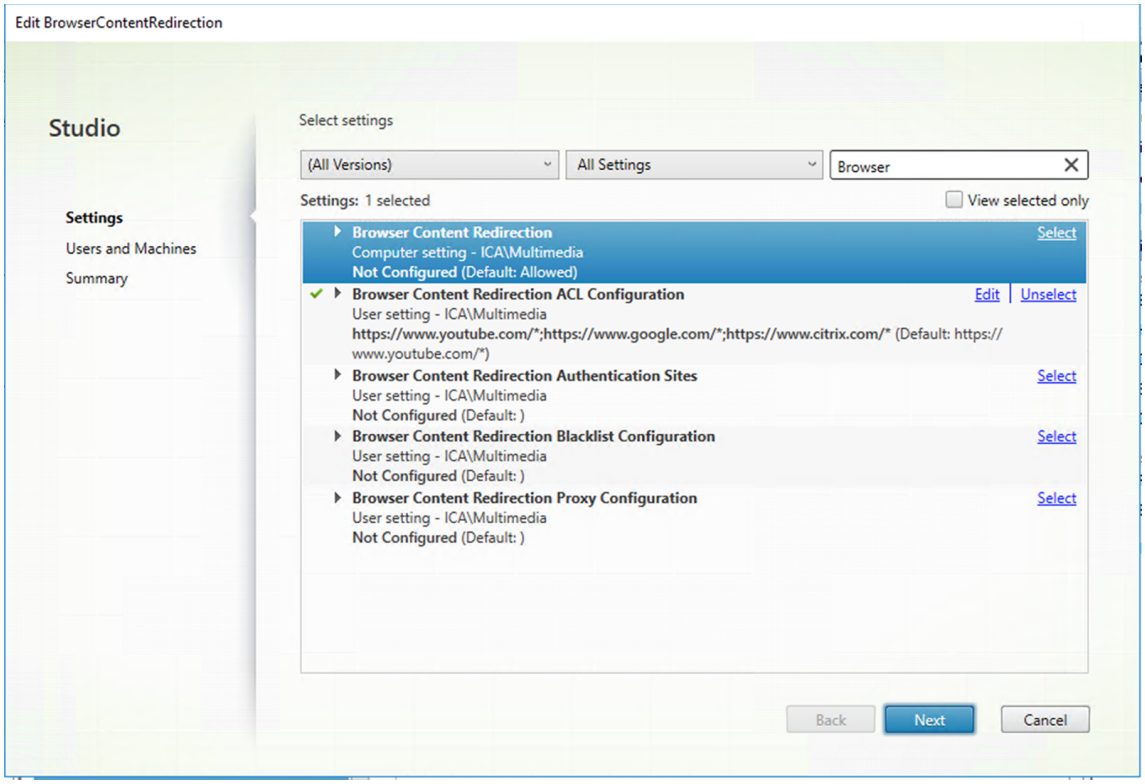
Linux VDA:

- Browser on the VDA: Google Chrome v66 or later with the Citrix browser content redirection extension added

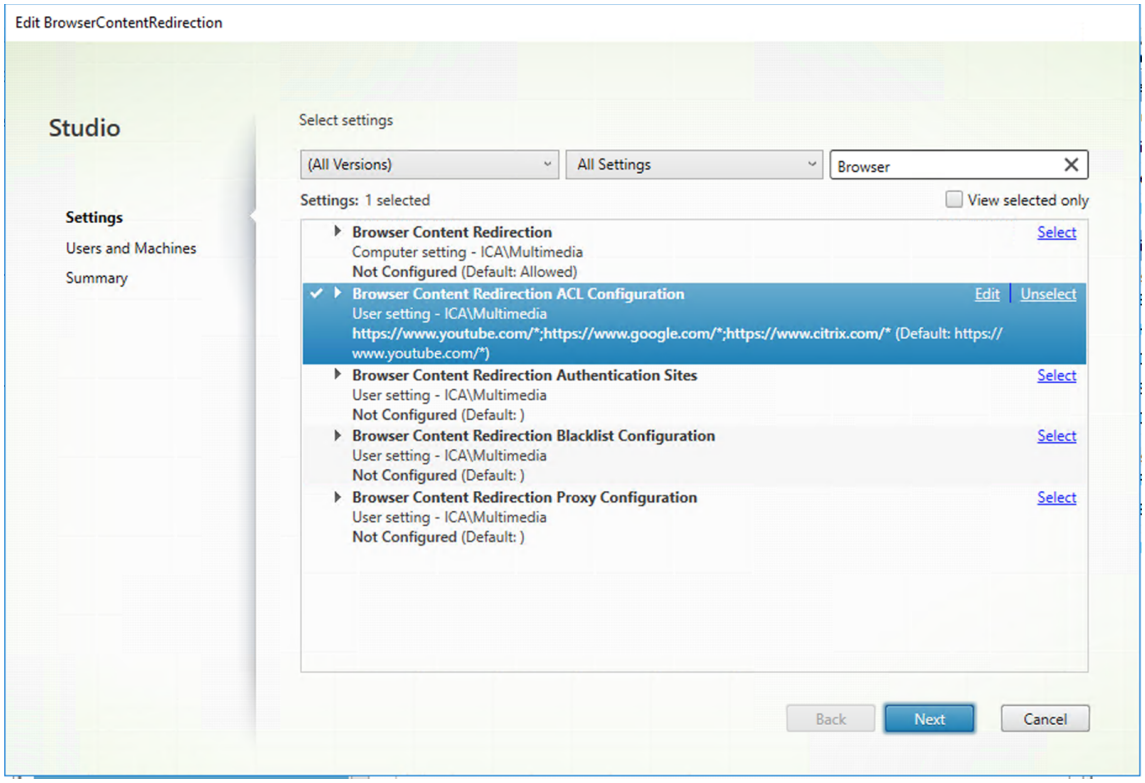
Configure browser content redirection

1. In Citrix Studio, configure policies to specify an allow list and a block list of URLs for browser content redirection. Browser content redirection is set to **Allowed** by default.

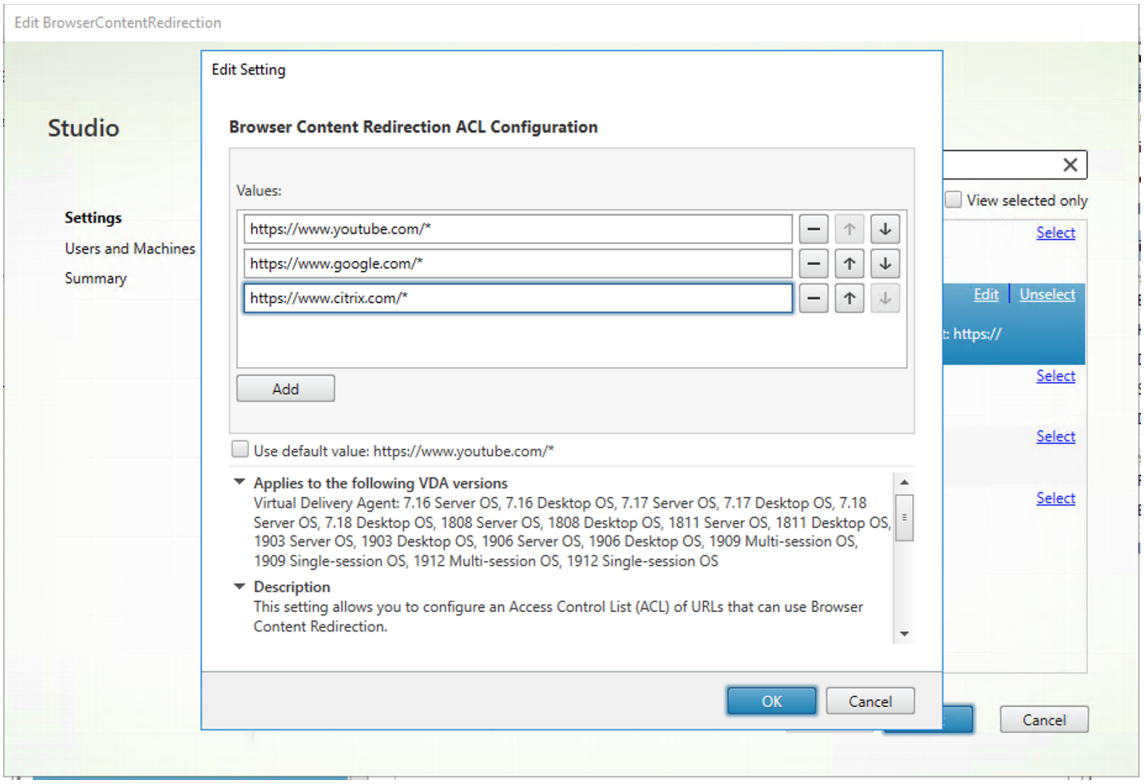
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



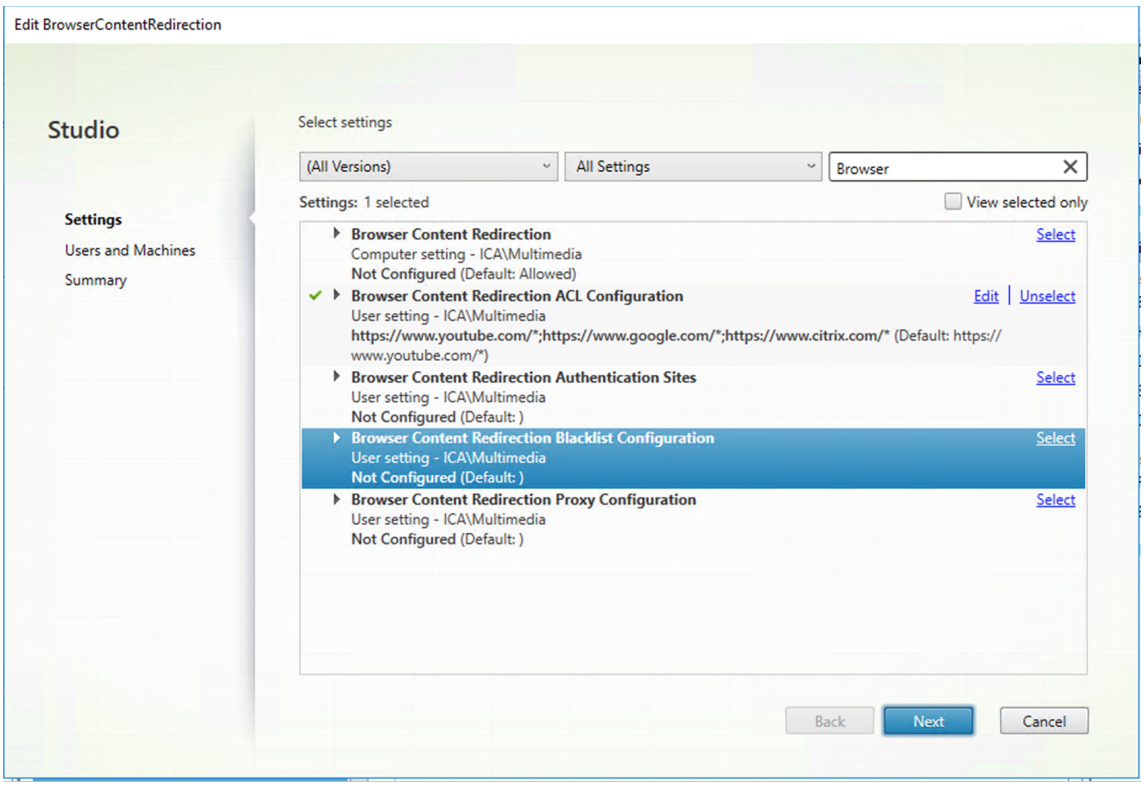
The **Browser Content Redirection ACL Configuration** setting specifies an allow list of URLs that can use browser content redirection.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



The **Browser Content Redirection Blacklist Configuration** setting specifies a block list of URLs that cannot use browser content redirection.

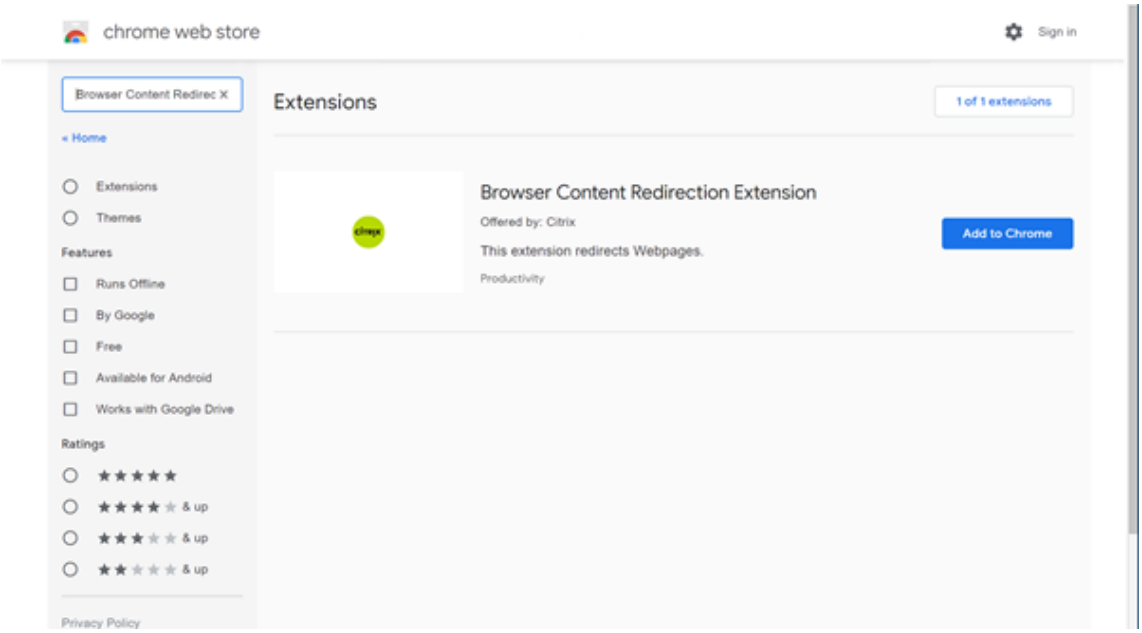


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> The Linux VDA currently does not support the **Browser Content Redirection Proxy Configuration** setting.

2. Click **Add to Chrome** on the VDA to add the Citrix browser content redirection extension from the Chrome Web Store. Doing so helps the browser on the VDA to detect whether a URL (being navigated to) matches an allow list or a block list.

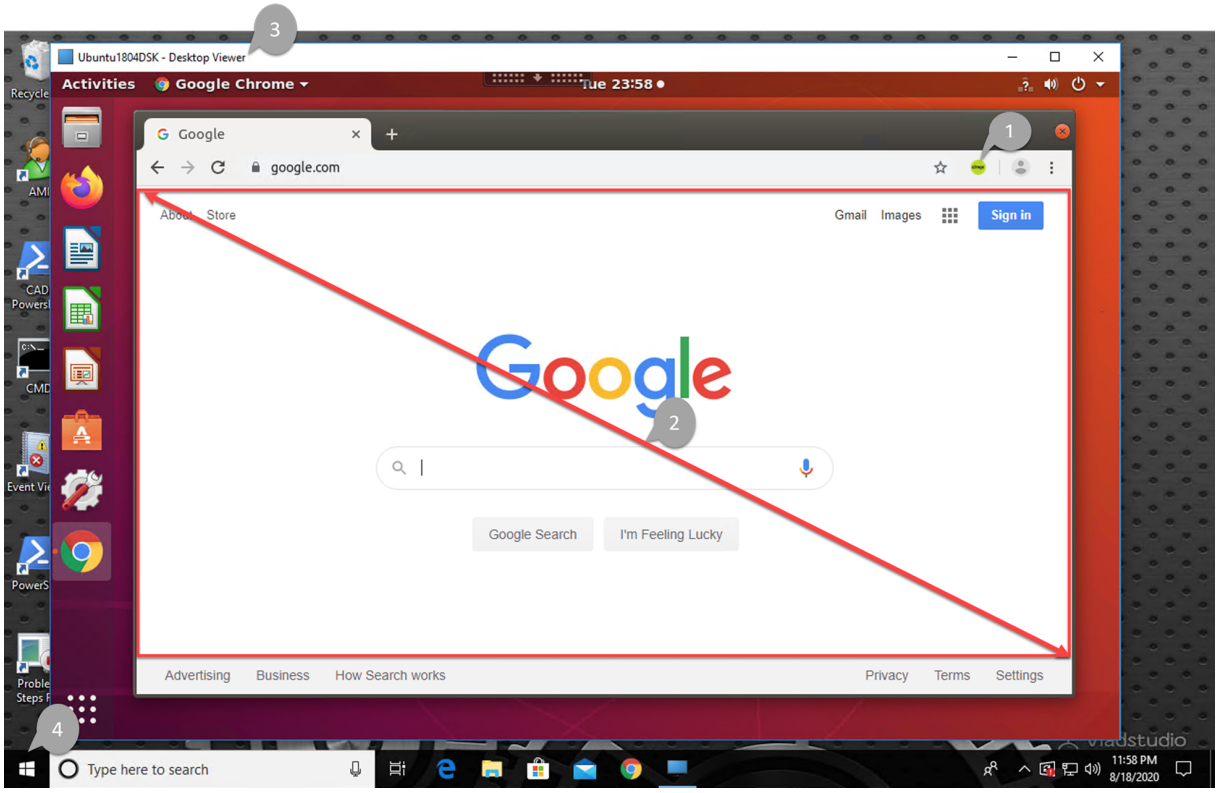
> **Important:**
>
> The extension is not required on the client. Add it only on the VDA.
>
> Chrome extensions are installed on a per-user basis. Updating a golden image to add or remove an extension is not required.



If a match to a URL is found in an allow list (for example, `https://www.mycompany.com/`) but not in any block list, a virtual channel (CTXCSB) instructs the Citrix Workspace app that a redirection is required and relays the URL. Citrix Workspace app then instantiates a local rendering engine and displays the website.

Citrix Workspace app then blends back the website into the virtual desktop browser content area seamlessly.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. Icon of the Citrix browser content redirection extension

   The color of the extension icon specifies the status of the Chrome extension. It is one of the three colors:

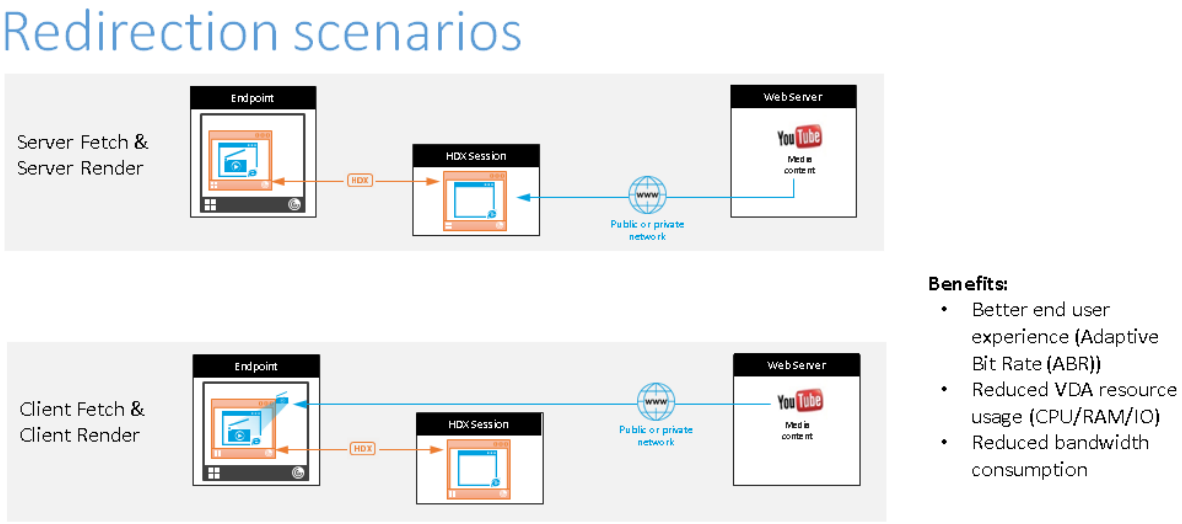
   - Green: Active and connected
   - Gray: Not active/idle on the current tab
   - Red: Broken/Not working

2. Viewport rendered on the client or blended back to the virtual desktop
3. Linux VDA
4. Windows client

Redirection scenarios

Here are scenarios of how the Citrix Workspace app fetches content:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Server fetch and server render:** There is no redirection because you did not add the site to the allow list or the redirection failed. We fall back to rendering the webpage on the VDA and use Thinwire to remote the graphics. Use policies to control the fallback behavior. This scenario causes high CPU, RAM, and bandwidth consumption on the VDA.
- **Client fetch and client render:** Because the Citrix Workspace app contacts the web server directly, it requires Internet access. This scenario offloads all the network, CPU, and RAM usage from your Citrix Virtual Apps and Desktops site.

Fallback mechanism

There might be times when client redirection fails. For example, if the client machine does not have direct Internet access, an error response might go back to the VDA. In such cases, the browser on the VDA can then reload and render the page on the server.

HDX webcam video compression

March 21, 2023

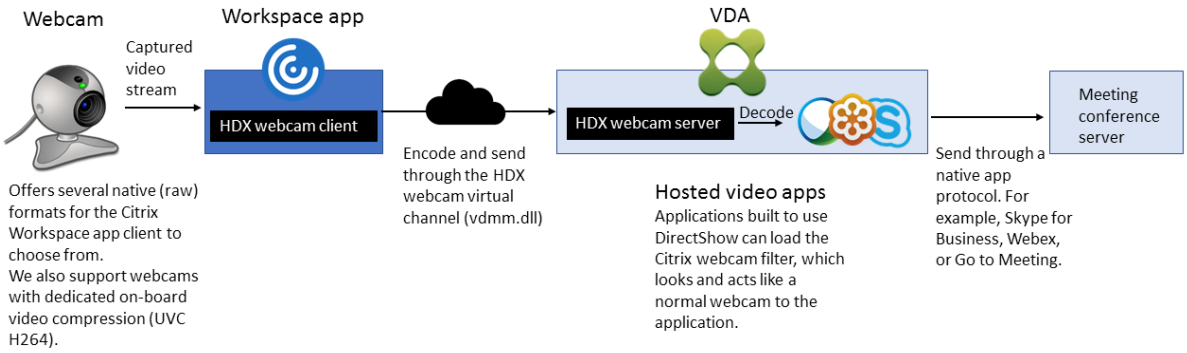
Overview

Users of video conferencing applications running in Linux VDA sessions can now use their webcams with HDX webcam video compression. The feature is enabled by default. We recommend you always use HDX webcam video compression if possible.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

HDX webcam video compression is also called **Optimized** webcam mode. This type of webcam video compression sends the H.264 video directly to the video conferencing application running in the virtual session. HDX webcam video compression uses the multimedia framework technology that is part of the client operating system to intercept video from capture devices, transcode, and compress it. Manufacturers of capture devices supply the drivers that plug into the OS kernel streaming architecture.

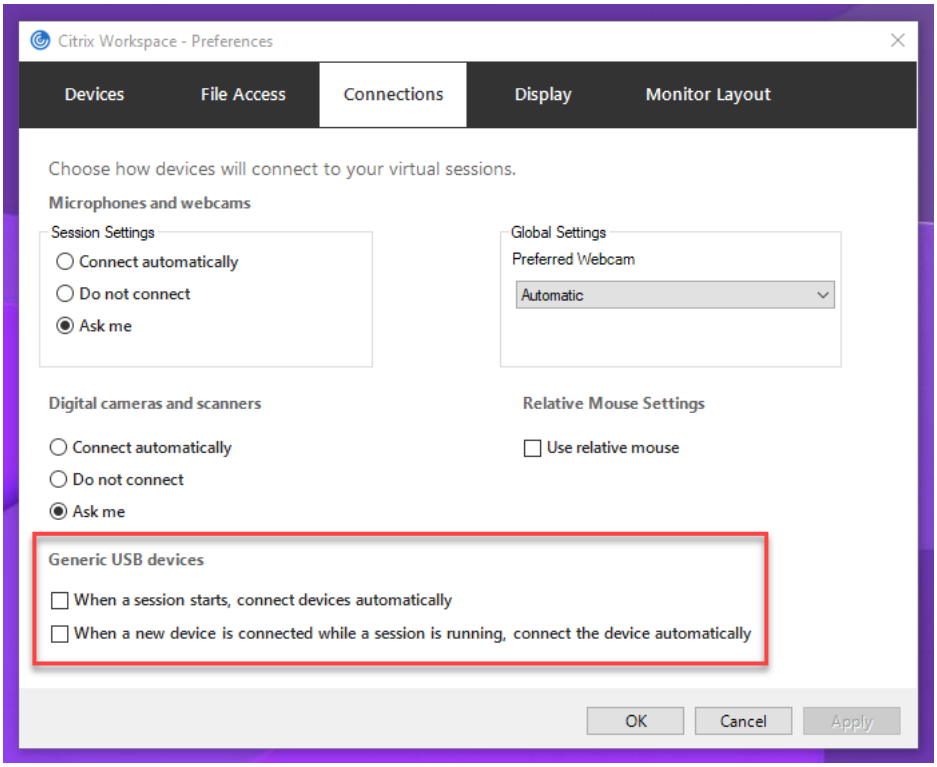
The client handles communication with the webcam. The client then sends the video only to the server that can display it properly. The server doesn't deal directly with the webcam, but its integration gives you the same experience in your desktop. Workspace app compresses the video to save bandwidth and provide better resiliency on WAN scenarios.



Note:

- The feature is not available for Azure machines because the **videodev** kernel module that the feature depends on is missing on Azure machines.
- The feature supports only H.264 videos from your Citrix Workspace app client.
- The supported webcam resolution ranges between 48x32 and 1920x1080.
- Do not choose **Generic USB devices** from your Citrix Workspace app toolbar when you are using a webcam. Otherwise, unexpected issues might occur.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Supported Citrix Workspace app

HDX webcam video compression supports the following versions of Citrix Workspace app:

Platform	Processor
Citrix Workspace app for Windows	Citrix Workspace app for Windows supports webcam video compression for 32-bit and 64-bit apps on XenApp and XenDesktop 7.17 and later. On earlier versions, Citrix Workspace app for Windows supports only 32-bit apps.
Citrix Workspace app for Chrome	Because some ARM Chromebooks don't support H.264 encoding, only 32-bit apps can use the optimized HDX webcam video compression.

Fully tested webcams

Different webcams offer different frame rates and have different levels of brightness and contrast. Citrix uses the following webcams for initial feature validation:

- Logitech HD Webcam C270

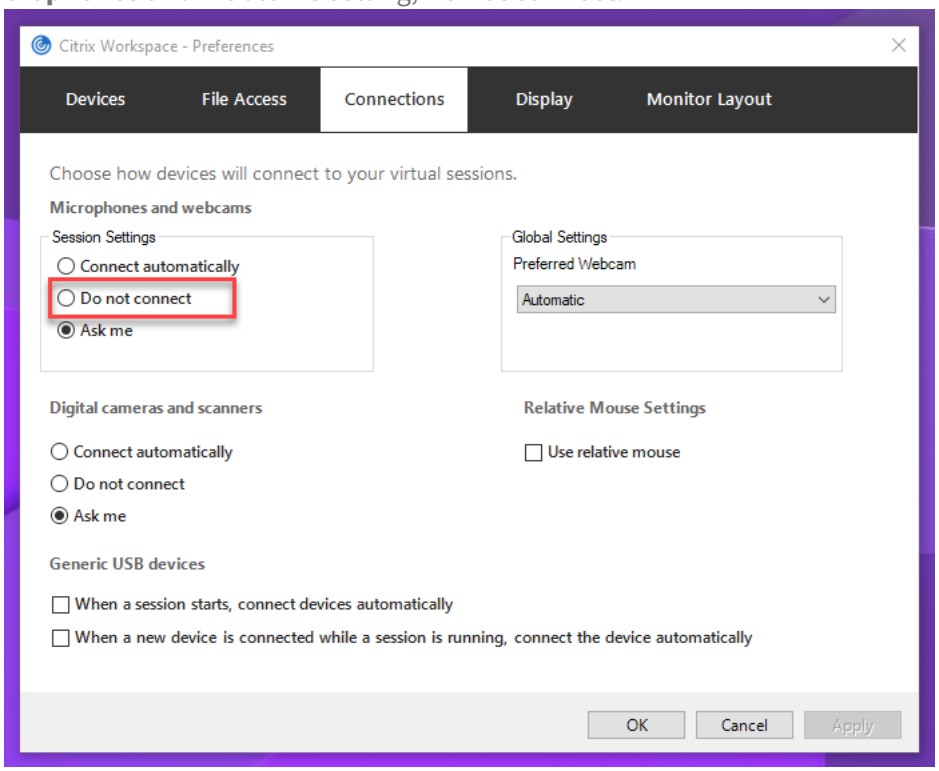
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

Configuration

This feature is enabled by default. To use it, complete the following verification and configuration:

> **Tip:**
>
> Citrix Workspace app users can override the default setting by choosing the Desktop Viewer **Microphones and webcams** setting, **Do not connect**.



1. After your VDA installation completes, verify that your VDA can register with the Delivery Controller and the published Linux desktop sessions can be launched successfully using Windows credentials.
2. Ensure that your VDA has Internet access and then run the `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` command to complete your webcam configurations. If your VDA does not have Internet access, go to step 3.

   > **Note:**
   >
   > Kernel mismatch might happen between `uname -r` and kernel headers. The mismatch

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> causes the ctxwcamcfg.sh script to fail. To use HDX webcam video compression properly, run **sudo apt-get dist-upgrade**, restart the VDA, and then rerun the ctxwcamcfg.sh script.

If your VDA is deployed on Debian, ensure that it is running on the latest kernel version. Otherwise, run the following commands to update to the latest kernel version:

```
sudo apt-get update
sudo apt-get dist-upgrade
sudo reboot
<!--NeedCopy-->
```

If your VDA is deployed on SUSE 15.3, SUSE 15.2, or SUSE 12.5, run the following commands to update to the latest kernel version and to reboot:

```
zypper up kernel-default
reboot
<!--NeedCopy-->
```

The ctxwcamcfg.sh script helps to:

a) Install the `kernel-devel` and Dynamic Kernel Module Support (DKMS) programs on your VDA.

- `kernel-devel` is used to build a virtual webcam kernel module of the corresponding version.
- DKMS is used to dynamically manage the virtual webcam kernel module.

> **Note:**
>
> When installing the preceding programs on RHEL and CentOS, the `ctxwcamcfg.sh` script installs and enables the following repositories on your VDA:
>
> - Extra Packages for Enterprise Linux (EPEL)
> - RPM Fusion

b) Download the `v4l2loopback` open source code from https://github.com/umlaeute/v4l2loopback and use DKMS to manage `v4l2loopback`.
`v4l2loopback` is a kernel module that allows you to create V4L2 loopback devices.

c) Run the `sudo service ctxwcamsd restart` command. The Linux VDA's webcam service - `ctxwcamsd` - restarts and loads the `v4l2loopback` kernel module for the HDX webcam video compression feature.

3. If your VDA does not have Internet access, build the v4l2loopback kernel module on another machine and then copy it to your VDA.

a) Prepare a build machine that has Internet access and has the same kernel version with your VDA. The `uname -r` command helps to find kernel versions.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) On the build machine, run the `sudo mkdir -p /var/xdl` command.

c) Copy `/var/xdl/configure_*` from your VDA to the build machine under `/var/xdl/`.

d) On the build machine, run the `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` command to build the kernel module. If the command runs successfully, it creates a v4l2loopback.ko file under the `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/` path. Ignore errors that might occur when you run the ctxwcamcfg.sh script.

e) Copy v4l2loopback.ko from the build machine to your VDA and place it under `/opt/Citrix/VDA/lib64/`.

f) On your VDA, run the `sudo service ctxwcamsd restart` command to restart the webcam service and load the v4l2loopback kernel module.

Non-domain-joined Linux VDAs

January 23, 2023

Overview

Non-domain-joined VDAs obliterate the need to join VDAs to Active Directory domains for VDA and user authentication. When creating a non-domain-joined VDA, you generate a public-private key pair for registering the VDA to the cloud control plane. Thus, joining an Active Directory domain is no longer required. When a user launches a session from the non-domain-joined VDA, the VDA creates a local mapping account using the user name that the user uses to log on to Citrix Workspace app. The VDA assigns a random password that the local mapping account uses for SSO and session reconnection. If you change the random password, SSO and session reconnection fail. To disable SSO, see Non-SSO authentication.

> **Important:**
>
> - Non-domain-joined VDAs are supported for Citrix DaaS.
>   - Your control plane must be deployed over Citrix DaaS.
>   - You can deploy non-domain-joined VDAs in a public cloud or on-premises data center. The control plane in Citrix DaaS manages non-domain-joined VDAs.
>   - You can configure Rendezvous V2 to bypass Citrix Cloud Connectors. Otherwise, you must install Cloud Connectors to connect VDAs with your control plane.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - To create non-domain-joined VDAs, you must use Machine Creation Services (MCS).
>   - MCS doesn't support bare metal servers.

Features available for non-domain-joined Linux VDAs

Create local users with specified attributes on non-domain-joined VDAs

When you open a session hosted on a non-domain-joined VDA, the VDA automatically creates a local user with default attributes. The VDA creates the local user based on the user name that you used to log on to Citrix Workspace app. You can also specify user attributes including the user's User Identifier (UID), Group ID (GID), home directory, and login shell. To use this feature, complete the following steps:

1. Run the following command to enable the feature:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent\LocalMappedAccount" -t "REG_DWORD" -v "
     CreateWithUidGid" -d "0x00000001" --force
2 <!--NeedCopy-->
```

2. Specify the following attributes in the `/var/xdl/getuidgid.sh` script under the installation path of the VDA:

Attribute	Required or optional	Description
`uid`	Required	A User Identifier (UID) is a number assigned by Linux to each user on the system. It determines which system resources that the user can access.
`gid`	Required	A Group Identifier (GID) is a number used to represent a specific group.
`homedir`	Optional	The Linux home directory is a directory for a particular user.
`shell`	Optional	A login shell is a shell given to a user upon login to their user account.

The following is an example of the `getuidgid.sh` script:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Make sure that the attributes specified in the script are valid.

```
#!/bin/bash

################################################################################

#
# Citrix Virtual Apps & Desktops For Linux Script: Get uid and gid
    for the user
#
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#

export LC_ALL="en_US.UTF-8"

function get_uid_gid_for_user()
{

echo "uid:12345"
echo "gid:1003"
echo "homedir:/home/$1"
echo "shell:/bin/sh"
 }


get_uid_gid_for_user $1
<!--NeedCopy-->
```

Non-SSO authentication

By default, the Linux VDA has single sign-on (SSO) enabled. Users log on to Citrix Workspace app and to VDA sessions using one set of credentials.
To have users log on to VDA sessions using a different set of credentials, disable SSO on the Linux VDA. For more information, see Non-SSO authentication.

Authentication with Azure Active Directory

The non-domain-joined VDAs that you deploy in Azure integrate with the AAD identity service to provide user authentication. For more information, see Authentication with Azure Active Directory.

Rendezvous V2

Non-domain-joined VDAs are supported for using Rendezvous V2 to bypass Citrix Cloud Connectors. For more information, see Rendezvous V2.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Create non-domain-joined Linux VDAs

Use MCS to create non-domain-joined Linux VDAs in Citrix DaaS. For more information, see Create non-domain-joined Linux VDAs.

Policy support list

January 23, 2023

Linux VDA policy support list

Studio Policy	Key Name	Type	Module	Default Value
Limit clipboard client to session transfer size	LimitClipboardTransferC2H	User	ICA	Disabled (0)
Limit clipboard session to client transfer size	LimitClipboardTransferH2C	User	ICA	Disabled (0)
Use local time of client	UseLocalTimeOfClient	User	ICA\Time Zone Control	Use server time zone
ICA round trip calculation	IcaRoundTripCheckEnabled	Computer	ICA\End User Monitoring	Enabled (1)
ICA round trip calculation interval	IcaRoundTripCheckPeriod	Computer	ICA\End User Monitoring	15
ICA round trip calculations for idle connections	IcaRoundTripCheckWhenIdle	Computer	ICA\End User Monitoring	Disabled (0)
Overall session bandwidth limit	LimitOverallBw	User	ICA\Bandwidth	0
Audio redirection bandwidth limit	LimitAudioBw	User	ICA\Bandwidth	0

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio Policy	Key Name	Type	Module	Default Value
Audio redirection bandwidth limit percent	LimitAudioBwPercent	User	ICA\Bandwidth	0
Client USB device redirection bandwidth limit	LimitUSBBw	User	ICA\Bandwidth	0
Client USB device redirection bandwidth percent	LimitUSBBwPercent	User	ICA\Bandwidth	0
Clipboard redirection bandwidth limit	LimitClipbdBW	User	ICA\Bandwidth	0
Clipboard redirection bandwidth limit percent	LimitClipbdBWPercent	User	ICA\Bandwidth	0
File redirection bandwidth limit	LimitCdmBw	User	ICA\Bandwidth	0
File redirection bandwidth limit percent	LimitCdmBwPercent	User	ICA\Bandwidth	0
Printer redirection bandwidth limit	LimitPrinterBw	User	ICA\Bandwidth	0
Printer redirection bandwidth limit percent	LimitPrinterBwPercent	User	ICA\Bandwidth	0
WebSockets connections	AcceptWebSocketsConnections	Computer	ICA\WebSockets	Prohibited

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio Policy	Key Name	Type	Module	Default Value
WebSockets port number	WebSocketsPort	Computer	ICA\WebSockets	8008
WebSockets trusted origin server list	WSTrustedOriginServerList	Computer	ICA\WebSockets	*
ICA keep alives	SendICAKeepAlives	Computer	**ICA keep alive**	Do not send ICA keep alive messages (0)
ICA keep alive timeout	ICAKeepAliveTimeout	Computer	**ICA keep alive**	60 seconds
ICA listener port number	IcaListenerPortNumber	Computer	ICA	1494
HDX adaptive transport	HDXoverUDP	Computer	ICA	Preferred(2)
Session reliability connections	AcceptSessionReliabilityConnections	Computer	ICA\Session Reliability	Allowed(1)
Reconnection UI transparency level	ReconnectionUiTransparencyLevel	Computer	ICA\Auto Client Reconnect	80%
Session reliability port number	SessionReliabilityPort	Computer	ICA\Session Reliability	2598
Session reliability timeout	SessionReliabilityTimeout	Computer	ICA\Session Reliability	180 s
Auto Client Reconnect	AllowAutoClientReconnect	User	ICA\Auto Client Reconnect	Allowed (1)
Client audio redirection	AllowAudioRedirection	User	Audio	Allowed (1)
Client printer redirection	AllowPrinterRedir	User	Printing	Allowed (1)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio Policy	Key Name	Type	Module	Default Value
Auto-create PDF Universal Printer	AutoCreatePDFPrinter	User	Printing	Disabled (0)
Printer driver mapping and compatibility	DriverMappingList	User	Printing	`"Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny"`
Client clipboard redirection	AllowClipboardRedir	User	Clipboard	Allowed (1)
Client USB device redirection	AllowUSBRedir	User	USB	Prohibited (0)
Client USB device redirection rules	USBDeviceRules	User	USB	“\0”
Moving image compression	MovingImageCompressionConfiguration	User	Thinwire	Enabled (1)
Extra color compression	ExtraColorCompression	User	Thinwire	Disabled (0)
Target minimum frame rate	TargetedMinimumFramesPerSecond	User	Thinwire	10 fps
Target frame rate	FramesPerSecond	User	Thinwire	30 fps
Visual quality	VisualQuality	User	Thinwire	Medium (3)
Use video codec for compression	VideoCodec	User	Thinwire	Use when preferred (3)
Use hardware encoding for video codec	UseHardwareEncodingForVideoCodec	User	Thinwire	Enabled (1)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio Policy	Key Name	Type	Module	Default Value
Allow visually lossless compression	AllowVisuallyLosslessCompression	User	Thinwire	Disabled (0)
Optimize for 3D graphics workload	OptimizeFor3dWorkload	User	Thinwire	Disabled (0)
Preferred color depth for simple graphics	PreferredColorDepth	User	Thinwire	24 bits per pixel(1)
Audio quality	SoundQuality	User	Audio	High –high definition audio (2)
Client microphone redirection	AllowMicrophoneRedir	User	Audio	Allowed (1)
Maximum number of sessions	MaximumNumberOfSessions	Computer	Load Management	250
Concurrent logons tolerance	ConcurrentLogonsTolerance	Computer	Load Management	2
Enable auto update of Controllers	EnableAutoUpdateOfControllers	Computer	Virtual Delivery Agent Settings	Allowed (1)
Clipboard selection update mode	ClipboardSelectionUpdateMode	User	Clipboard	3
Primary selection update mode	PrimarySelectionUpdateMode	User	Clipboard	3
Max speex quality	MaxSpeexQuality	User	Audio	5
Auto connect client drives	AutoConnectDrives	User	File redirection/CDM	Enabled (1)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Studio Policy	Key Name	Type	Module	Default Value
Client optical drives	AllowCdromDrives	User	File redirection/CDM	Allowed (1)
Client fixed drives	AllowFixedDrives	User	File redirection/CDM	Allowed (1)
Client floppy drives	AllowFloppyDrives	User	File redirection/CDM	Allowed (1)
Client network drives	AllowNetworkDrives	User	File redirection/CDM	Allowed (1)
Client drive redirection	AllowDriveRedir	User	File redirection/CDM	Allowed (1)
Read-only client drive access	ReadOnlyMappedDrive	User	File redirection/CDM	Disabled (0)
Automatic keyboard display	AllowAutoKeyboardPopup	User	MRVC	Disabled (0)
Allow file transfer between desktop and client	AllowFileTransfer	User	File Transfer	Allowed
Download file from desktop	AllowFileDownload	User	File Transfer	Allowed
Upload file to desktop	AllowFileUpload	User	File Transfer	Allowed
Session idle timer	EnableSessionIdleTimer	User	Session Timers	Enabled (1)
Session idle timer interval	SessionIdleTimerInterval	User	Session Timers	1440 minutes
Disconnected session timer	EnableSessionDisconnectTimer	User	Session Timers	Disabled (0)
Disconnected session timer interval	SessionDisconnectTimerPeriod	User	Session Timers	1440 minutes

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

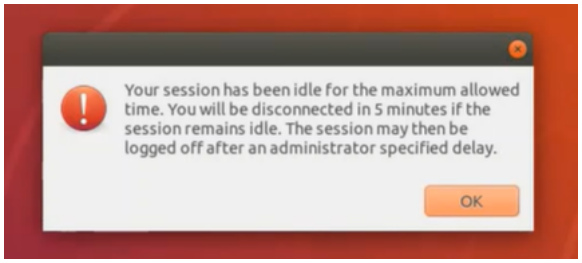
> **Note:**
>
> Only the Windows Virtual Delivery Agent (VDA) supports audio over User Datagram Protocol (UDP). The Linux VDA does not. For more information, see Audio over User Datagram Protocol (UDP) Real-time Transport.

You can use the following Citrix policy settings to configure session connection timers in Citrix Studio:

- **Session idle timer**: Determines whether to enforce a time limit for idle sessions.
- **Session idle timer interval**: Sets a time limit for idle sessions. If **Session idle timer** is **Enabled** and an active session has not received user input during the set time, the session disconnects.
- **Disconnected session timer**: Determines whether to enforce a time limit for disconnected sessions.
- **Disconnected session timer interval**: Sets an interval before a disconnected session is logged off.

When you update any of the policy settings, ensure that they are consistent across your deployment.

A warning message appears when your time limit for idle sessions expires. See the following screen capture for an example. Pressing **OK** closes the warning message but cannot keep your session active. To keep your session active, provide user input to reset the idle timer.



The following policies can be configured in Citrix Studio Version 7.12 and later.

- MaxSpeexQuality

  Value (integer): [0–10]

  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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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 rate. 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

- PrimarySelectionUpdateMode

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

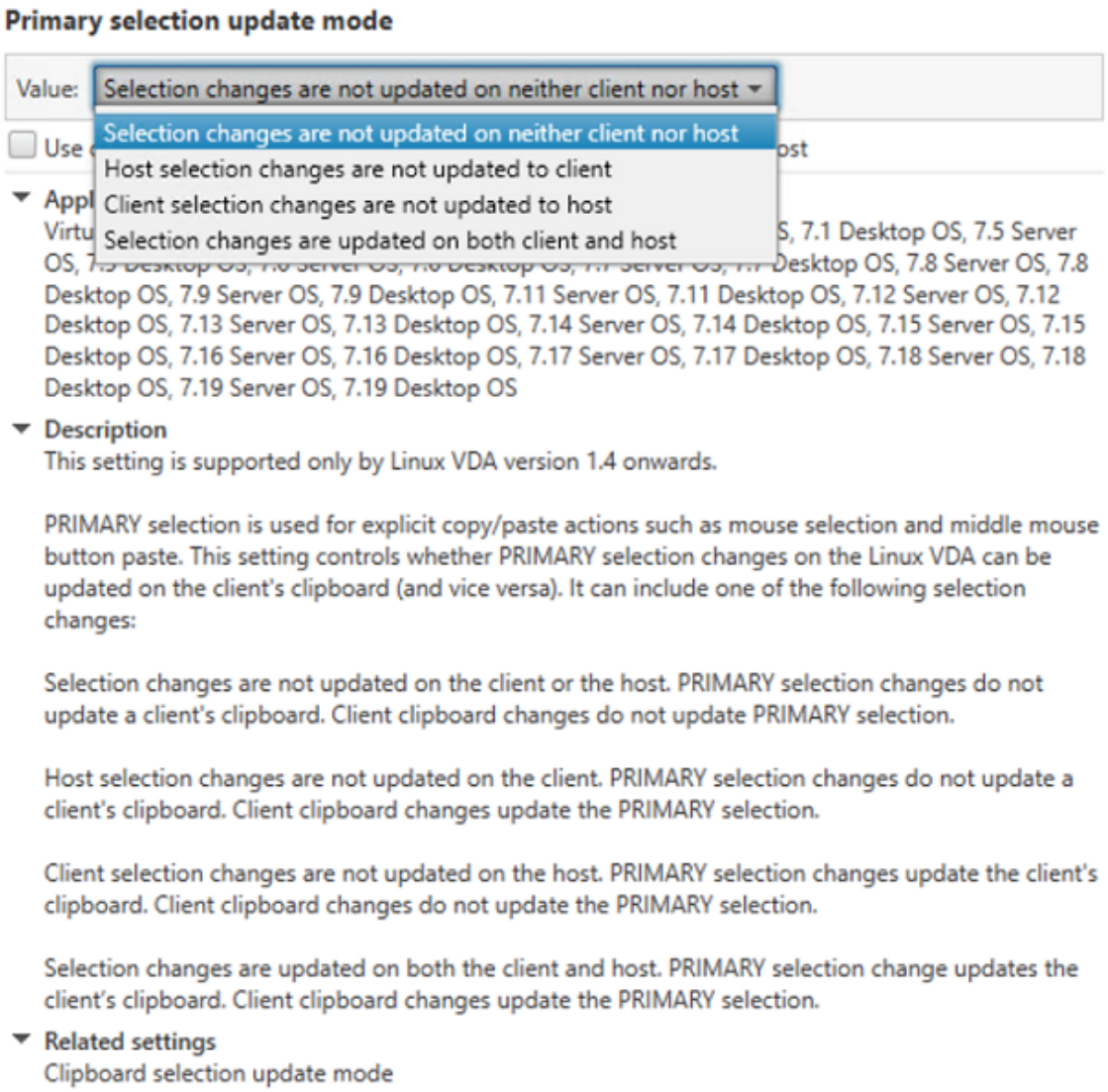
  Default value: 3

  Details:

  Primary selection is used when you select data and paste it by pressing the middle mouse button.

  This policy controls whether primary selection changes on the Linux VDA and the client can update the clipboard on each other. There are four value options:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Selection changes are not updated on neither client nor host**
  Primary selection changes on the Linux VDA do not update the clipboard on the client. Primary selection changes on the client do not update the clipboard on the Linux VDA.
- **Host selection changes are not updated to client**
  Primary selection changes on the Linux VDA do not update the clipboard on the client. Primary selection changes on the client update the clipboard on the Linux VDA.
- **Client selection changes are not updated to host**
  Primary selection changes on the Linux VDA update the clipboard on the client. Primary selection changes on the client do not update the clipboard on the Linux VDA.
- **Selection changes are updated on both client and host**
  Primary selection changes on the Linux VDA update the clipboard on the client. Primary selection changes on the client update the clipboard on the Linux VDA. This option is the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

default value.

Related Setting: Clipboard selection update mode

- ClipboardSelectionUpdateMode

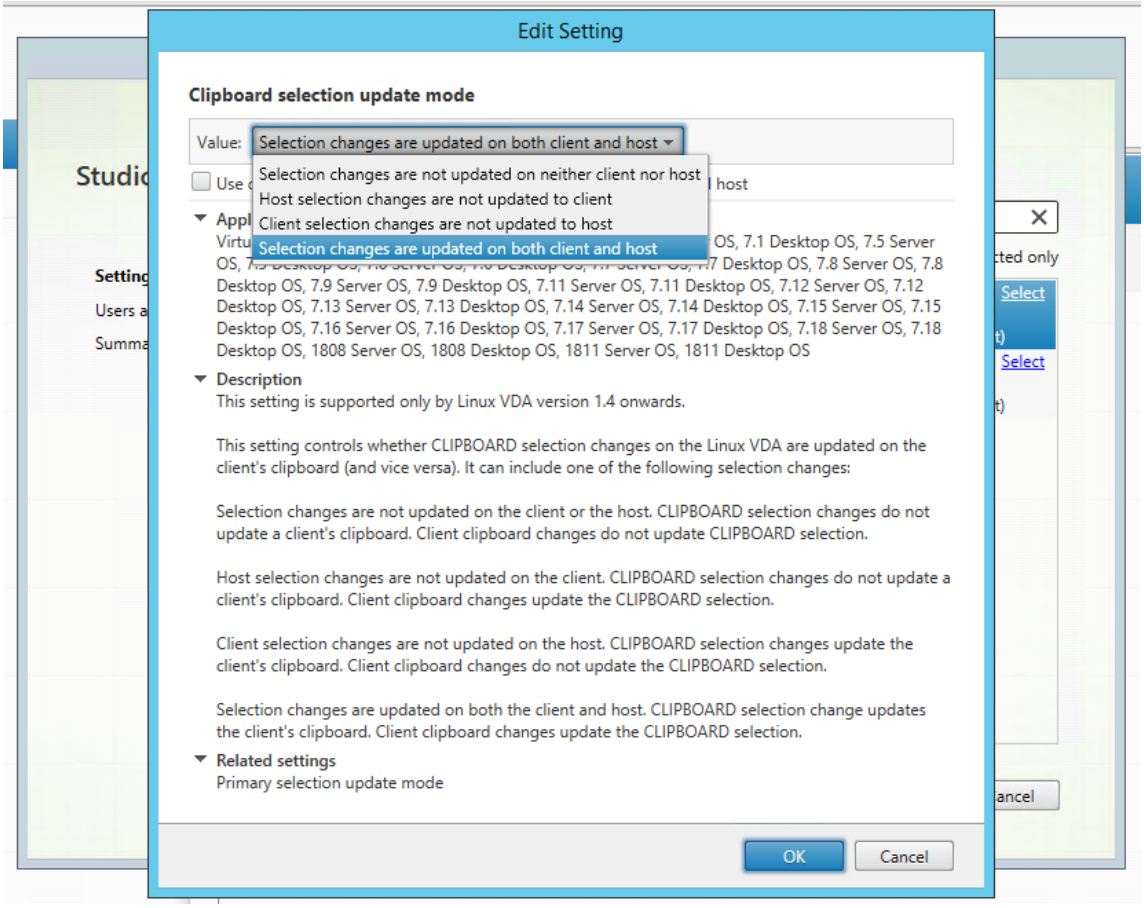
  Value (enum): [0, 1, 2, 3]

  Default value: 3

  Details:

  Clipboard selection is used when you select some data and explicitly request it to be "copied" to the clipboard, such as by selecting "Copy"from the shortcut menu. Clipboard selection is primarily used in connection with Microsoft Windows clipboard operations while primary selection is unique to Linux.

  This policy controls whether clipboard selection changes on the Linux VDA and the client can update the clipboard on each other. There are four value options:



  - **Selection changes are not updated on neither client nor host**
    Clipboard selection changes on the Linux VDA do not update the clipboard on the client. Clipboard selection changes on the client do not update the clipboard on the Linux VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Host selection changes are not updated to client**
  Clipboard selection changes on the Linux VDA do not update the clipboard on the client. Clipboard selection changes on the client update the clipboard on the Linux VDA.
- **Client selection changes are not updated to host**
  Clipboard selection changes on the Linux VDA update the clipboard on the client. Clipboard selection changes on the client do not update the clipboard on the Linux VDA.
- **Selection changes are updated on both client and host**
  Clipboard selection changes on the Linux VDA update the clipboard on the client. Clipboard selection changes on the client update the clipboard on the Linux VDA. This option is the default value.

Related Setting: Primary selection update mode

> **Note:**
>
> The Linux VDA supports both clipboard selection and primary selection. To control the copy and paste behaviors between the Linux VDA and the client, we recommend that you set both clipboard selection update mode and primary selection update mode to the same value.

Printing

January 23, 2023

This section contains the following topics:

- Printing best practices
- PDF printing

Printing best practices

January 23, 2023

This article provides information about printing best practices.

Installation

The Linux VDA requires both **cups** and **foomatic** filters. The filters are installed when you install the VDA. You can also install the filters manually based on the distribution. For example:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

On RHEL 7:

```
sudo yum  –y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```

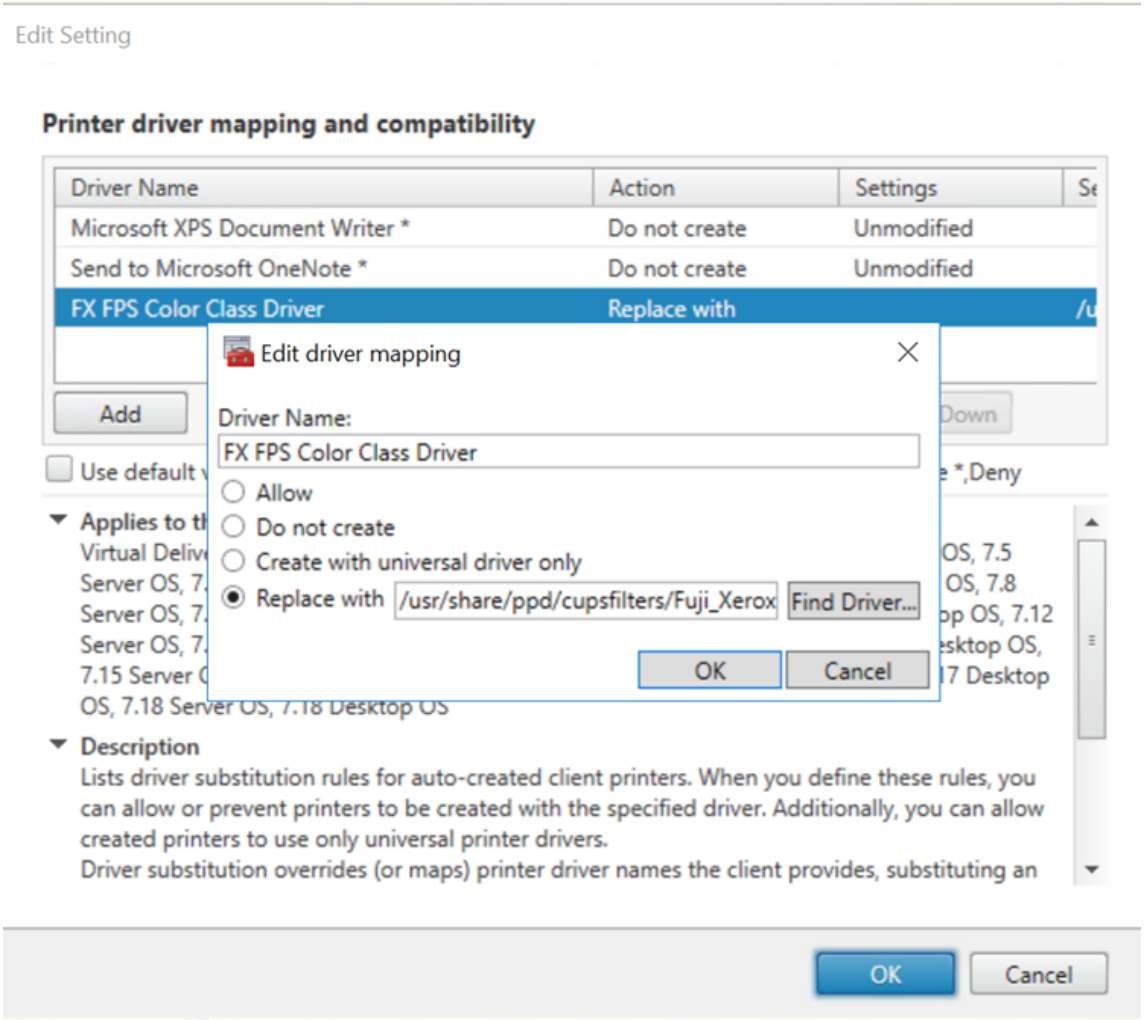
Configuration

There are three types of Universal Printer Driver supplied by Citrix (postscript, pcl5, and pcl6). However, the Universal Printer Driver might not be compatible with your client printer. In this case, your only option in earlier releases was to edit the ~/.CtxlpProfile$CLIENT_NAME configuration file. Starting with Version 1906, you can choose to configure the **Printer driver mapping and compatibility** policy in Citrix Studio instead.

To configure the **Printer driver mapping and compatibility** policy in Citrix Studio:

1. Select the **Printer driver mapping and compatibility** policy.
2. Click **Add**.
3. Fill in **Driver name** with the driver name of the client printer. If you are using Citrix Workspace app for Linux, fill in the printer name instead.
4. Choose **Replace with** and type in the absolute path of the driver file on the VDA.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Note:

- Only PPD driver files are supported.
- Other options of the **Printer driver mapping and compatibility** policy are not supported. Only **Replace with** takes effect.

Usage

You can print from both published desktops and published applications. Only the client-side default printer is mapped into a Linux VDA session. The printer names are different for desktops and applications:

- For published desktops:
  `CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`
- For published applications:
  `CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> If the same user opens both a published desktop and a published application, both printers are available to the session. Printing on a desktop printer in a published application session, or printing on an application printer in a published desktop fails.

Troubleshooting

Unable to print

When printing is not working correctly, check the print daemon, **ctxlpmngt**, and the CUPs framework.

The print daemon, **ctxlpmngt**, is a per-session process and must be running for the length of the session. Run the following command to verify that the printing daemon is running. If **ctxlpmngt** is not running, start **ctxlpmngt** manually from a command line.

```
ps –ef | grep ctxlpmngt
<!--NeedCopy-->
```

If printing is still not working, check the CUPS framework. The **ctxcups** service is used for printer management and communicates with the Linux CUPS framework. It is a single process per machine and can be checked by running the following command:

```
service ctxcups status
<!--NeedCopy-->
```

Extra steps for collecting CUPS logs

To collect CUPS logs, run the following commands to configure the CUPS service file. Otherwise, CUPS logs cannot be recorded in **hdx.log**:

```
sudo service cups stop

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

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> This configuration is made only for collecting the full printing log when an issue arises. Under normal circumstances, this configuration is not recommended because it breaks CUPS security.

Print output is garbled

An incompatible printer driver can cause garbled output. 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=
<!--NeedCopy-->
```

> **Important:**
>
> The **printername** is a field containing the name of the current client-side default printer. It is a read-only value. Do not edit it.
>
> The fields **ppdpath**, **model**, and **drivertype** cannot 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 using the **model**= option. You can find the current model name of the printer by using 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

  <!--NeedCopy-->
  ```

  You can then set the model to match the printer:

  ```
  model=xerox/ph3115.ppd.gz
  <!--NeedCopy-->
  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

- There are three types of Universal Printer Driver supplied by Citrix (postscript, pcl5, and pcl6). You can configure the driver type based on your printer properties.

  For example, if the client default printer driver type is PCL5, set **drivertype** to:

  ```
  drivertype=pcl5
  <!--NeedCopy-->
  ```

Output size is zero

Try different types of printers. And try 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, an issue can occur.

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

1. Log on to a published desktop session.
2. Run the **vi ~/.CtxlpProfile$CLIENT_NAME** command.
3. Add the following field to save the spool file on the Linux VDA:

   ```
   deletespoolfile=no
   <!--NeedCopy-->
   ```

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. Check whether the spool is empty. If the spool file is zero, it represents an issue. Contact Citrix Support (and provide the printing log) for more 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. Check whether the content is correct.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

If the spool file is PCL, or if the client OS is Windows, copy the spool file to the client and print it on the client-side printer by using a different printer driver.

8. Change the mapped printer to use a different printer driver. The following example uses 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
   <!--NeedCopy-->
   ```

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

   d) Retain the cups-ctx connection, then click Continue to change the printer driver.

   e) In the **Make** and **Model** fields, choose a different printer driver from the Citrix UPD driver. For example, if the CUPS-PDF virtual printer is installed, select the Generic CUPS-PDF Printer driver. Save the change.

   f) If this process succeeds, configure the PPD file path of the driver in **.CtxlpProfile$CLIENT_NAME** to allow the mapped printer to use the newly selected driver.

Known issues

The following issues have been identified during printing on 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 document is transferred over the server connection. On slow connections, the transfer 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 changing the CUPS configuration file: **/etc/cups/cupsd.conf**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Locate the current policy name configured in the file:

```
DefaultPolicy default
```

If the policy name is *default*, add the following lines to 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>
<!--NeedCopy-->
```

PDF printing

January 23, 2023

Using a version of Citrix Workspace app that supports PDF printing, you can print PDFs converted from within the Linux VDA sessions. Session print jobs are sent to the local machine where Citrix Workspace app is installed. On the local machine, you can open PDFs using your PDF viewer of choice and print them on your printer of choice.

The Linux VDA supports PDF printing on the following versions of Citrix Workspace app:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Receiver for HTML5 Versions 2.4 through 2.6.9, Citrix Workspace app 1808 for HTML5 and later
- Citrix Receiver for Chrome Versions 2.4 through 2.6.9, Citrix Workspace app 1808 for Chrome and later
- Citrix Workspace app 1905 for Windows and later

Configuration

Apart from using a version of Citrix Workspace app that supports PDF printing, enable the following policies in Citrix Studio:

- **Client Printer Redirection** (enabled by default)
- **Auto-create PDF Universal Printer** (disabled by default)

With these policies enabled, a print preview appears on the local machine for you to select a printer when you click **Print** within your launched session. See the Citrix Workspace app documentation for information about setting default printers.

Remote PC Access

February 1, 2023

Overview

Remote PC Access is an extension of Citrix Virtual Apps and Desktops. It enables organizations to easily allow employees to access their physical office PCs remotely in a secure manner. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work.

Remote PC Access uses the same Citrix Virtual Apps and Desktops components that deliver virtual desktops and applications. The requirements and process of deploying and configuring Remote PC Access are the same as the requirements and process required for deploying Citrix Virtual Apps and Desktops. This uniformity provides a consistent and unified administrative experience. Users receive the best user experience by using Citrix HDX to deliver their remote office PC sessions.

For more information, see Remote PC Access in the Citrix Virtual Apps and Desktops documentation.

Considerations

These considerations are specific to the Linux VDA:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- On physical machines, use the Linux VDA only in non-3D mode. Due to limitations on NVIDIA's driver, the local screen of the PC cannot be blacked out when HDX 3D mode is enabled. Showing this screen is a potential security risk.
- Use machine catalogs of type single-session OS for physical Linux machines.
- Automatic user assignment is not available for Linux machines. With automatic user assignment, users are assigned to their machines automatically when they log on locally to the PCs. This logon occurs without administrator intervention. Citrix Workspace app on the client helps users access the applications and data on the office PC within the Remote PC Access desktop session.
- If users are already logged on to their PCs locally, attempts to launch the PCs from StoreFront fail.
- Power saving options are not available for Linux machines.

Configuration

To deliver Linux PC sessions, install the Linux VDA on target PCs, create a machine catalog of the **Remote PC Access** type, and create a Delivery Group to make the PCs in the machine catalog available for users who request access. The following section details the procedure:

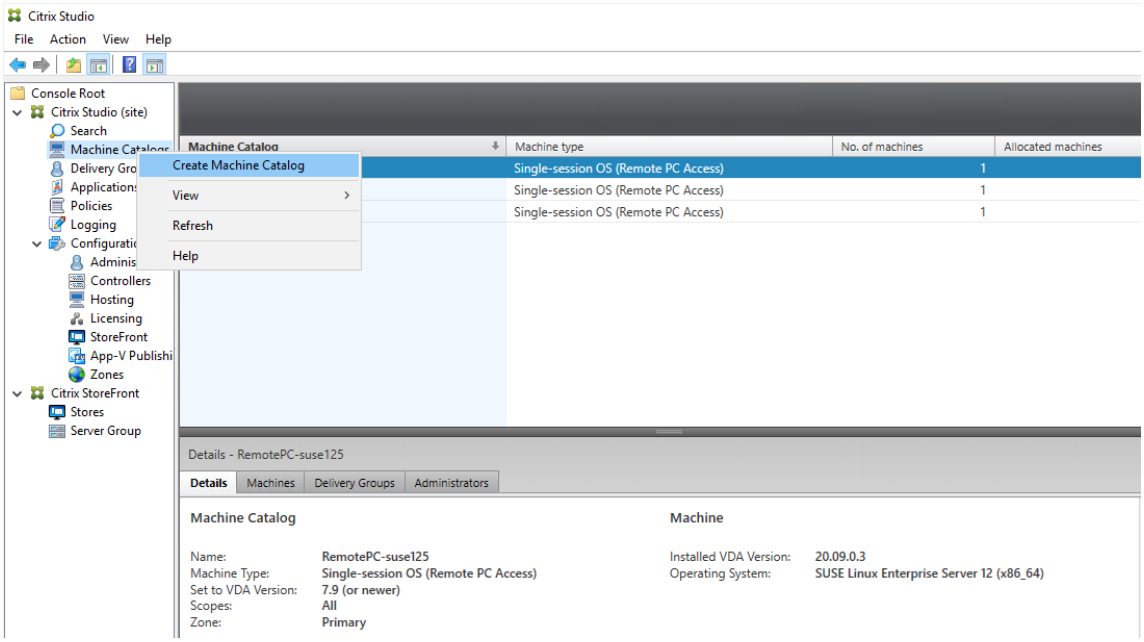
Step 1 - Install the Linux VDA on target PCs

We recommend you use easy install to install the Linux VDA. During the installation, set the value of the `CTX_XDL_VDI_MODE` variable to `Y`.

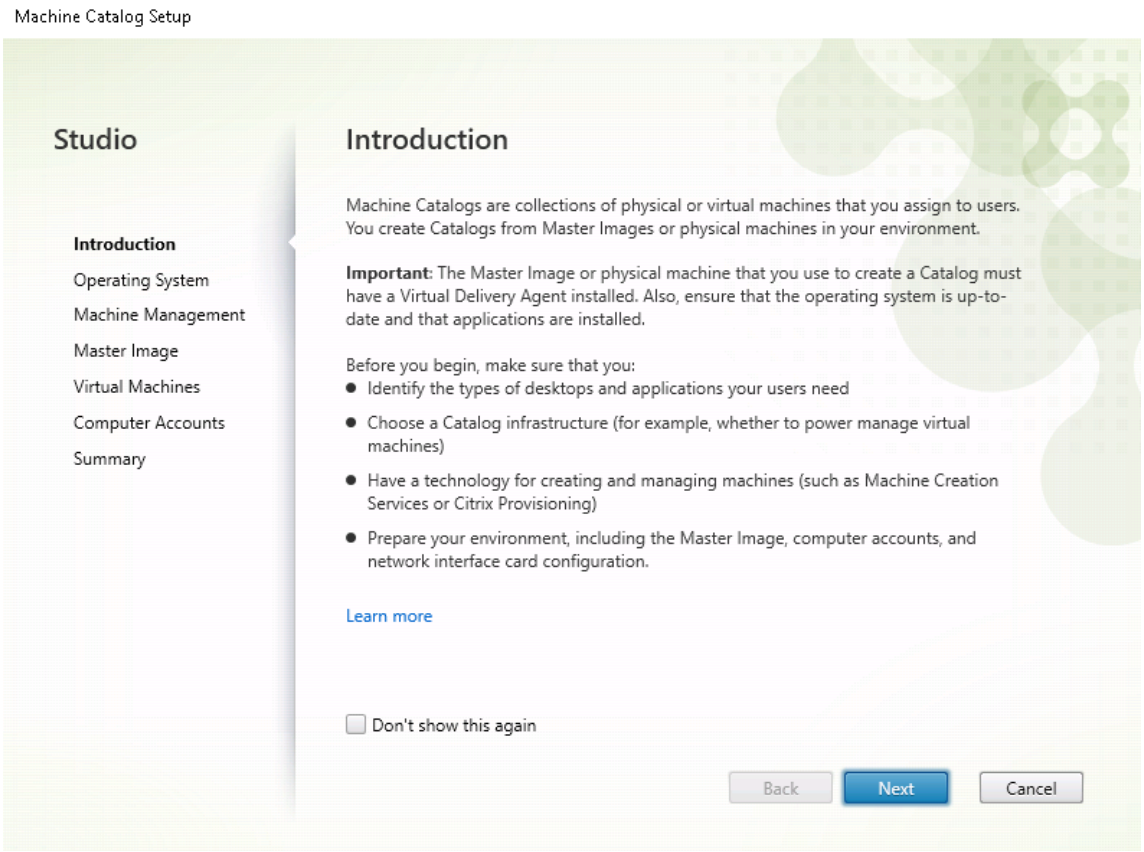
Step 2 - Create a machine catalog of the Remote PC Access type

1. In Citrix Studio, right-click **Machine Catalogs** and select **Create Machine Catalog** from the shortcut menu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

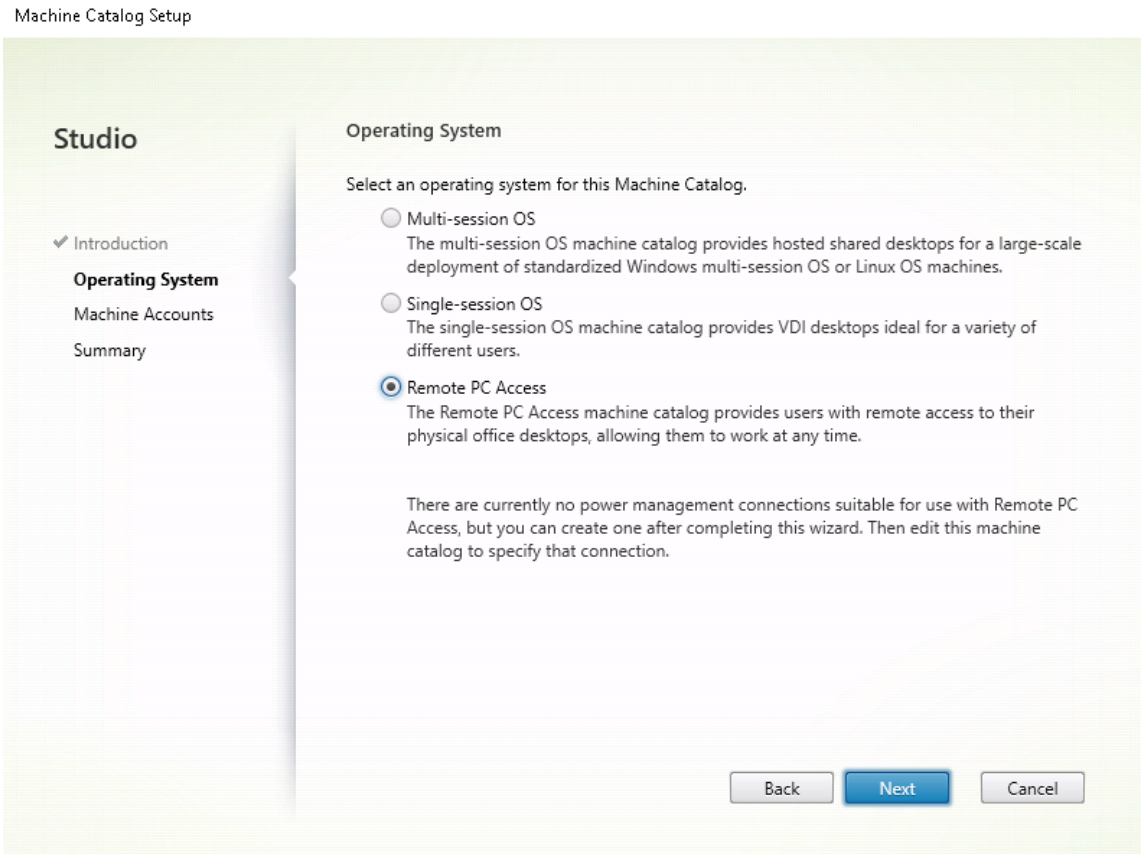


2. Click **Next** on the **Introduction** page.



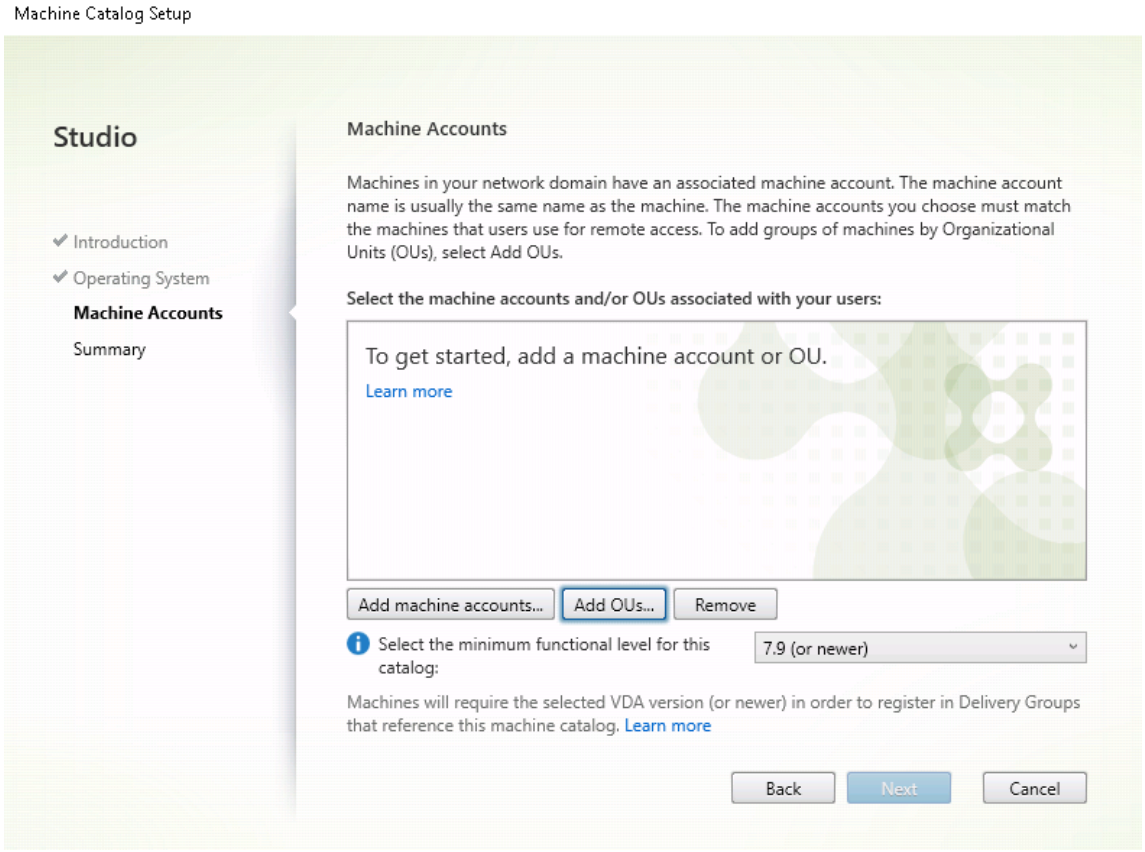
3. Select **Remote PC Access** on the **Operating System** page.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



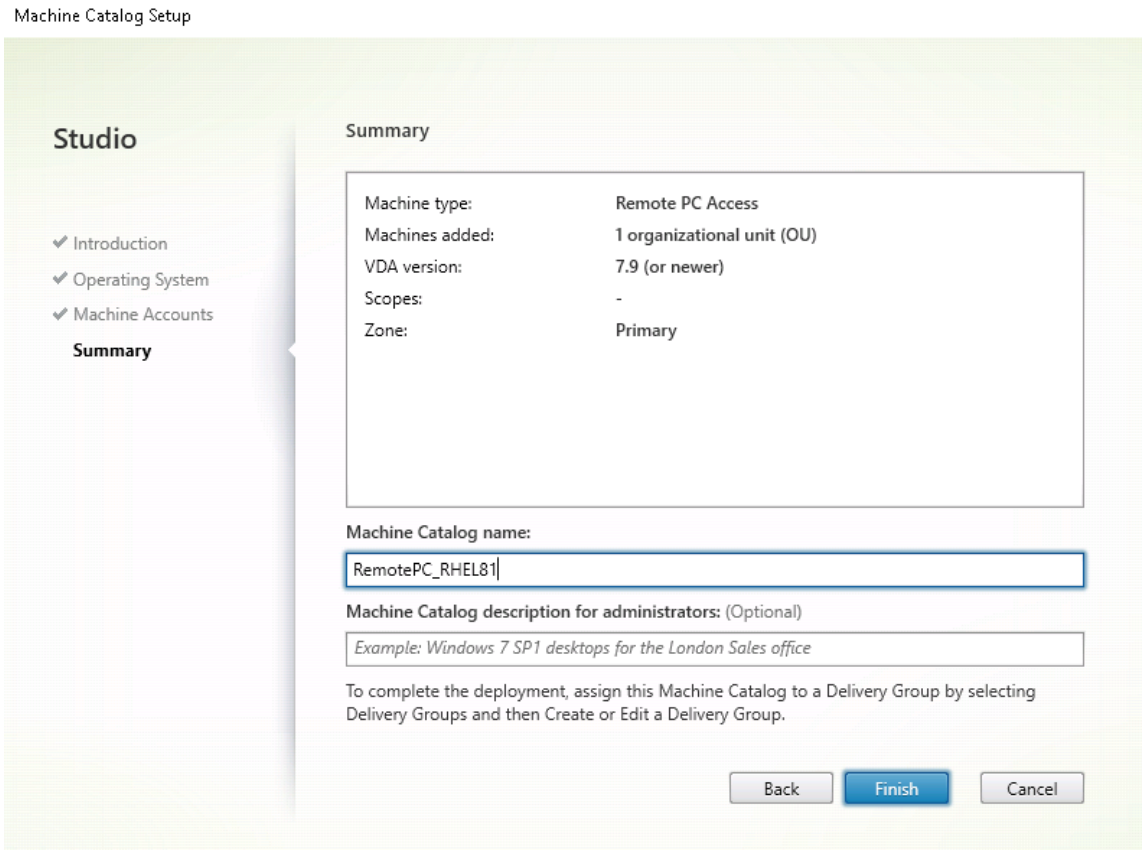
4. Click **Add OUs** to select OUs that contain the target PCs, or click **Add machine accounts** to add individual machines to the machine catalog.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

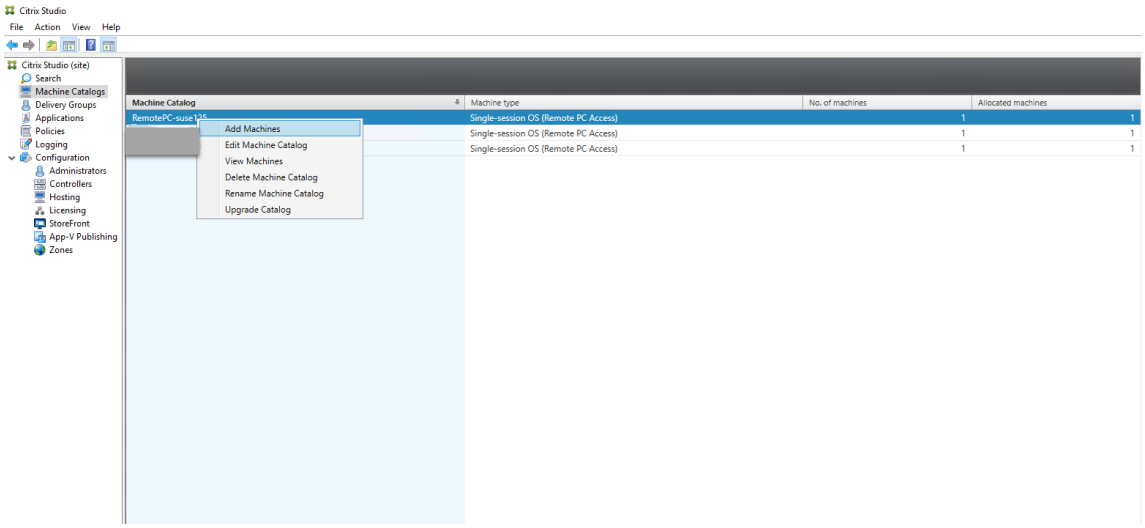


5. Name the machine catalog.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



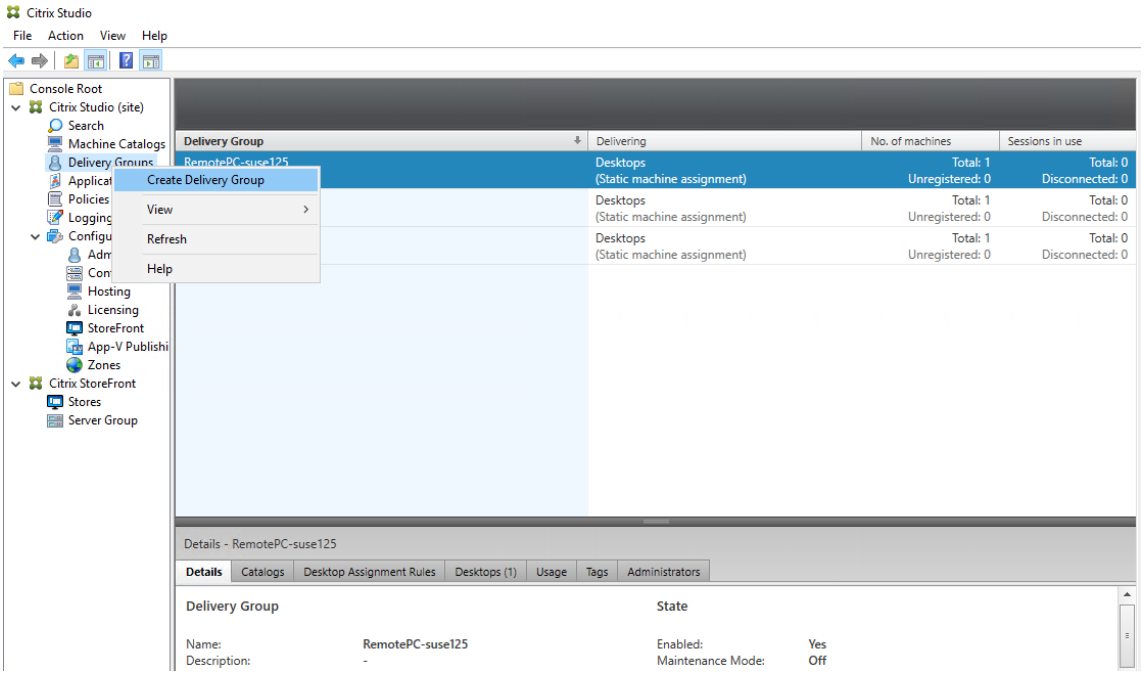
6. (Optional) Right-click the machine catalog to perform relevant operations.



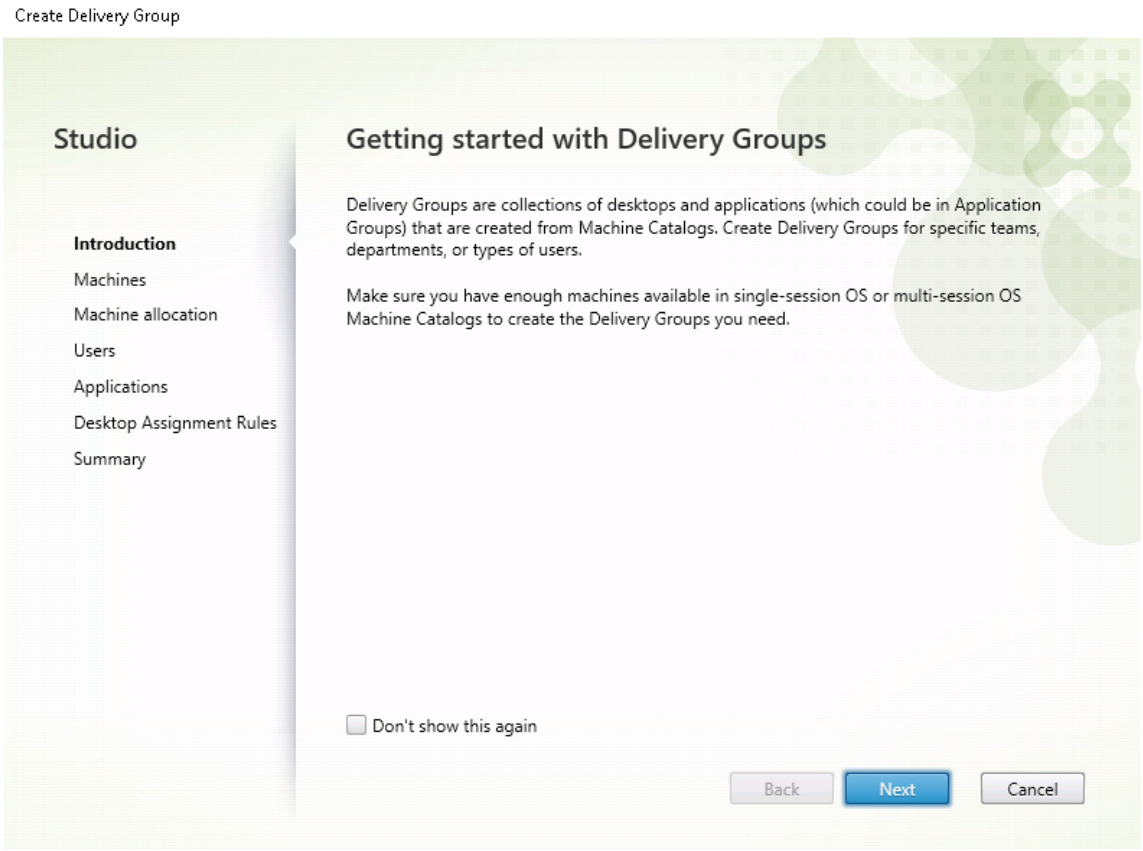
Step 3 - Create a Delivery Group to make the PCs in the machine catalog available for users who request access

1. In Citrix Studio, right-click **Delivery Groups** and select **Create Delivery Group** from the shortcut menu.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

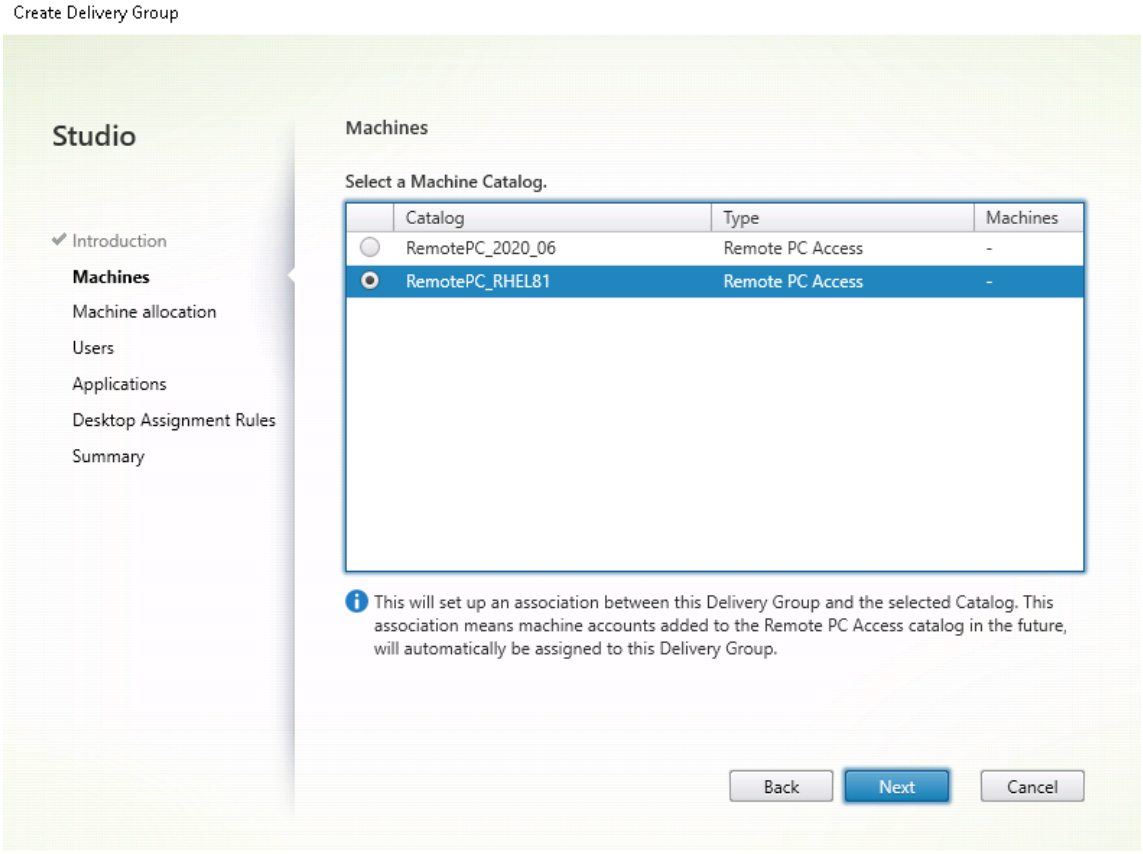


2. Click **Next** on the **Getting started with Delivery Groups** page.



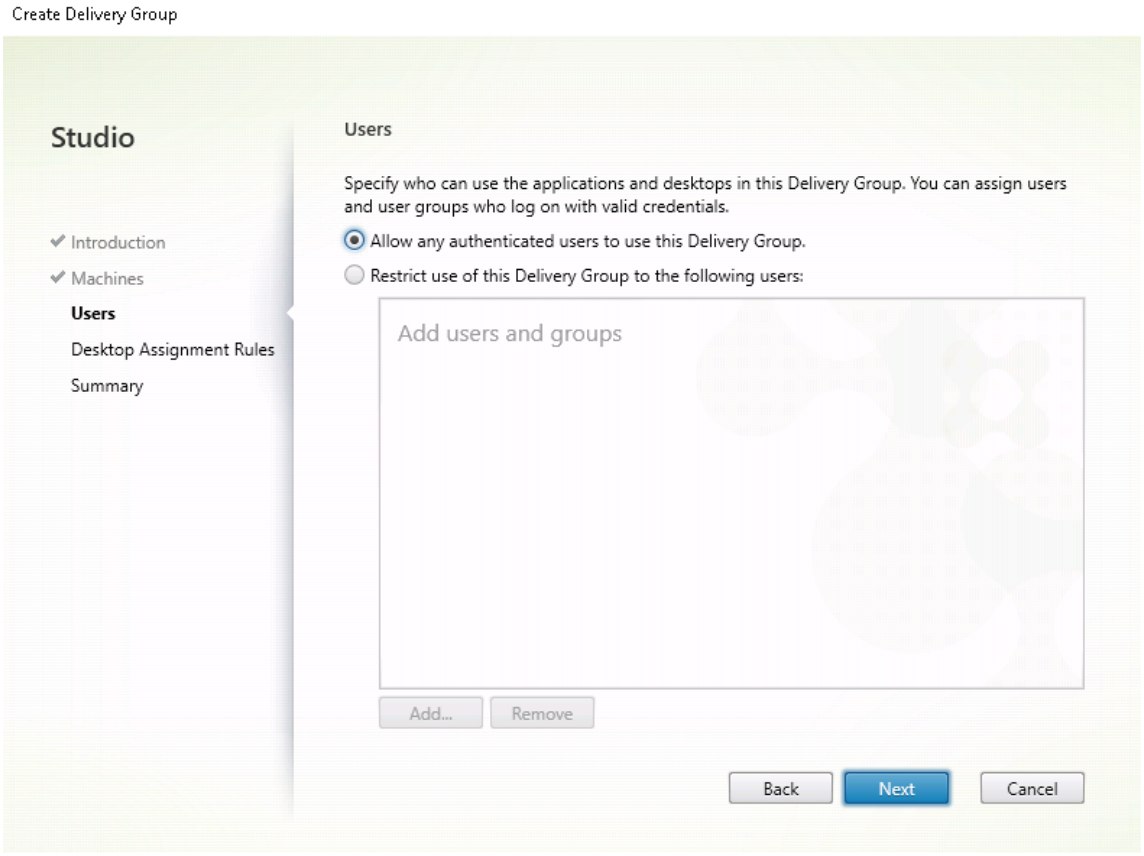
3. Select the machine catalog created in Step 2 to associate it with the Delivery Group.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Add users who can access the PCs in the machine catalog. The users you add can use Citrix Workspace app on a client device to access the PCs remotely.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Wake on LAN

Remote PC Access supports Wake on LAN, which gives users the ability to turn on physical PCs remotely. This feature enables users to keep their office PCs turned off when not in use to save energy costs. It also enables remote access when a machine has been turned off inadvertently.

With the Wake on LAN feature, the magic packets are sent directly from the VDA running on the PC to the subnet in which the PC resides when instructed by the delivery controller. This allows the feature to work without dependencies on extra infrastructure components or third-party solutions for delivery of magic packets.

The Wake on LAN feature differs from the legacy SCCM-based Wake on LAN feature. For information on the SCCM-based Wake on LAN, see Wake on LAN –SCCM-integrated.

System requirements

The following are the system requirements for using the Wake on LAN feature:

- Control plane:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)
  - Citrix Virtual Apps and Desktops 2012 or later

- Physical PCs:
  - VDA version 2012 or later
  - Wake on LAN enabled in BIOS and on the NIC

Configure Wake on LAN

Currently, the configuration of integrated Wake on LAN is only supported using PowerShell.

To configure Wake on LAN:

1. Create the Remote PC Access machine catalog if you do not have one already.
2. Create the Wake on LAN host connection if you do not have one already.

   > **Note:**
   >
   > To use the Wake on LAN feature, if you have a host connection of the "Microsoft Configuration Manager Wake on LAN"type, create a host connection.

3. Retrieve the Wake on LAN host connection's unique identifier.
4. Associate the Wake on LAN host connection with a machine catalog.

   To create the Wake on LAN host connection:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
            -Name $connectionName `
            -HypervisorAddress "N/A" `
            -UserName "woluser" `
            -Password "wolpwd" `
            -ConnectionType Custom `
            -PluginId VdaWOLMachineManagerFactory `
            -CustomProperties "<CustomProperties></
               CustomProperties>" `
            -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -
       HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

When the host connection is ready, run the following commands to retrieve the host connection's unique identifier:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>
    "
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

After you retrieve the connection's unique identifier, run the following commands to associate the connection with the Remote PC Access machine catalog:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

5. Enable Wake on LAN in BIOS and on the NIC on each VM in the machine catalog.

   Note: The method for enabling Wake on LAN varies with different machine configurations.

   - To enable Wake on LAN in BIOS:
     a) Enter BIOS and enable the Wake on LAN feature.
        The method for accessing BIOS depends on the manufacturer of your motherboard and the BIOS vendor the manufacturer has selected.
     b) Save your settings and restart the machine.
   - To enable Wake on LAN on the NIC:
     a) Run the `sudo ethtool <NIC>` command to check whether your NIC supports magic packets.
        `<NIC>` is the device name of your NIC, for example, `eth0`. The `sudo ethtool <NIC>` command provides output about the capabilities of your NIC:
        - If the output contains a line similar to `Supports Wake-on: <letters>` where `<letters>` contains the letter `g`, your NIC supports the Wake on LAN magic packet method.
        - If the output contains a line similar to `Wake-on: <letters>` where `<letters>` contains the letter `g` and does not contain the letter `d`, the Wake on LAN magic packet method is enabled. However, if `<letters>` contains the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

letter `d`, it indicates that the Wake on LAN feature is disabled. In this case, enable Wake on LAN by running the `sudo ethtool -s <NIC> wol g` command.

b) On most distributions, the `sudo ethtool -s <NIC> wol g` command is required after each startup. To persistently set this option, complete the following steps based on your distributions:

Ubuntu:

Add the `up ethtool -s <NIC> wol g` line to the interface configuration file `/etc/network/interfaces`. For example:

```
# ifupdown has been replaced by netplan(5) on this system.
    See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
# sudo apt install ifupdown
auto eth0
iface eth0 inet static
           address 10.0.0.1
           netmask 255.255.240.0
           gateway 10.0.0.1
           up ethtool -s eth0 wol g
<!--NeedCopy-->
```

RHEL/SUSE:

Add the following `ETHTOOL_OPTS` parameter to the interface configuration file `/etc/sysconfig/network-scripts/ifcfg-<NIC>`:

```
ETHTOOL_OPTS="-s ${
 DEVICE }
  wol g"
<!--NeedCopy-->
```

Design considerations

When you are planning to use Wake on LAN with Remote PC Access, consider the following:

- Multiple machine catalogs can use the same Wake on LAN host connection.
- For a PC to wake up another PC, both PCs must be in the same subnet and use the same Wake on LAN host connection. It does not matter if the PCs are in the same or different machine catalogs.
- Host connections are assigned to specific zones. If your deployment contains more than one zone, you need a Wake on LAN host connection in each zone. The same applies to machine catalogs.
- Magic packets are broadcasted using the global broadcast address 255.255.255.255. Ensure that the address is not blocked.
- There must be at least one PC turned on in the subnet - for every Wake on LAN connection - to be able to wake up machines in that subnet.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Operational considerations

The following are considerations for using the Wake on LAN feature:

- The VDA must register at least once before the PC can be woken up using the integrated Wake on LAN feature.
- Wake on LAN can only be used to wake up PCs. It does not support other power actions, such as restart or shut down.
- After the Wake on LAN connection is created, it is visible in Studio. However, editing its properties within Studio is not supported.
- Magic packets are sent in one of the two ways:
  - When a user tries to launch a session to their PC and the VDA is unregistered
  - When an administrator sends a power on command manually from Studio or PowerShell
- Because the delivery controller is unaware of a PC's power state, Studio displays **Not Supported** under power state. The delivery controller uses the VDA registration state to determine whether a PC is on or off.

More resources

The following are other resources for Remote PC Access:

- Solution design guidance: Remote PC Access Design Decisions.
- Examples of Remote PC Access architectures: Reference Architecture for Citrix Remote PC Access Solution.

Session

January 23, 2023

This section contains the following topics:

- Adaptive transport
- Logon with a temp home directory
- Publish applications
- Session reliability
- Rendezvous V1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Rendezvous V2
- Secure user sessions using TLS
- Secure user sessions using DTLS

Adaptive transport

January 29, 2023

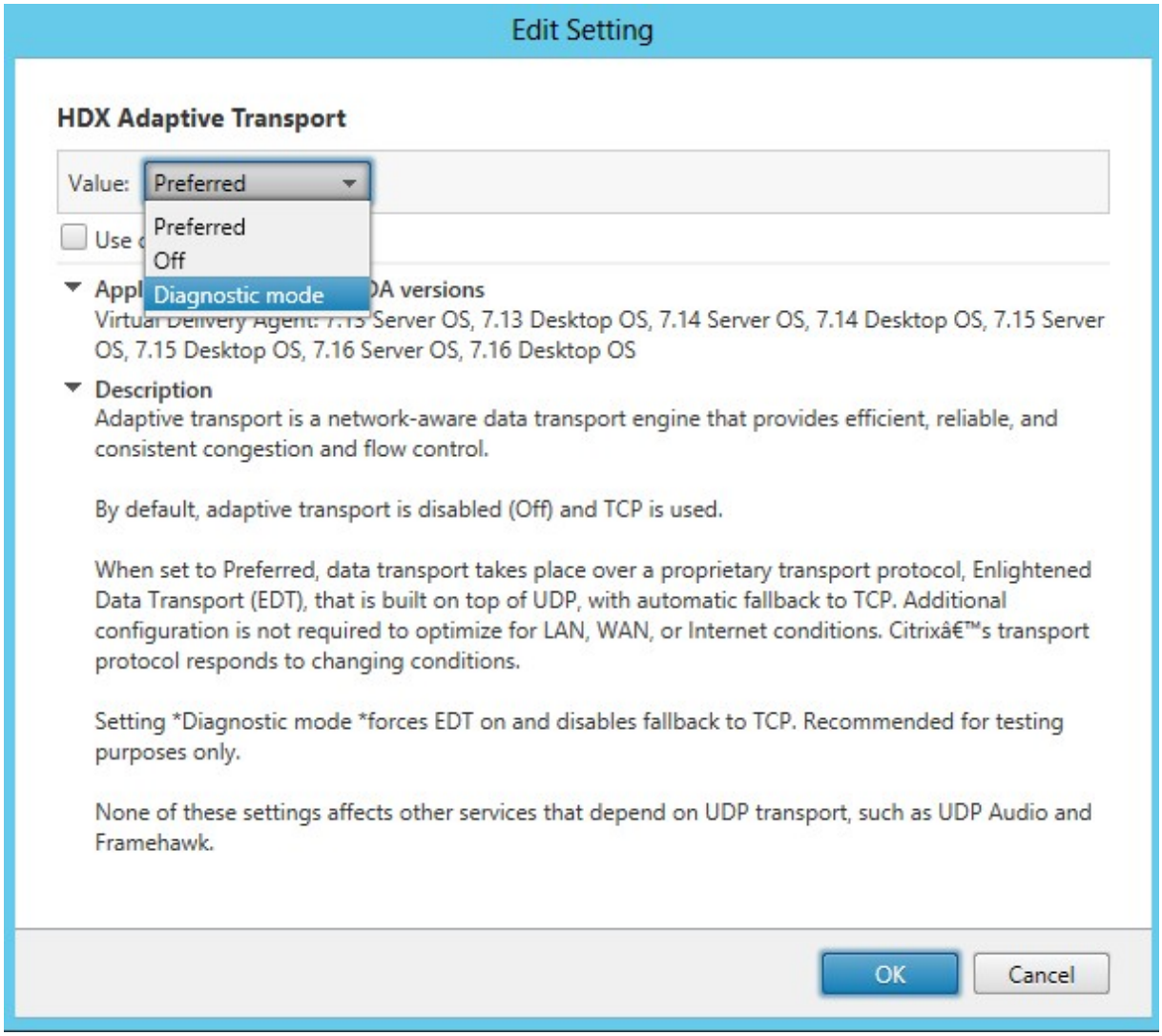
Adaptive transport is a data transport mechanism for Citrix Virtual Apps and Desktops. It is faster, more scalable, improves application interactivity, and is more interactive on challenging long-haul WAN and internet connections. For more information about adaptive transport, see Adaptive transport.

Enable adaptive transport

In Citrix Studio, verify that the **HDX Adaptive Transport** policy is set to **Preferred** or **Diagnostic mode**. **Preferred** is selected by default.

- **Preferred**: Adaptive transport over Enlightened Data Transport (EDT) is used when possible, with fallback to TCP.
- **Diagnostic mode**: EDT is forced on and fallback to TCP is disabled.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Disable adaptive transport

To disable adaptive transport, set the **HDX Adaptive Transport** policy to **Off** in Citrix Studio.

Check whether adaptive transport is enabled

To check whether UDP listeners are running, run the following command.

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

In normal circumstances, the output is similar to the following.

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
udp        0      0 :::1494                 :::*
<!--NeedCopy-->
```

EDT MTU discovery

EDT automatically determines the Maximum Transmission Unit (MTU) when establishing a session. Doing so prevents EDT packet fragmentation that might result in performance degradation or failure to establish a session.

Minimum requirements:

- Linux VDA 2012
- Citrix Workspace app 1911 for Windows
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- Session reliability must be enabled

If using a client platform or version that does not support this feature, you can configure a custom EDT MTU that is appropriate for your environment. For more information, see Knowledge Center article CTX231821.

> **Warning:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of **Registry Editor** can be solved. Use **Registry Editor** at your own risk. Be sure to back up the registry before you edit it.

Enable or disable EDT MTU discovery on the VDA

EDT MTU discovery is disabled by default.

- To enable EDT MTU discovery, set the `MtuDiscovery` registry key by using the following command, restart the VDA, and wait for the VDA to register:

  ```
  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd"-t "REG_DWORD"-v "MtuDiscovery"-d "0x00000001"--force
  ```

- To disable EDT MTU discovery, delete the `MtuDiscovery` registry value.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Control EDT MTU discovery on the client

You can control EDT MTU discovery selectively on the client by adding the `MtuDiscovery` parameter in the ICA file. To disable the feature, set the following under the `Application` section:

```
MtuDiscovery=Off
```

To re-enable the feature, remove the `MtuDiscovery` parameter from the ICA file.

> **Important:**
>
> For this ICA file parameter to work, enable EDT MTU discovery on the VDA. If EDT MTU discovery is not enabled on the VDA, the ICA file parameter has no effect.

Custom backgrounds and banner messages on session logon screens

January 23, 2023

You can use the following commands to add a custom background or banner message to session **logon** screens. To add both a background and a banner message to session **logon** screens, you can embed the banner message into the background image.

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
      "LogonDisplayString" -d "<text of custom logon banner message>" --
     force
2 <!--NeedCopy-->
```

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
      "BackgroundImagePath" -d "<path to your custom logon screen
     background image>" --force
2 <!--NeedCopy-->
```

To use the feature on SUSE 15.3, install `imlib2` from http://download.opensuse.org/distribution/leap/15.3/repo/oss/.

> **Tip:**
>
> If you add a custom banner message using LogonDisplayString, the logon screen background is blue by default.

Custom desktop environments by session users

January 23, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

You can specify a desktop environment for session users by using the **CTX_XDL_DESKTOP_ENVIRONMENT** variable. Starting with the 2209 release, session users can customize their own desktop environments. To enable this feature, you must install desktop environments on the VDA in advance.

The following table shows a matrix of the Linux distributions and the desktop environments that support custom desktop environments by session users.

Linux distribution	Supported desktop
Debian11.3	MATE, GNOME, GNOME-Classic, KDE
RHEL 8.6, RHEL 8.4	MATE, GNOME, GNOME-Classic
RHEL 7.9	MATE, GNOME, GNOME-Classic, KDE
Rocky Linux 8.6	MATE, GNOME, GNOME-Classic, KDE
SUSE 15.3	MATE, GNOME, GNOME-Classic
Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04	MATE, GNOME, GNOME-Classic, KDE

Desktop switching commands

To switch to a target desktop environment, run the corresponding command within the session:

If the target desktop environment is	Run the command
GNOME	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME`
GNOME Classic	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC`
MATE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh MATE`
KDE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh KDE`

KDE tips

- Magnus might load at startup in KDE. As a workaround, you can remove the Magnus package by running `sudo apt remove magnus`.
- To disable QT warnings that occur during KDE startup, edit `/usr/share/qt5/qtlogging.ini` as a root user by adding the following entries:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
qt.qpa.xcb.xcberror.error=false
qt.qpa.xcb.warning=false
qt.qpa.xcb.error=false
<!--NeedCopy-->
```

- Screen unlock might fail for KDE. As a workaround, we recommend you disable the auto-lock feature of your desktop.

Logon with a temp home directory

January 23, 2023

You can specify a temp home directory for cases where the mount point on the Linux VDA fails. With a temp home directory specified, a prompt shows during a session logon when the mount point fails. User data is then stored under the temp home directory.

The following table describes registry keys that help with your home directory settings.

Registry key	Description	Command
LogNoHome	Controls whether users can log on to sessions without a home directory. The default value is 1 and it means yes. If the value is set to 0, session logons without a home directory are disabled.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "LogNoHome"-d "0x00000001"--force
HomeMountPoint	Sets a local mount point on the Linux VDA. For example, if /mnt/home is the mount point, a user's home directory is /mnt/home/domain/<user_name>. Make sure that the mount point is the same as the user home directory in your environment.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "HomeMountPoint"-d "<A directory where the NFS share is to be mounted>"--force

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registry key	Description	Command
TempHomeDirectoryPath	Sets a temp home directory on the Linux VDA in case the mount point fails. The default value is /tmp. The registry key depends on HomeMountPoint. It takes effect only when the system detects that the mount point is unavailable. A temp home directory for a user is /tmp/CTXSmf_user_id.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "TempHomeDirectoryPath"-d "</tmp by default>"--force
RemoveHomeOnLogoff	Controls whether to remove temp home directories on user logoffs. 1 means yes. 0 means no.	create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "RemoveHomeOnLogoff"-d "0x00000000"--force

Publish applications

January 23, 2023

With Linux VDA Version 7.13, Citrix added the seamless applications feature to all the supported Linux platforms. No specific installation procedures are required to use this feature.

> **Tip:**
>
> With Linux VDA version 1.4, Citrix added support for non-seamless published applications and session sharing.

Publish applications using Citrix Studio

You can publish applications installed on a Linux VDA when you create a delivery group or add applications to an existing delivery group. The process is similar to publishing applications installed on a

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows VDA. For more information, see the Citrix Virtual Apps and Desktops documentation (based on the version of Citrix Virtual Apps and Desktops being used).

> **Note:**
>
> - When configuring delivery groups, ensure that the delivery type is set to **Desktop and applications** or **Applications**.
> - 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, we recommend that you create separate delivery groups for app and desktop deliveries.
> - To use seamless applications, do not disable the seamless mode on StoreFront. The seamless mode is enabled by default. If you have already disabled it by setting "TWIMode=Off," remove this setting instead of changing it to "TWIMode=On."Otherwise you might not be able to launch a published desktop.

Limitation

The Linux VDA does not support the launch of multiple concurrent instances of the same application by a single user.

In an app session, only shortcuts that are specific to the app work as expected.

Known issues

The following known issues are identified during publishing applications:

- Non-rectangular windows are not supported. The corners of a window might show the server-side background.
- Preview of the content of a window from a published application is not supported.
- When you run multiple LibreOffice applications, only the one launched first shows on Citrix Studio because these applications share the process.
- Published Qt5-based applications like "Dolphin"might not show icons. To resolve the issue, see the article at https://wiki.archlinux.org/title/Qt.

Rendezvous V1

January 23, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

When using the Citrix Gateway service, the Rendezvous protocol allows traffic to bypass the Citrix Cloud Connectors and connect directly and securely with the Citrix Cloud control plane.

There are two types of traffic to consider: 1) control traffic for VDA registration and session brokering; 2) HDX session traffic.

Rendezvous V1 allows for HDX session traffic to bypass Cloud Connectors, but it still requires Cloud Connectors to proxy all control traffic for VDA registration and session brokering.

Requirements

- Access to environment using Citrix Workspace and Citrix Gateway service.
- Control Plane: Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).
- Linux VDA Version 2112 or later.
  - Version 2112 is the minimum required for no-transparent HTTP proxies.
  - Version 2204 is the minimum required for transparent and SOCKS5 proxies.
- Enable the Rendezvous protocol in the Citrix policy. For more information, see Rendezvous protocol policy setting.
- The VDAs must have access to `https://*.nssvc.net`, including all subdomains. If you cannot whitelist all subdomains in that manner, use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see the Internet Connectivity Requirements section of the Citrix Cloud documentation (under Virtual Apps and Desktop service) and the Knowledge Center article CTX270584.
- Cloud Connectors must obtain the VDAs' FQDNs when brokering a session. To achieve this goal, enable DNS resolution for the site: Using the Citrix DaaS Remote PowerShell SDK, run the command `Set-BrokerSite -DnsResolutionEnabled $true`. For more information about the Citrix DaaS Remote PowerShell SDK, see SDKs and APIs.

Proxy configuration

The VDA supports establishing Rendezvous connections through HTTP and SOCKS5 proxies.

Proxy considerations

Consider the following when using proxies with Rendezvous:

- Non-transparent HTTP proxies and SOCKS5 proxies are supported.
- Packet decryption and inspection are not supported. Configure an exception so that the ICA traffic between the VDA and the Gateway Service is not intercepted, decrypted, or inspected. Otherwise, the connection breaks.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- HTTP proxies support machine-based authentication by using the Negotiate and Kerberos authentication protocols. When you connect to the proxy server, the Negotiate authentication scheme automatically selects the Kerberos protocol. Kerberos is the only scheme that the Linux VDA supports.

  > **Note:**
  >
  > To use Kerberos, you must create the service principal name (SPN) for the proxy server and associate it with the proxy's Active Directory account. The VDA generates the SPN in the format `HTTP/<proxyURL>` when establishing a session, where the proxy URL is retrieved from the **Rendezvous proxy** policy setting. If you don't create an SPN, authentication fails.

- Authentication with a SOCKS5 proxy is not currently supported. If using a SOCKS5 proxy, you must configure an exception so that traffic destined to Gateway Service addresses (specified in the requirements) can bypass authentication.
- Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

Transparent proxy

Transparent HTTP proxy is supported for Rendezvous. If using a transparent proxy in your network, no additional configuration is required on the VDA.

Non-transparent proxy

When using a non-transparent proxy in your network, configure the Rendezvous proxy configuration setting. When the setting is enabled, specify the HTTP or SOCKS5 proxy address for the VDA to know which proxy to use. For example:

- Proxy address: `http://<URL or IP>:<port>` or `socks5://<URL or IP>:<port>`

Rendezvous validation

If you meet all requirements, follow these steps to validate if Rendezvous is in use:

1. Launch a terminal on the VDA.
2. Run `/opt/Citrix/VDA/bin/ctxquery -f iP`.
3. The TRANSPORT PROTOCOLS indicates the type of connection:
   - TCP Rendezvous: TCP - TLS - CGP - ICA
   - EDT Rendezvous: UDP - DTLS - CGP - ICA

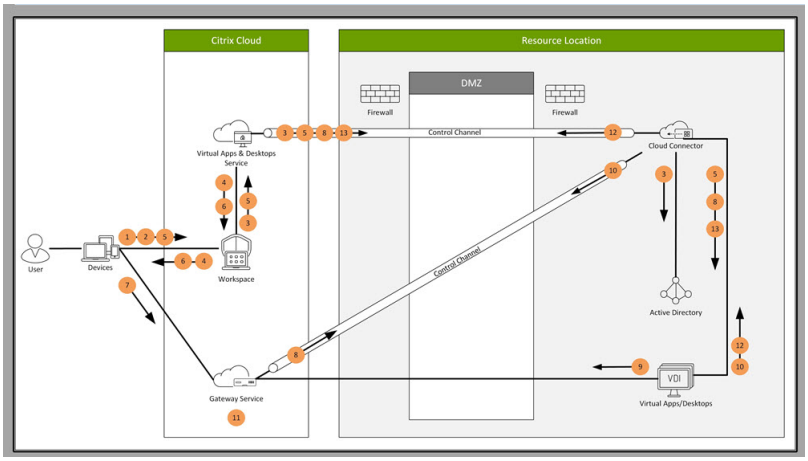
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Proxy through Cloud Connector: TCP - PROXY - SSL - CGP - ICA or UDP - PROXY - DTLS - CGP - ICA

> **Tip:**
>
> If the VDA cannot reach the Citrix Gateway service directly with Rendezvous enabled, the VDA falls back to proxy the HDX session through the Cloud Connector.

How Rendezvous works

This diagram is an overview of the Rendezvous connection flow.



Follow the steps to understand the flow.

1. Navigate to Citrix Workspace.
2. Enter credentials in Citrix Workspace.
3. If using on-premises Active Directory, Citrix DaaS authenticates credentials with Active Directory using the Cloud Connector channel.
4. Citrix Workspace displays enumerated resources from Citrix DaaS.
5. Select resources from Citrix Workspace. Citrix DaaS sends a message to the VDA to prepare for an incoming session.
6. Citrix Workspace sends an ICA file to the endpoint that contains an STA ticket generated by Citrix Cloud.
7. The endpoint connects to the Citrix Gateway service, provides the ticket to connect to the VDA, and Citrix Cloud validates the ticket.
8. The Citrix Gateway service sends connection information to the Cloud Connector. The Cloud Connector determines if the connection is a Rendezvous connection and sends the information to the VDA.
9. The VDA establishes a direct connection to the Citrix Gateway service.
10. If a direct connection between the VDA and the Citrix Gateway service isn't possible, the VDA proxies its connection over the Cloud Connector.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11. The Citrix Gateway service establishes a connection between the endpoint device and the VDA.
12. The VDA verifies its license with Citrix DaaS through the Cloud Connector.
13. Citrix DaaS sends session policies to the VDA through the Cloud Connector. Those policies are applied.

Rendezvous V2

January 23, 2023

When using the Citrix Gateway service, the Rendezvous protocol allows traffic to bypass the Citrix Cloud Connectors and connect directly and securely with the Citrix Cloud control plane.

There are two types of traffic to consider: 1) control traffic for VDA registration and session brokering; 2) HDX session traffic.

Rendezvous V1 allows for HDX session traffic to bypass Cloud Connectors, but it still requires Cloud Connectors to proxy all control traffic for VDA registration and session brokering.

Standard AD domain joined machines and non-domain joined machines are supported for using Rendezvous V2 with single-session and multi-session Linux VDAs. With non-domain joined machines, Rendezvous V2 allows for both HDX traffic and control traffic to bypass the Cloud Connectors.

Requirements

The requirements for using Rendezvous V2 are:

- Access to the environment using Citrix Workspace and Citrix Gateway service.
- Control Plane: Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).
- VDA version 2201 or later.
  - Version 2204 is the minimum required for HTTP and SOCKS5 proxies.
- Enable the Rendezvous protocol in the Citrix policy. For more information, see Rendezvous protocol policy setting.
- The VDAs must have access to `https://*.nssvc.net`, including all subdomains. If you cannot whitelist all subdomains in that manner, use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see the Internet Connectivity Requirements section of the Citrix Cloud documentation (under Virtual Apps and Desktop service) and the Knowledge Center article CTX270584.
- The VDAs must be able to connect to the addresses mentioned previously:
  - On TCP 443, for TCP Rendezvous.
  - On UDP 443, for EDT Rendezvous.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Proxy configuration

The VDA supports connecting through proxies for both control traffic and HDX session traffic when using Rendezvous. The requirements and considerations for both types of traffic are different, so review them carefully.

Control traffic proxy considerations

- Only HTTP proxies are supported.
- Packet decryption and inspection are not supported. Configure an exception so the control traffic between the VDA and the Citrix Cloud control plane is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Proxy authentication is not supported.
- To configure a proxy for control traffic, edit the registry as follows:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -t "REG_SZ" -v "ProxySettings" -d "http
   ://<URL or IP>:<port>" --force
<!--NeedCopy-->
```

HDX traffic proxy considerations

- HTTP and SOCKS5 proxies are supported.
- EDT can only be used with SOCKS5 proxies.
- To configure a proxy for HDX traffic, use the Rendezvous proxy configuration policy setting.
- Packet decryption and inspection are not supported. Configure an exception so the HDX traffic between the VDA and the Citrix Cloud control plane is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- HTTP proxies support machine-based authentication by using the Negotiate and Kerberos authentication protocols. When you connect to the proxy server, the Negotiate authentication scheme automatically selects the Kerberos protocol. Kerberos is the only scheme that the Linux VDA supports.

  > **Note:**
  >
  > To use Kerberos, you must create the service principal name (SPN) for the proxy server and associate it with the proxy's Active Directory account. The VDA generates the SPN in the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> format HTTP/<proxyURL> when establishing a session, where the proxy URL is retrieved from the **Rendezvous proxy** policy setting. If you don't create an SPN, authentication fails.

- Authentication with a SOCKS5 proxy is not currently supported. If using a SOCKS5 proxy, you must configure an exception so that traffic destined to Gateway Service addresses (specified in the requirements) can bypass authentication.
- Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

Transparent proxy

Transparent HTTP proxy is supported for Rendezvous. If using a transparent proxy in your network, no additional configuration is required on the VDA.

How to configure Rendezvous V2

Following are the steps for configuring Rendezvous in your environment:

1. Make sure that all requirements are met.
2. After the VDA is installed, run the following command to set the required registry key:

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

3. Restart the VDA machine.
4. Create a Citrix policy, or edit an existing one:
   - Set the Rendezvous Protocol setting to **Allowed**.
   - Ensure that the Citrix policy filters are set properly. The policy applies to the machines that need Rendezvous to be enabled.
   - Ensure that the Citrix policy has the correct priority so that it does not overwrite another one.

Rendezvous validation

To check whether a session is using the Rendezvous protocol, run the `/opt/Citrix/VDA/bin/ctxquery -f iP` command in the terminal.

The transport protocols displayed indicate the type of connection:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- TCP Rendezvous: TCP - TLS - CGP - ICA
- EDT Rendezvous: UDP - DTLS - CGP - ICA
- Proxy through Cloud Connector: TCP - PROXY - SSL - CGP - ICA or UDP - PROXY - DTLS - CGP - ICA

If Rendezvous V2 is in use, the protocol version shows 2.0.

> **Tip:**
>
> If the VDA cannot reach the Citrix Gateway service directly with Rendezvous enabled, the VDA falls back to proxy the HDX session through the Cloud Connector.

Secure user sessions using DTLS

January 23, 2023

DTLS encryption is a fully supported feature starting with the 7.18 release. By default, this feature is enabled on the Linux VDA. For more information, see Transport Layer Security.

Enable DTLS encryption

Verify that adaptive transport is enabled

In Citrix Studio, verify that the **HDX Adaptive Transport** policy is set to **Preferred** or **Diagnostic mode**.

Enable SSL encryption on the Linux VDA

On the Linux VDA, use the **enable_vdassl.sh** tool at **/opt/Citrix/VDA/sbin** to enable (or disable) SSL encryption. For information about the options available in the tool, run the `/opt/Citrix/VDA/sbin/enable_vdassl.sh -h` command.

> **Note:**
>
> The Linux VDA supports both DTLS 1.0 and DTLS 1.2 and uses DTLS 1.2 by default. Check which version of DTLS is in use on your Citrix Workspace app. Ensure that the same version of DTLS is used on both the Linux VDA and your Citrix Workspace app. If your Citrix Workspace app supports only DTLS 1.0 (for example, Citrix Receiver for Windows 4.11), set **SSLMinVersion** to **TLS_1.0** and **SSLCipherSuite** to **COM** or **ALL** using the **enable_vdassl.sh** tool.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure user sessions using TLS

January 23, 2023

Starting with Version 7.16, the Linux VDA supports TLS encryption for secure user sessions. TLS encryption is disabled by default.

Enable TLS encryption

To enable TLS encryption for secure user sessions, install certificates and enable TLS encryption on both the Linux VDA and the Delivery Controller (the Controller).

Install certificates on the Linux VDA

Obtain server certificates in PEM format and root certificates in CRT format. A server certificate contains the following sections:

- Certificate
- Unencrypted private key
- Intermediate certificates (optional)

An example of a server certificate:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
-----BEGIN CERTIFICATE-----
MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL
MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE
ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G
A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALCTTOdxcivbIOLOF66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9
t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEwl3YxM6COyBf7L6psrsCDNnBPlq8TJH
4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+OFQ2Bq3NhwsRhnAgMBAAGj
gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8yOw
gZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB
AD5axBYHwIxJCJzNt2zdXnbp2O0yUTowElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68
Vel8u1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbuOIjOtr3pkxAe
b6CFJtNLudHUrwF6lOrB72zbyz3PiIx+HEwt1jOj8z4K
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q
fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy
R+MaDyF1HmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB
AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea
FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSxOYb/lAdck/
FXzUOtqytUe/KHgcSgjtjrSeqLJqMm+yxzBAatVRTTzGdwAhAkEA3l1kRZjIN5uz
Enmi2RTI3ngBhBP/S3GEbvJfKsD5n2Ri9O+OoEPxclvvp5ne8QOzUpshbjFEPbOC
ykZ6UassFwJBAMtI5yPnV9ewPzJoaNjZIJcMtNXDchSlxXiJiyzv+Qmr8RuQz9Pv
fIenmTrfZ+Wo4DaKg+8ar2OvOnKFOHFAmDECQQDEWRlH6cE3WyCfN1u942M9XkhR
GvSpR7+b///vL6Nwwv3CwPV9n8DTpL+wuDkJZ9nCvRteil9MlaMTYjs3alNvAkEA
qy5JzZcbBnrYzMbVO32jju7ZPISnhTGO1xDjzMSLLpTGpNLN34b0k3sTclr8L42E
uQjtTqRm+wdsrVF3lFazkQJANudmsUVv3gZKhMGaV2hzIdXIfHyOIYv+3leZhQY6
h5eEmxSZS5OTvyNGt2e6m2ZgaZmjTagH59TCBHvR5nof2g==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDGTCCAoKgAwIBAgIJAMvJwvHXAd9hMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNDExMVoXDTI4MDkyNTEwNDExMVowZzELMAkGA1UEBhMCVUsx
EjAQBgNVBAgTCUNhbWJyaWRnZTESMBAGA1UEBxMJQ2FtYm9lcm5lMRQwEgYDVQQK
EwtDaXRyaXggVGVzdDEaMBgGA1UEAxMRY2EwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKVZmF7Uj7uOnvO3Qwdfi0nr3QkNH2DXpWrZ
Zh8cI9Vv+UFRUiC6oB7izLtBMFn3fOUP7i2CfkHN3ZGJ17p89pdyjket1MslVeJw
acOqrYvD+fNNSvJjunTbaCywVtALjmFSfMHeZJXVSckrpEhnk0nkMS16tcrya/K/
osSlzvI3AgMBAAGjgcwwgckwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU85kN1EPJ
OcVhcOss1slseDQwGsIwgZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQw
GsKha6RpMGcxCzAJBgNVBAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNV
BAcTCUNhbWJvdXJuZTEUMBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNh
MDAxLmNpdHJpdGUubmV0ggkAy8nC8dcB32EwDQYJKoZIhvcNAQEFBQADgYEAIZ4Z
gXLLXf12RNqh/awtSbd41Ugv8BIKAsg5zhNAiTiXbzz8Cl3ec53Fb6nigMWc5Tli
UNCLXwnxRUiD4O0tESLX9ACUNH3I94yxOgujkSOSBni21jjZTvfBB32Rmr5DByJg
UmKORn/hdqMlcqpe5wO6as6+HN4WUOi+hEtUMME=
-----END CERTIFICATE-----
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Enable TLS encryption

Enable TLS encryption on the Linux VDA On the Linux VDA, use the `enable_vdassl.sh` script in the **/opt/Citrix/VDA/sbin** directory to enable (or disable) TLS encryption. For information about the options available in the script, run the `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help` command.

```
root@lxu1804:~# /opt/Citrix/VDA/sbin/enable_vdassl.sh
===Enable/Disable SSL on Linux VDA===
To enable SSL, a certificate file must be specified, otherwise the local certificate file under
/etc/xdl/.sslkeystore/ is used, If the local certificate file does not exist, the command
fails. You can specify the SSL port number, version and cipher suite, otherwise, their default
values are used!

Usage: enable_vdassl.sh -Disable
       Disable Linux VDA SSL.

Usage: enable_vdassl.sh -Enable [-Certificate <CERT-FILE>] [-SSLPort <SSL-PORT-NUMBER>]
       [-SSLMinVersion <SSL-MIN-VERSION>] [-SSLCipherSuite <SSL-CIPHER-SUITE>]
       Enable Linux VDA SSL.

Options:
       -Certificate <CERT-FILE>
       Specify a certificate file, where <CERT-FILE> must include the full file path. Only one format
       is currently supported, that is PEM.

       -RootCertificate <ROOT-CERT-FILE>
       Specify a root certificate file, where <ROOT-CERT-FILE> must include the full file path, The root certificate will be put in the local keystore(under /etc/xdl/.sslkeystore/cacerts).

       -SSLPort <SSL-PORT-NUMBER>
       Specify an SSL port number. Unless otherwise specified, the default port 443 used.

       -SSLMinVersion <TLS_1.0|TLS_1.1|TLS_1.2|TLS_1.3>
       Specify SSL version. Unless otherwise specified, the default value TLS_1.2 is used.

       -SSLCipherSuite <GOV|COM|ALL>
       Specify an SSL Cipher suite. Unless otherwise specified, the default value GOV is used.

Examples:
       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem"
       Enable Linux VDA SSL using Certificate cert001.pem.

       enable-vdassl.sh -Enable -RootCertificate "/home/rootCR.cer"
       Enable Linux VDA SSL using Root Certificate rootCR.cer with local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -SSLPort 445
       Enable Linux VDA SSL on port 445 using local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445
       Enable Linux VDA SSL using Certificate cert001.pem on port 445, with default SSLMinVersion and SSLCipherSuite.

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and default SSLCipherSuite..

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2" -SSLCipherSuite "GOV"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and SSLCipherSuite GOV.
```

Tip: A server certificate must be installed on each Linux VDA server and root certificates must be installed on each Linux VDA server and client.

Enable TLS encryption on the Controller

> **Note:**
>
> You can enable TLS encryption only for entire delivery groups. You cannot enable TLS encryption for specific applications.

In a PowerShell window on the Controller, run the following commands in sequence to enable TLS encryption for the target delivery group.

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

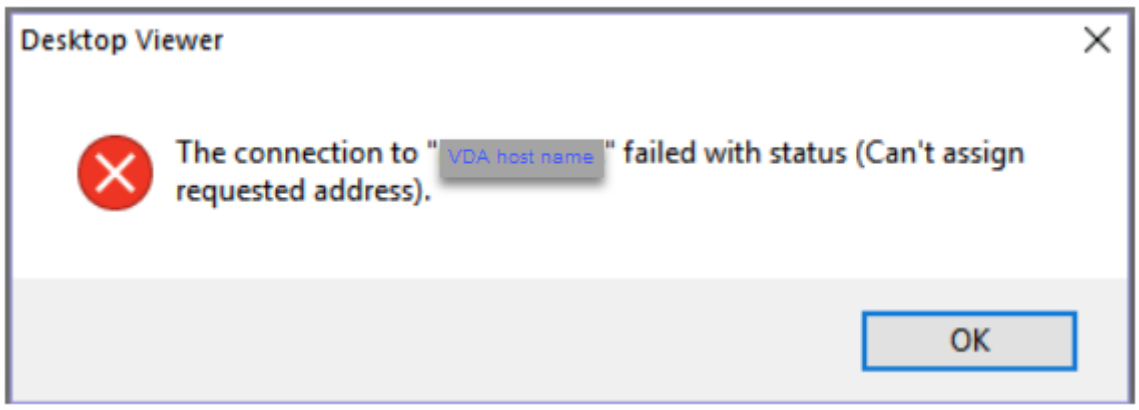
> **Note:**
>
> To ensure that only VDA FQDNs are contained in an ICA session file, you can also run the `Set-BrokerSite –DnsResolutionEnabled $true` command. The command enables DNS resolution. If you disable DNS resolution, an ICA session file discloses VDA IP addresses and provides FQDNs only for the TLS-related items such as `SSLProxyHost` and `UDPDTLSPort`.

To disable TLS encryption on the Controller, run the following commands in sequence:

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

Troubleshooting

The following "Can't assign requested address" error might occur in Citrix Workspace app for Windows when you try to access a published desktop session:



As a workaround, add an entry to the **hosts** file, which is similar to:

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

On Windows machines, the **hosts** file typically locates at `C:\Windows\System32\drivers\etc\hosts`.

Session reliability

January 23, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix introduces the session reliability feature to all supported Linux platforms. Session reliability is enabled by default.

Session reliability reconnects ICA sessions seamlessly across network interruptions. For more information about session reliability, see Auto client reconnect and session reliability.

Note: Data transmitted through a session reliability connection is in plain text by default. For security purposes, We recommend that you enable TLS encryption. For more information about TLS encryption, see Secure user sessions using TLS.

Configuration

Policy settings in Citrix Studio

You can set the following policies for session reliability in Citrix Studio:

- Session reliability connections
- Session reliability timeout
- Session reliability port number
- Reconnection UI transparency level

For more information, see Session reliability policy settings and Auto client reconnect policy settings.

Note: After setting the **Session reliability connections** or **Session reliability port number** policy, restart the VDA service and the HDX service, in this order, for your settings to take effect.

Settings on the Linux VDA

- **Enable/disable the session reliability TCP listener**

By default, the session reliability TCP listener is enabled and listening on port 2598. To disable the listener, run the following command.

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

Note: Restart the HDX service for your settings to take effect. Disabling the TCP listener does not disable session reliability. Session reliability is still available through other listeners (for example, SSL) if the feature is enabled through the **Session reliability connections** policy.

- **Session reliability port number**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

You can also set the session reliability port number by using the following command (using port number 2599 as an example).

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

Note: Restart the HDX service for your setting to take effect. If the port number has been set through the policy setting in **Citrix Studio**, your setting on the Linux VDA is ignored. Ensure that the firewall on the VDA is configured not to prohibit network traffic through the set port.

- **Server-to-client keep-alive interval**

Keep-alive messages are sent between the Linux VDA and the client when there's no activity (for example, no mouse movement or screen update) in a session. The keep-alive messages are used to detect whether the client is still responsive. If there is no response from the client, the session is suspended until the client reconnects. This setting specifies the number of seconds between successive keep-alive messages. By default, this setting is not configured. To configure it, run the following command (using 10 seconds as an example).

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

- **Client-to-server keep-alive interval**

This setting specifies the number of seconds between successive keep-alive messages sent from the ICA client to the Linux VDA. By default, this setting is not configured. To configure it, run the following command (using 10 seconds as an example).

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

Troubleshooting

Unable to launch sessions after enabling session reliability through the policy setting.

To work around this issue, do the following:

1. Ensure that the VDA service and HDX service are restarted, in this order, after you enable session reliability through the policy setting in Citrix Studio.
2. On the VDA, run the following command to verify that the session reliability TCP listener is running (using port 2598 as an example).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

If there is no TCP listener on the session reliability port, enable the listener by running the following command.

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

Session recording (experimental)

January 23, 2023

As an experimental feature, you can record and replay sessions hosted on a Linux VDA.

Enable or disable session recording

To enable or disable session recording for a Linux VDA, set **SmAudAllowed** to **1** or **0**, respectively. You can use the following commands:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
   SmAudAllowed" -d "0x00000001" --force
<!--NeedCopy-->
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
   SmAudAllowed" -d "0x00000000" --force
<!--NeedCopy-->
```

> **Note:**
>
> After you enable session recording on a Linux VDA, users are notified about their sessions being recorded when they log on to their sessions.

Specify file size for recordings

As recordings grow in size, recording files take longer to download and respond more slowly when you use the seek slider to navigate during playback. To control file size, specify a threshold limit for

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a file. When the recording reaches this limit, the current file is closed, and an extra file is created to continue recording. This action is called a rollover.

Using the following commands, you can specify two thresholds for a rollover:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    RolloverFileSizeInMB" -d "0x00000032" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    RolloverTimeInHours" -d "0x0000000c" --force
<!--NeedCopy-->
```

- **RolloverFileSizeInMB**. The current file closes when it reaches the size, and a new file opens. By default, the rollover occurs when the size exceeds 50 MB. Supported values: 10–300.
- **RolloverTimeInHours**. When the duration is reached, the current file closes and a new file opens. By default, the rollover occurs when the session records for 12 hours. Supported values: 1–24.

Rollovers occur when the first of the two conditions above is met. For example, you specify 17 MB for the file size and 6 hours for the duration. When your recording reaches 17 MB in 3 hours, session recording closes the file and opens a new one.

To prevent the creation of many small files, rollover doesn't happen until at least one hour elapses regardless of the value specified for the file size. The exception to this rule is if the file size surpasses 300 MB.

Specify where recordings are stored

Recording files are stored under /var/xdl/session_recordings by default. To specify a different path, run the following command:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_SZ" -v "Path"
     -d "<your custom storage path>" --force
<!--NeedCopy-->
```

You can store recordings on a local drive or a mount point that points to a network path. Configure proper access permissions to the storage path that you set and grant the user ctxsrvr the write permission to the path.

View recordings

To view recordings, complete the following steps to install the Session Recording player or the Session Recording web player:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Use your Citrix account credentials to access the Citrix Virtual Apps and Desktops download page and download the product file. Unzip the file.
2. Double-click SessionRecordingPlayer.msi and SessionRecordingWebPlayer.msi and follow the instructions to complete the installation.

> **Tip:**
>
> To use the Session Recording web player, install it on the Session Recording server only and ensure that recordings are available on the Session Recording server. For more information, see the Citrix Session Recording documentation.

Limitations

- For virtual app sessions, recording notifications might not be centered.

USB device redirection

January 12, 2024

USB devices are shared between Citrix Workspace app and the Linux VDA desktop. When a USB device is redirected to the desktop, you can use the USB device as if it were locally connected.

> **Tip:**
>
> We recommend using USB device redirection when the network latency is lower than 100 milliseconds. Do not use USB device redirection when the network latency is higher than 200 milliseconds.

USB device redirection includes three main areas of functionality:

- Open-source USB/IP project
- Citrix USB session module
- Citrix USB service module

Open-source USB/IP project:

The USB/IP project consists of a Linux kernel driver and some user mode libraries that let you communicate with the kernel driver to get all USB data.

The Linux VDA implements USB device redirection based on the open-source USB/IP project and reuses the kernel driver and user mode libraries of USB/IP. However, all USB data transfers between the Linux VDA and Citrix Workspace app are encapsulated by the Citrix ICA USB protocol.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix USB session module:

The Citrix USB session module acts as a communication bridge between the USB/IP kernel module and Citrix Workspace app.

Citrix USB service module:

The Citrix USB service module manages all operations on USB devices, for example, attach or detach USB devices.

How USB device redirection works

Typically, if a USB device is redirected successfully to the Linux VDA, one or more device nodes are created in the system /dev path. Sometimes, however, the redirected device isn't usable for an active Linux VDA session. USB devices rely on drivers to function properly and some devices require special drivers. If drivers aren't provided, the redirected USB devices are inaccessible to the active Linux VDA session. To make sure of USB device connectivity, install the drivers and configure the system properly.

The Linux VDA supports a list of USB devices that are successfully redirected from the client.

Supported USB devices

> **Tip:**
>
> We have added support for USB 3.0 ports. You can insert USB 3.0 devices into USB 3.0 ports on a client device.

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

USB mass storage device	VID:PID	File system
Netac Technology Co., Ltd	0dd8:173c	FAT32, NTFS
Kingston Datatraveler 101 II	0951:1625	FAT32, NTFS
Kingston Datatraveler GT101 G2	1567:8902	FAT32, NTFS
SanDisk SDCZ80 flash drive	0781:5580	FAT32, NTFS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

USB mass storage device	VID:PID	File system
WD HDD	1058:10B8	FAT32, NTFS
Toshiba Kingston DataTraveler 3.0 USB device	0930:6545	FAT32, NTFS
Taiwan OEM – OBSOLETE VendorCo ProductCode Disk 2.0	FFFF:5678	FAT32, NTFS
TD-RDF5A Transcend USB device	8564:4000	FAT32, NTFS

> **Note:**
>
> To use NTFS on Amazon Linux 2, CentOS, RHEL, Rocky Linux, and SUSE, enable NTFS support on these distributions first.

USB 3D mouse	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

USB scanner	VID:PID
Epson Perfection V330 photo	04B8: 0142

Yubico USB	VID:PID
Yubico YubiKey OTP+FIDO+CCID - Keyboard, HID	1050:0407

Webcam USB	VID:PID
Logitech composite USB device – WebCam, Audio	0460:0825

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Configure USB device redirection

Install or compile the USB/IP kernel module (for CentOS, RHEL, and Rocky Linux only)

The Linux VDA uses USB/IP as the virtual host controller for USB device redirection. Because in most cases the USB/IP kernel module is released with the Linux kernel version 3.17 and later, you don't have to build the kernel module by default. However, the USB/IP kernel module is not available for CentOS, RHEL, and Rocky Linux. To use USB device redirection with these Linux distributions, you must install or compile the USB/IP kernel module. Download and install USB/IP from https://pkgs.org/download/kmod-usbip based on your Linux distribution.

Set USB device redirection policies

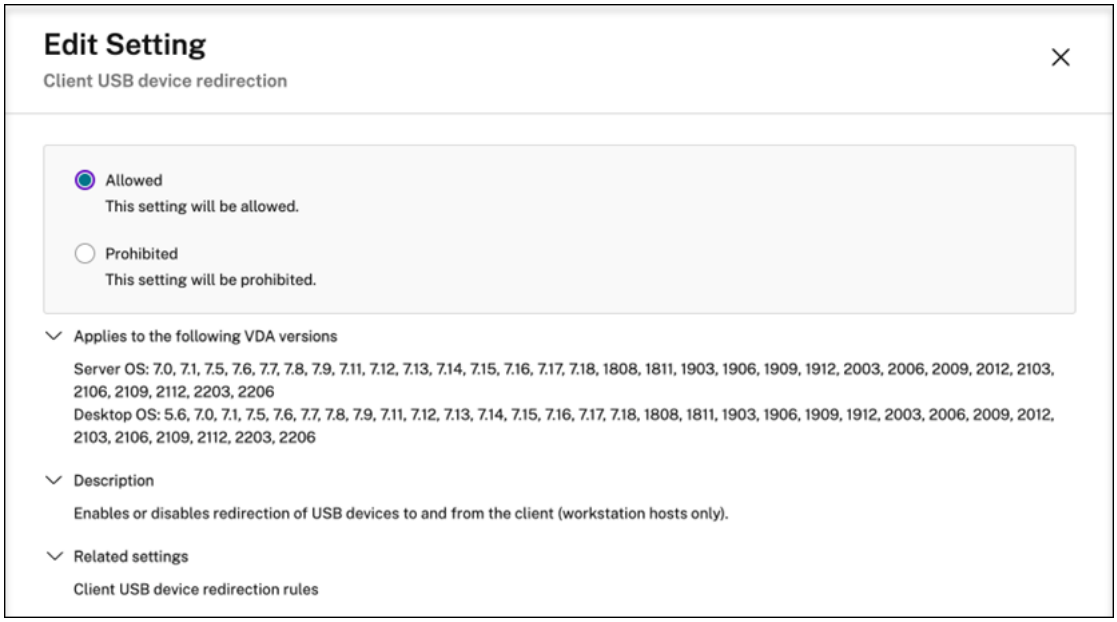
A Citrix policy controls whether USB device redirection is enabled or disabled. The type of device can also be specified using a Delivery Controller policy. When configuring USB device redirection for the Linux VDA, configure the following policy and rules:

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

Enable USB device redirection In Citrix Studio, enable (or disable) USB device redirection from the client (for workstation hosts only).

In the **Edit Setting** dialog:

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

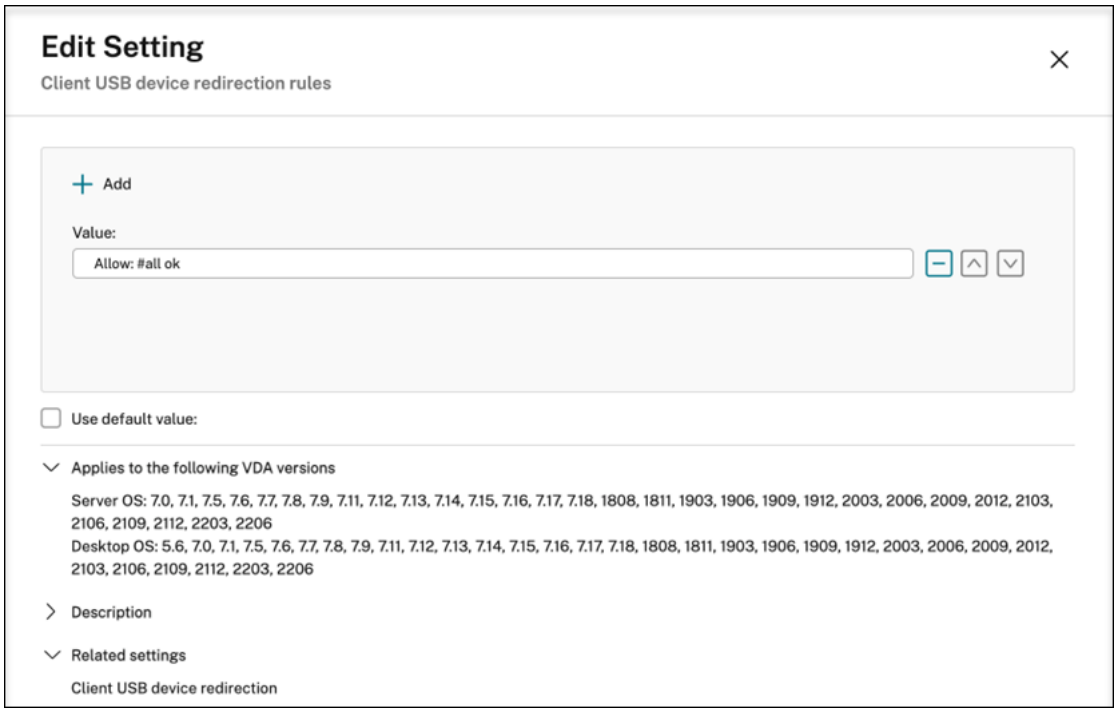


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Set USB device redirection rules After enabling the USB redirection policy, set the 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 editing) a rule, click **OK**.



For more information about configuring generic USB device redirection, see Citrix Generic USB Redirection Configuration Guide.

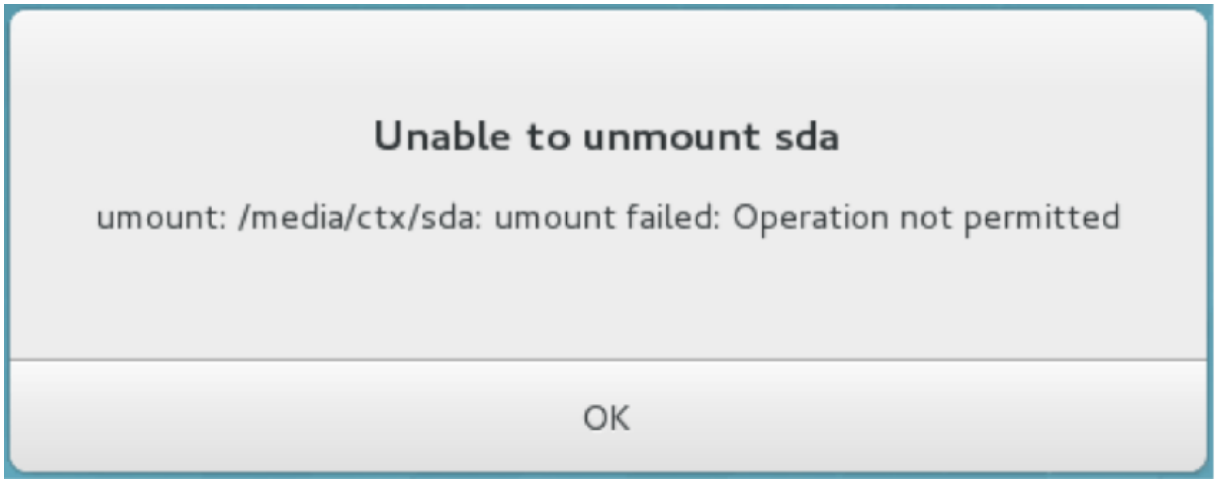
Troubleshoot USB device redirection issues

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

Unable to unmount the redirected USB disk

The Linux VDA manages all USB disks redirected from Citrix Workspace app under the administrative privilege to make sure that only the owner can access the redirected device. As a result, you can unmount the device only with the administrative privilege.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



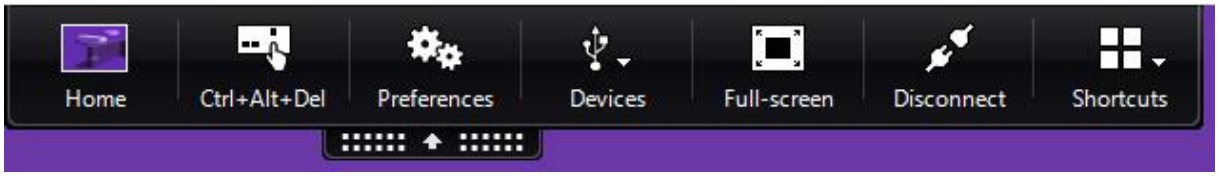
File lost when you stop redirecting a USB disk

If you stop redirecting a USB disk immediately using the toolbar of Citrix Workspace app, the files you modified or created on the disk 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 isn't written to the disk itself. If you stop redirecting using the toolbar of Citrix Workspace app, there's no time remaining for data being flushed to the disk, which results in lost data.

To resolve this issue, use the **sync** command in a terminal to flush data to the disk before stopping USB redirection.

No devices in the toolbar of Citrix Workspace app

Sometimes, you might not be able to see devices listed in the toolbar of Citrix Workspace app, which indicates that no USB redirection is taking place.



If you come across the issue, verify the following:

- The policy is configured to allow USB device redirection.
- The Citrix USB service module is running.

If the policy is not set correctly, correct it by referencing the Set USB device redirection policies section in this article.

If the Citrix USB service module is not running, complete the following steps:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. Check whether a USB/IP kernel module is available on your Linux distribution using the following command:

```
modinfo usbip-core
<!--NeedCopy-->
```

2. If the output is shown as follows, install or compile the USB/IP kernel module based on your Linux distribution:

```
modinfo: ERROR: Module usbip-core not found.
<!--NeedCopy-->
```

   - For Amazon Linux 2, CentOS, RHEL, and Rocky Linux, see the Install or compile the USB/IP kernel module section in this article.
   - For SUSE, download and install the USB/IP package from https://software.opensuse.org/package/usbip.
   - For Ubuntu/Debian, complete the following steps to compile and install the USB/IP kernel module:

     a) Download the USB/IP kernel module source code.

     Go to the Linux kernel repository at https://github.com/torvalds/linux/tree/master/drivers/usb/usbip, select the target Linux kernel version (v4.15 or later) tag, and get the link such as https://github.com/torvalds/linux/tree/v4.15/drivers/usb/usbip.

     Go to DownGit and enter the preceding link to create a download link for downloading the USB/IP source code.

     b) Unzip the source file using the following commands:

```
unzip ${
 USBIP_SRC }
 .zip

cd usbip
<!--NeedCopy-->
```

     c) Modify the **Makefile** file as follows:

```
# SPDX-License-Identifier: GPL-2.0

ccflags-$(CONFIG_USBIP_DEBUG) := -DDEBUG

obj-$(CONFIG_USBIP_CORE) += usbip-core.o

usbip-core-y := usbip_common.o usbip_event.o

obj-$(CONFIG_USBIP_VHCI_HCD) += vhci-hcd.o

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
vhci-hcd-y := vhci_sysfs.o vhci_tx.o vhci_rx.o vhci_hcd.o

#obj-$(CONFIG_USBIP_HOST) += usbip-host.o

#usbip-host-y := stub_dev.o stub_main.o stub_rx.o stub_tx.o

#obj-$(CONFIG_USBIP_VUDC) += usbip-vudc.o

#usbip-vudc-y := vudc_dev.o vudc_sysfs.o vudc_tx.o vudc_rx.
   o vudc_transfer.o vudc_main.o
<!--NeedCopy-->
```

d) Compile the source code:

```
apt-get install linux-headers-`uname -r`

make -C /lib/modules/`uname -r`/build M=$PWD
<!--NeedCopy-->
```

e) Install the USB/IP kernel module:

```
cp usbip-core.ko vhci-hcd.ko /opt/Citrix/VDA/lib64/
<!--NeedCopy-->
```

f) Restart the **ctxusbsd** service to load the USB/IP kernel module:

```
service ctxusbsd restart
<!--NeedCopy-->
```

Failed redirection when USB devices can be seen in the toolbar of Citrix Workspace app, but are labeled *policy restricted*

When the issue occurs, do the following:

- Configure the Linux VDA policy to enable redirection.
- Check whether any additional policy restrictions are configured in the registry of Citrix Workspace app. Check **DeviceRules** in the registry path to make sure that the device isn't denied access by this setting:

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

For more information, see the Knowledge Center article How to Configure Automatic Redirection of USB Devices.

A USB device is redirected successfully, but I can't use it in my session

Typically, only supported USB devices can be redirected. Other devices might be redirected to an active Linux VDA session too. For every redirected device, a node owned by the user is created in the

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

system **/dev** path. However, it's 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:**
>
> For 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. It might not be the case for devices that aren't in the supported device list.

Virtual Channel SDK (experimental)

January 23, 2023

With the Virtual Channel Software Development Kit (SDK) for the Linux VDA, you can write server-side applications to run on the VDA. For more information, see the Citrix Virtual Channel SDK for the Linux VDA documentation.

Citrix Virtual Channel SDK for the Linux VDA is available for download at the Citrix Virtual Apps and Desktops download page. Expand the appropriate version of Citrix Virtual Apps and Desktops and click **Components** to select the Linux VDA download.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).