Linux Virtual Delivery Agent 7.15

Contents

Was ist neu

October 5, 2022

Releasedatum: 7. Juli 2022

Neue Features in 7.15

Das kumulative Update 9 (CU9) ist das neueste Release von Linux VDA 7.15 LTSR. CU9 umfasst einen zusätzlichen Fix zu Linux VDA 7.15 CU8.

PDF-Druck

Zuvor als ein experimentelles Feature verfügbar, ist PDF-Druck jetzt eine vollständig unterstützte Funktion in dieser Version. Hiermit können Benutzer von Citrix Receiver für Chrome und HTML5 aus den Linux VDA-Sitzungen heraus PDFs drucken.

Systemverhaltensänderungen

Ab diesem Release müssen Sie nicht mehr das Skript Ctxsetup .sh- ausführen, nachdem Sie den Linux VDA aktualisiert haben.

Behobene Probleme

August 8, 2022

Behobene Probleme in CU9

- Beim Deinstallieren von Linux VDAs unter SUSE oder RHEL werden leere Ordner im Verzeichnis /opt/Citrix/ möglicherweise nicht gelöscht. [CVADHELP-18241]

Behobene Probleme in CU8

- Wenn die Kanalbindung aktiviert ist, können Versuche, einen Linux VDA beim Delivery Controller zu registrieren, möglicherweise fehlschlagen. [CVADHELP-14481]

Behobene Probleme in CU6

- Eine Linux-Sitzung hört möglicherweise auf zu reagieren, wenn Maus und Tastatur nicht auf dasselbe Fenster fokussiert sind oder die Maus den Fokus nicht ändert. [CVADHELP-12768]
- Der Versuch, ein USB-Laufwerk generisch zu einem Linux VDA umzuleiten, kann fehlschlagen. Das Problem tritt bei NTFS-formatierten USB-Laufwerken auf. [CVADHELP-13675]
- Linux VDAs erreichen möglicherweise nicht den Wert, der in der Einstellung **Frameratesollwert** (FramesPerSecond) angegeben ist. Das Problem tritt auf, wenn eine GPU auf einem Linux VDA installiert ist. [CVADHELP-14267]

Behobene Probleme in CU5

- Das Kopieren und Einfügen von Inhalt zwischen einem Client und einer Sitzung über die Zwischenablage kann fehlschlagen. [LD2047]
- Wenn Sie eine Sitzung auf einem Linux VDA starten und eine Aktion ausführen, wird die Verbindung möglicherweise getrennt. [LD2257]

Behobene Probleme in CU4

- Wenn Sie versuchen, Inhalt auf einem Endpunkt zu kopieren und in eine Anwendung auf einem Linux VDA einzufügen, wird der Inhalt möglicherweise nicht kopiert. [LC8760]
- Unter SUSE Linux Enterprise Server 11 Service Pack 4 funktioniert die Tastatur möglicherweise nicht. Daher werden die Tastenanschläge nicht auf dem Bildschirm angezeigt und das Tastaturlayout nicht korrekt eingestellt. [LC9906]
- Der **ctxctl**-Prozess kann in einer Benutzersitzung auf einem Linux VDA möglicherweise nicht ausgeführt werden. [LD0353]

Behobene Probleme in CU3

- Der Linux VDA kann Citrix Richtlinien möglicherweise nicht anwenden. Das Problem tritt auf, wenn Sie eine Richtlinie so konfigurieren, dass für die Zugriffssteuerung der Verbindungstyp “NetScaler Gateway”verwendet wird. [LC9842]

Behobene Probleme in CU2

- Die Registrierung eines Linux VDAs mit dem Delivery Controller kann zeitweilig fehlschlagen. [LC7982]

- Wenn Citrix Director 7.13 auf einem Red Hat Enterprise Linux Server 7.3 ausgeführt wird, können die Sitzungsdetails der Maschine möglicherweise nicht angezeigt werden. Die folgende Fehlermeldung wird angezeigt:

  Daten können nicht abgerufen werden. [LC8204]

- Ein Linux VDA registriert sich möglicherweise beim Delivery Controller und hebt die Registrierung nach einer Weile auf. [LC8205]
- Bestimmte Anwendungen von Drittanbietern, die zum Überprüfen der Sitzungsanzeige eines Linux VDAs verwendet werden, zeigen möglicherweise nicht alle Pixel an. [LC8419]
- Wenn mehrere LDAP-Server vorhanden sind, können Versuche fehlschlagen, eine Anwendung auf einem Linux VDA zu starten, nachdem Richtlinien aktualisiert wurden und eine Sitzung das Zeitlimit überschreitet. [LC8444]
- Der ctxhdx-Prozess wird möglicherweise unerwartet mit einem **segfault**-Fehler beendet, wenn die Sitzung mit einem Linux VDA verbunden ist. [LC8611]
- Wenn Sie den Linux VDA 7.16 Early Access Release verwenden, kann der Brokeragent den Anwendungsnamen möglicherweise nicht abrufen. Dieser Fehler führt dazu, dass Director die Meldung **Agent angefordert** anzeigt und die Neuregistrierung gestartet wird. [LC9243]

Behobene Probleme in CU1

- Ein Linux VDA registriert sich möglicherweise beim Delivery Controller und hebt die Registrierung nach einer Weile auf. [LC8205]
- Bestimmte Anwendungen von Drittanbietern, die zum Überprüfen der Sitzungsanzeige eines Linux VDAs verwendet werden, zeigen möglicherweise nicht alle Pixel an. [LC8419]
- Wenn mehrere LDAP-Server vorhanden sind, können Versuche fehlschlagen, eine Anwendung auf einem Linux VDA zu starten, nachdem Richtlinien aktualisiert wurden und eine Sitzung das Zeitlimit überschreitet. [LC8444]

Behobene Probleme in 7.15 LTSR

Die folgenden Probleme wurden in diesem Linux VDA-Release gelöst:

- Easy Install kann dazu führen, dass der Linux VDA vom Netzwerk getrennt wird, wenn Sie die DNS-IP-Adresse eingeben. [LNXVDA-2152]
- Bei der Wiedergabe eines Videos schlägt das Sitzungsroaming von Citrix Receiver für Windows zu Citrix Receiver für Android fehl. [LNXVDA-2164]

Bekannte Probleme

August 8, 2022

Die folgenden Probleme wurden in diesem Release identifiziert:

- Die Version von Citrix Scout, die in XenApp und XenDesktop 7.15 LTSR CU6 integriert ist, kann keine Protokolle vom Linux VDA 7.15 sammeln. Der Linux VDA 7.15 unterstützt den Citrix Telemetriedienst nicht, den Citrix Scout zum Sammeln von Protokollen verwendet.
- Der `indicator-datetime-service`-Prozess verbraucht nicht die Umgebungsvariable $TZ. Wenn sich Client und Sitzung in unterschiedlichen Zeitzonen befinden, wird auf dem Unity-Desktop in Ubuntu 16.04 nicht die Uhrzeit des Clients angezeigt. [LNXVDA-2128]
- Ubuntu-Grafiken: In HDX 3D Pro wird nach dem Ändern des Desktop Viewer u. U. ein schwarzer Rahmen angezeigt oder der Hintergrund ist schwarz.
- Drucker, die mit der Linux VDA-Druckumleitung erstellt wurden, können nach dem Abmelden von einer Sitzung u. U. nicht entfernt werden.
- CDM-Dateien fehlen, wenn das Verzeichnis viele Dateien und Unterverzeichnisse enthält Wenn clientseitig zu viele Dateien oder Verzeichnisse vorliegen, kann dieses Problem auftreten.
- In diesem Release wird nur UTF-8-Codierung für andere Sprachen als Englisch unterstützt.
- Der Status der Feststelltaste in Citrix Receiver für Android kann beim Sitzungsroaming umgekehrt werden. Der Status der Feststelltaste kann aufgehoben werden, wenn über eine vorhandene Verbindung Roaming zu Citrix Receiver für Android erfolgt. Verwenden Sie als Workaround die Umschalttaste auf der erweiterten Tastatur, um zwischen Groß- und Kleinbuchstaben zu wechseln.
- Tastenkombinationen mit der Alt-Taste funktionieren nicht immer, wenn Sie mit Citrix Receiver für Mac eine Verbindung zu einem Linux VDA herstellen. Citrix Receiver für Mac sendet standardmäßig für die linke und die rechte Alt-Taste den Befehl "Alt Gr". Sie können dieses Verhalten in den Einstellungen für Citrix Receiver ändern, die Ergebnisse sind jedoch je nach Anwendung unterschiedlich.
- Die Registrierung schlägt fehl, wenn der Linux VDA der Domäne wieder hinzugefügt wird. Beim erneuten Verbindungsaufbau wird ein neuer Satz Kerberos-Schlüssel generiert. Der Broker verwendet jedoch unter Umständen ein veraltetes zwischengespeichertes VDA-Dienstticket, das auf dem vorherigen Kerberos-Schlüsselsatz basiert. Wenn der VDA sich dann mit dem Broker verbinden will, kann der Broker u. U. keinen Sicherheitskontext zum VDA herstellen. Normalerweise schlägt die VDA-Registrierung dann fehl.

  Dieses Problem löst sich irgendwann von selber, wenn das VDA-Dienstticket abläuft und

erneuert wird. Diensttickets haben jedoch eine lange Lebensdauer, sodass dies einige Zeit dauern kann.

Deaktivieren Sie als Workaround den Ticketcache des Brokers. Starten Sie den Broker neu oder führen Sie als Administrator auf dem Broker folgenden Befehl an einer Eingabeaufforderung aus:

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

Mit diesem Befehl werden alle Diensttickets im LSA-Cache des Netzwerkdienstprinzipals gelöscht, unter dem der Citrix Brokerdienst ausgeführt wird. Es werden jedoch auch Diensttickets für andere VDAs und möglicherweise andere Dienste entfernt. Dies ist aber kein Problem, die Diensttickets werden bei Bedarf einfach erneut vom KDC geladen.

- Audio Plug-n-Play wird nicht unterstützt Sie können Audioaufnahmegeräte mit der Clientmaschine verbinden, bevor Sie mit dem Aufzeichnen von Audio in der ICA-Sitzung beginnen. Wenn ein Aufzeichnungsgerät angeschlossen wird, nachdem die Audioaufzeichnungsanwendung gestartet wurde, reagiert die Anwendung u. U. nicht mehr und muss neu gestartet werden. Ein ähnliches Problem kann auftreten, wenn Sie ein Aufzeichnungsgerät während der Aufzeichnung entfernen.
- Bei Citrix Receiver für Windows können während der Aufzeichnung Audiostörungen auftreten.

Hinweise zu Drittanbietern

December 9, 2022

Linux Virtual Desktop Version 7.15 (PDF-Download)

Dieses Release des Linux VDA enthält u. U. Software von Drittanbietern, die gemäß den Bedingungen in dem Dokument lizenziert wurden.

Systemanforderungen

March 26, 2021

Linux-Distributionen

Folgende Linux-Distributionen werden vom Linux VDA unterstützt:

- SUSE Linux Enterprise:
  - Desktop 12 Service Pack 2
  - Server 12 Service Pack 2
  - Server 11 Service Pack 4
- Red Hat Enterprise Linux
  - Workstation 7.3
  - Workstation 6.9
  - Workstation 6.6
  - Server 7.3
  - Server 6.9
  - Server 6.6
- CentOS Linux
  - CentOS 7.3
  - CentOS 6.6
- Ubuntu Linux
  - Ubuntu Desktop 16.04 (mit Kernelversion 4.4.x)
  - Ubuntu Server 16.04 (mit Kernelversion 4.4.x)

Die folgende Tabelle bietet eine Übersicht der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden. Weitere Informationen finden Sie unter XorgModuleABIVersions.

Linux-Distribution	Xorg-Version
RHEL 7.3, CentOS 7.3	1.17
RHEL 6.9	1.17
RHEL 6.6, CentOS 6.6	1.15
Ubuntu 16.04	1.18
SUSE 12.2	1.18
SUSE 11.4	1.6.5

Verwenden Sie den HWE Xorg-Server 1.19 nicht in Ubuntu 16.04.

In allen Fällen wird die Prozessorarchitektur x86-64 unterstützt.

> **Hinweis:**
>
> Citrix unterstützt Plattformen und Versionen von Linux OS nur so lange, wie diese vom Betriebssystemhersteller unterstützt werden.
>
> **Wichtig:**
>
> Gnome- und KDE-Desktops werden in SUSE, RHEL und CentOS unterstützt Unity-Desktop wird nur unter Ubuntu unterstützt. Mindestens ein Desktop muss installiert sein.

XenDesktop

Der Linux VDA ist kompatibel mit allen zurzeit unterstützten Versionen von XenDesktop. Weitere Informationen zum XenDesktop-Produktlebenszyklus und wann Citrix die Unterstützung bestimmter Produktversionen beendet, finden Sie unter Citrix Product Lifecycle Matrix.

Die Konfiguration von Linux VDAs ist etwas anders als bei Windows VDAs. Alle Delivery Controller-Farmen können jedoch Windows- und Linux-Desktops vermitteln.

> **Hinweis:**
>
> Der Linux VDA ist nicht mit XenDesktop 7.0 oder früheren Versionen kompatibel.

Citrix Receiver

Die folgenden Versionen von Citrix Receiver werden unterstützt:

- Citrix Receiver für UWP (Universelle Windows-Plattform) Version 1.0
- Citrix Receiver für Windows Version 4.8 oder höher
- Citrix Receiver für Linux Version 13.5
- Citrix Receiver für Mac OSX Version 12.6 oder höher
- Citrix Receiver für Android Version 3.11
- Citrix Receiver für iOS Version 7.2
- Citrix Receiver für Chrome Version 2.5
- Citrix Receiver für HTML5 Version 2.5 (nur über Access Gateway)

Hypervisors

Die folgenden Hypervisors werden zum Hosten von Linux VDA Gast-VMs unterstützt:

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

- Nutanix AHV

Bare-Metal-Hosting wird ebenfalls unterstützt.

> **Tipp:**
>
> Eine Liste der unterstützten Plattformen finden Sie in der Herstellerdokumentation.

Active Directory-Integrationspakete

Die folgenden Active Directory-Integrationspakete und -produkte werden vom Linux VDA unterstützt:

- Samba Winbind
- Quest Authentication Services v4.1 oder höher
- Centrify DirectControl
- SSSD

> **Tipp:**
>
> Eine Liste der unterstützten Plattformen finden Sie in der Dokumentation der Hersteller der Active Directory-Integrationspakete.

HDX 3D Pro

Die folgenden Hypervisors, Linux-Distributionen und NVIDIA GRID™ GPU sind für die Unterstützung von HDX 3D Pro erforderlich.

Hypervisors

Die folgenden Hypervisors werden unterstützt:

- XenServer
- VMware ESX und ESXi
- Nutanix AHV

Linux-Distributionen

Die folgenden Linux-Distributionen unterstützen HDX 3D Pro:

- Red Hat Enterprise Linux - Workstation 7.3
- Red Hat Enterprise Linux - Server 7.3
- Red Hat Enterprise Linux - Workstation 6.9

- Red Hat Enterprise Linux - Server 6.9
- Red Hat Enterprise Linux - Workstation 6.6
- Red Hat Enterprise Linux - Server 6.6
- SUSE Linux Enterprise Desktop 12 Service Pack 2
- SUSE Linux Enterprise Server 12 Service Pack 2
- Ubuntu Linux Desktop 16.04
- Ubuntu Linux Server 16.04

Grafikprozessor

Für die folgenden GPUs wird GPU-Passthrough unterstützt:

- NVIDIA GTX750Ti
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - K2

Für die folgenden GPUs wird vGPU unterstützt:

- NVIDIA GRID - Tesla M60
- NVIDIA GRID - Tesla M10

Installationsübersicht

February 21, 2019

Die allgemeinen Schritte zum Installieren des Linux Virtual Delivery Agent (VDA) sind dieselben bei allen unterstützten Linux-Distributionen.

1. Vorbereiten der Installation
2. Vorbereiten des Hypervisors
3. Hinzufügen der virtuellen Linux-Maschine zur Windows-Domäne
4. Installieren des Linux VDA
5. Konfigurieren des Linux VDA
6. Erstellen des Maschinenkatalogs in XenApp oder XenDesktop
7. Erstellen der Bereitstellungsgruppe in XenApp oder XenDesktop

Abweichungen und spezielle Befehle sind für jede Distribution dokumentiert.

Konfigurieren von Delivery Controllern

May 11, 2020

XenDesktop 7.6 oder frühere Version erfordern Änderungen, damit der Linux VDA unterstützt wird. Für diese Versionen ist ein Hotfix oder Updateskript erforderlich. Anleitungen zur Installation und Überprüfung finden Sie in diesem Artikel.

Aktualisieren der Delivery Controller-Konfiguration

Wenden Sie bei XenDesktop 7.6 SP2 das Hotfix Update 2 an, um den Broker für Linux Virtual Desktops zu aktualisieren. Hotfix Update 2 ist hier verfügbar:

- CTX142438: Hotfix Update 2 - für Delivery Controller 7.6 (32 Bit) –Englisch
- CTX142439: Hotfix Update 2 - für Delivery Controller 7.6 (64 Bit) –Englisch

Für Versionen vor XenDesktop 7.6 SP2 können Sie das PowerShell-Skript **Update-BrokerServiceConfig.ps1** verwenden, um die Brokerdienstkonfiguration zu aktualisieren. Dieses Skript ist im folgenden Paket verfügbar:

- citrix-linuxvda-scripts.zip

Führen Sie die folgenden Schritte auf jedem Delivery Controller in der Farm aus:

1. Kopieren Sie das Skript **Update-BrokerServiceConfig.ps1** auf den Delivery Controller.
2. Öffnen Sie als lokaler Administrator eine Windows PowerShell-Konsole.
3. Navigieren Sie zu dem Ordner, der das Skript **Update-BrokerServiceConfig.ps1** enthält.
4. Führen Sie das Skript **Update-BrokerServiceConfig.ps1** aus:

```
.\Update-BrokerServiceConfig.ps1
<!--NeedCopy-->
```

> **Tipp:**
>
> Standardmäßig verhindert die Konfiguration von PowerShell das Ausführen von PowerShell-Skripts. Wenn das Skript nicht ausgeführt wird, müssen Sie die PowerShell-Ausführungsrichtlinie ändern und das Skript erneut ausführen:
>
> ```
> Set-ExecutionPolicy Unrestricted
> <!--NeedCopy-->
> ```

Das Skript **Update-BrokerServiceConfig.ps1** aktualisiert die Brokerdienstkonfigurationsdatei mit neuen WCF-Endpunkten, die der Linux VDA erfordert, und startet den Brokerdienst neu. Das Skript

bestimmt den Speicherort der Brokerdienstkonfigurationsdatei automatisch. Im selben Verzeichnis wird ein Backup der ursprünglichen Konfigurationsdatei mit der Dateinamenerweiterung **.prelinux** angelegt.

Diese Änderungen haben keine Auswirkungen auf die Vermittlung von Windows VDAs, die dieselbe Delivery Controller-Farm verwenden. Mit nur einer Controller-Farm können Sitzungen für Windows und Linux VDAs nahtlos verwaltet und vermittelt werden.

Überprüfen der Delivery Controller-Konfiguration

Nachdem die erforderlichen Konfigurationsänderungen auf einen Delivery Controller angewendet wurden, wird die Zeichenfolge **EndpointLinux** fünfmal in der Datei **%PROGRAMFILES%\Citrix\Broker\Service\B** angezeigt.

Melden Sie sich an der Windows-Eingabeaufforderung als lokaler Administrator an, um dies zu prüfen:

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

Easy Install

June 16, 2022

Easy Install wird offiziell ab Linux VDA-Version 7.13 unterstützt. Mit "Easy Install"(einfache Installation) können Sie die Umgebung zum Ausführen des Linux VDA einrichten, wobei die erforderlichen Pakete automatisch installiert und die Konfigurationsdateien automatisch angepasst werden.

Unterstützte Distributionen

	Winbind	SSSD	Centrify
RHEL 7.3	Ja	Ja	Ja
RHEL 6.9	Ja	Ja	Ja
RHEL 6.6	Ja	Ja	Ja
CentOS 7.3	Ja	Ja	Ja
Ubuntu 16.04	Ja	Ja	Ja

	Winbind	SSSD	Centrify
SUSE 12.2	Ja	Nein	Ja

Verwenden von Easy Install

Um dieses Feature zu verwenden, führen Sie folgende Schritte aus:

1. Bereiten Sie die Konfigurationsinformationen und die Linux-Maschine vor.
2. Installieren Sie das Linux VDA-Paket.
   Rufen Sie die Citrix-Website auf und laden Sie das entsprechende Linux VDA-Paket herunter, je nach Linux-Distribution.
3. Richten Sie die Laufzeitumgebung für die Linux VDA-Installation ein.

Schritt 1: Vorbereiten der Konfigurationsinformationen und der Linux-Maschine

Halten Sie die folgenden Konfigurationsinformationen für Easy Install bereit:

- Hostname: Hostname der Maschine, auf der der Linux VDA installiert werden soll
- IP-Adresse des Domänennamenservers
- IP-Adresse oder Zeichenfolgenname des NTP-Servers
- Domänenname: Der kurze NetBIOS-Name der Active Directory-Domäne
- Bereichsname: Der Kerberos-Bereichsname
- FQDN der aktiven Domäne: Vollqualifizierter Domänenname

> **Wichtig:**
>
> - Für die Installation des Linux VDA muss sichergestellt sein, dass die Repositorys der Linux-Maschine richtig hinzugefügt wurden.
> - Zum Starten einer Sitzung muss sichergestellt sein, dass das X Window System und die Desktopumgebungen installiert sind.

Schritt 2: Installieren des Linux VDA-Pakets

Führen Sie die folgenden Befehle aus, um die Umgebung für den Linux VDA einzurichten.

RHEL- und CentOS-Distributionen:

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

Ubuntu-Distributionen:


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

SUSE-Distributionen:

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

Schritt 3: Einrichten der Laufzeitumgebung für die Linux VDA-Installation

Nach der Installation des Linux VDA-Pakets müssen Sie die Laufzeitumgebung konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Sie können das Skript im interaktiven Modus oder im automatischen Modus ausführen.

Interaktiver Modus:

Führen Sie für eine manuelle Konfiguration den folgenden Befehl aus und geben Sie die entsprechenden Parameter an jeder Eingabeaufforderung ein.

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

Automatischer Modus:

Um Easy Install im automatischen Modus zu verwenden, müssen Sie die folgenden Umgebungsvariablen vor dem Ausführen von “ctxinstall”festgelegt.

- **CTX_EASYINSTALL_HOSTNAME**=host-name –Der Hostname des Linux VDA-Servers.
- **CTX_EASYINSTALL_DNS**=ip-address-of-dns –IP-Adresse des DNS.
- **CTX_EASYINSTALL_NTPS**=address-of-ntps –IP-Adresse oder Zeichenfolgenname des NTP-Servers.
- **CTX_EASYINSTALL_DOMAIN**=domain-name –Der NetBIOS-Name der Domäne.
- **CTX_EASYINSTALL_REALM**=realm-name –Der Kerberos-Bereichsname.
- **CTX_EASYINSTALL_FQDN**=ad-fqdn-name
- **CTX_EASYINSTALL_ADINTEGRATIONWAY**=winbind | sssd | centrify –Die Active Directory-Integrationsmethode.
- **CTX_EASYINSTALL_USERNAME**=domain-user-name –Der Name des Domänenbenutzers; wird zum Domänenbeitritt verwendet.
- **CTX_EASYINSTALL_PASSWORD**=password –Das Kennwort des Domänenbenutzers; wird zum Domänenbeitritt verwendet.

Die folgenden Variablen werden von ctxsetup.sh verwendet:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME** = Y | N –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz.
- **CTX_XDL_DDC_LIST**=list-ddc-fqdns –Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME muss angegeben werden.
- **CTX_XDL_VDA_PORT**=port-number –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port.
- **CTX_XDL_REGISTER_SERVICE** = Y | N –Die Linux Virtual Desktop-Dienste werden nach dem Systemstart gestartet.
- **CTX_XDL_ADD_FIREWALL_RULES**=Y | N –Für die Linux Virtual Desktop-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen.
- **CTX_XDL_HDX_3D_PRO**=Y | N –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Bei aktiviertem HDX 3D Pro wird der VDA für VDI-Desktopmodus (Einzelsitzungen) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE**=Y | N –Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Legen Sie den Wert bei Umgebungen mit HDX 3D Pro auf "Y"fest.
- **CTX_XDL_SITE_NAME**=dns-name –Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Wenn dies unnötig ist, kann **<none>** festgelegt werden.
- **CTX_XDL_LDAP_LIST**=list-ldap-servers –Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389. Wenn dies unnötig ist, kann **<none>** festgelegt werden.
- **CTX_XDL_SEARCH_BASE**=search-base-set –Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Wenn dies unnötig ist, kann **<none>** festgelegt werden.
- **CTX_XDL_START_SERVICE**=Y | N –Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Konfiguration abgeschlossen ist.

Wenn ein Parameter nicht festgelegt ist, wird die Installation in den interaktiven Modus versetzt und eine Benutzereingabe ist erforderlich. Das Skript ctxinstall.sh fordert keine Antworten, wenn alle Parameter bereits über die Umgebungsvariablen voreingestellt sind.

Im automatischen Modus müssen Sie erst die folgenden Befehle ausführen, um die Umgebungsvariablen einzurichten. Führen Sie dann das Skript ctxinstall.sh aus.


```
export CTX_EASYINSTALL_HOSTNAME=host-name

export CTX_EASYINSTALL_DNS=ip-address-of-dns

export CTX_EASYINSTALL_NTPS=address-of-ntps

export CTX_EASYINSTALL_DOMAIN=domain-name

export CTX_EASYINSTALL_REALM=realm-name

export CTX_EASYINSTALL_FQDN=ad-fqdn-name

export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify

export CTX_EASYINSTALL_USERNAME=domain-user-name

export CTX_EASYINSTALL_PASSWORD=password

export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y | N

export CTX_XDL_ADD_FIREWALL_RULES=Y | N

export CTX_XDL_HDX_3D_PRO=Y | N

export CTX_XDL_VDI_MODE=Y | N

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

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

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

export CTX_XDL_START_SERVICE=Y | N

sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
<!--NeedCopy-->
```

Sie müssen die Option -E mit dem Befehl “sudo”angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Citrix empfiehlt, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:

```
sudo CTX_EASYINSTALL_HOSTNAME=host-name \

CTX_EASYINSTALL_DNS=ip-address-of-dns \

```



```
CTX_EASYINSTALL_NTPS=address-of-ntps \

CTX_EASYINSTALL_DOMAIN=domain-name \

CTX_EASYINSTALL_REALM=realm-name \

......

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y \

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

Überlegungen

- Der Arbeitsgruppenname ist standardmäßig der Domänenname. Mit folgenden Schritten passen Sie die Arbeitsgruppe in Ihrer Umgebung an:

  a. Erstellen Sie die Datei /tmp/ctxinstall.conf auf der Linux VDA-Maschine.
  b. Fügen Sie der Datei die Zeile "workgroup=<your workgroup>"hinzu.

- Centrify unterstützt keine reine IPv6-DNS-Konfiguration. Es ist mindestens ein DNS-Server mit IPv4 in /etc/resolv.conf für `adclient` erforderlich, damit die AD-Dienste ordnungsgemäß gefunden werden.

- Easy Install kann für Centrify unter CentOS beim Centrify-Tool für die Umgebungsprüfung "`adcheck`"fehlschlagen und meldet dann den folgenden Fehler:

  Protokoll:

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

  Dieses Problem basiert auf der speziellen Konfiguration von Centrify. Führen Sie folgende Schritte aus, um das Problem zu beheben:

  a. Öffnen Sie **Verwaltungstools** auf dem Delivery Controller.
  b. Wählen Sie **Active Directory-Standorte und -Dienste** aus.
  c. Geben Sie in **Subnetze** eine richtige Subnetzadresse ein.

- Wenn Sie Centrify als Methode zum Domänenbeitritt wählen, benötigt das Skript ctxinstall.sh das Centrify-Paket. Es gibt zwei Möglichkeiten für ctxinstall.sh, das Centrify-Paket abzurufen:

- Mit Easy Install wird das Centrify-Paket automatisch über das Internet heruntergeladen. Dies sind die URLs für die Distributionen:

  RHEL: wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-rhel4-x86_64.tgz?_ga=1.178323680.558673738.1478847956

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

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

  Ubuntu: wget http://edge.centrify.com/products/centrify-suite/2016-update-1/installers/centrify-suite-2016.1-deb7-x86_64.tgz?_ga=1.178323680.558673738.1478847956

- Abrufen des Centrify-Pakets von einem lokalen Verzeichnis. Führen Sie die folgenden Schritte aus, um das Verzeichnis des Centrify-Pakets festzulegen:

  a. Erstellen Sie die Datei /tmp/ctxinstall.conf auf dem Linux VDA-Server, wenn sie nicht vorhanden ist.
  b. Fügen Sie der Datei die Zeile “centrifypkgpath=<path name>”hinzu.

  Beispiel:

```
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
```



```
16                    4 -r--r--r--. 1 root root     2749 Apr  7
        2015 release-notes-nis-rhel4-x86_64.txt
17                    12 -r--r--r--. 1 root root     9133 Mar 21
        2016 release-notes-openssh-rhel4-x86_64.txt
18  <!--NeedCopy-->
```

Problembehandlung

Verwenden Sie die Informationen in diesem Abschnitt, um Probleme zu beheben, die sich aus der Verwendung dieser Funktion ergeben können.

Fehler beim Beitreten zu einer Domäne mit SSSD

Beim Versuch, einer Domäne beizutreten, kann ein Fehler auftreten, wobei die Ausgabe ähnlich wie das folgende Ergebnis aussieht (siehe Protokolle):

```
Step 6: join Domain!Enter ctxadmin's password:Failed to join domain:
 failed to lookup DC info for domain 'CITRIXLAB.LOCAL'over rpc: The
network name cannot be found
```

/var/log/xdl/vda.log:

```
1  2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service
       successfully obtained the following list of 1 delivery controller(s)
        with which to register: 'CTXDDC.citrixlab.local (10.158.139.214)'.
2  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))
3  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')
4  Check the following:- The system clock is in sync between this machine
       and the delivery controller.
5  -  The Active Directory provider (e.g. winbind daemon) service is
       running and correctly configured.
6  -  Kerberos is correctly configured on this machine.
7  If the problem persists, please refer to Citrix Knowledge Base article
       CTX117248 for further information.
8  Error Details:
9  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'.
10 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.
11 Ensure that the system clock is in sync between this machine and the
       delivery controller.
```



```
12 Verify the NTP daemon is running on this machine and is correctly
      configured.
13 2016-11-04 02:11:52.364 [ERROR] - Could not register with any
      controllers. Waiting to try again in 120000 ms. Multi-forest - false
14 2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
      register with any controllers in the last 470 minutes.
15 <!--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
```

Lösen des Problems:

1. Führen Sie den Befehl `rm -f /etc/krb5.keytab` aus.
2. Führen Sie den Befehl `net ads leave $REALM -U $domain-administrator` aus.
3. Entfernen Sie den Maschinenkatalog und die Bereitstellungsgruppe vom Delivery Controller.
4. Führen Sie /opt/Citrix/VDA/sbin/ctxinstall.sh aus.
5. Erstellen Sie den Maschinenkatalog und die Bereitstellungsgruppe auf dem Delivery Controller.

Grauer Bildschirm bei Ubuntu Desktopsitzungen

Dieses Problem tritt auf, wenn Sie eine Sitzung starten, die dann in einem leeren Desktop blockiert wird. Darüber hinaus zeigt die Konsole der Serverbetriebssystemmaschine bei der Anmeldung mit einem lokalen Benutzerkonto einen grauen Bildschirm an.

Lösen des Problems:

1. Führen Sie den Befehl `sudo apt-get update` aus.
2. Führen Sie den Befehl `sudo apt-get install unity lightdm` aus.
3. Fügen Sie /etc/lightdm/lightdm.conf folgende Zeile hinzu:
   greeter-show-manual-login=true

Ubuntu Desktop-Sitzungen können aufgrund des fehlenden Homeverzeichnisses nicht gestartet werden

/var/log/xdl/hdx.log:

```
1 2016-11-02 13:21:19.015 <P22492:S1> citrix-ctxlogin: StartUserSession:
      failed to change to directory(/home/CITRIXLAB/ctxadmin) errno(2)
```

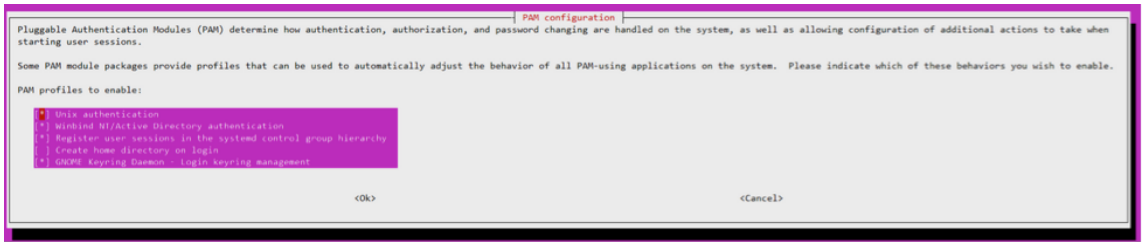


```
2
3 2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:
     Session started for user ctxadmin.
4
5 2016-11-02 13:21:19.023 <P22492:S1> citrix-ctxlogin: ChildPipeCallback:
      Login Process died: normal.
6
7 2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting
     normally.
8 <!--NeedCopy-->
```

> **Tip:**
>
> Die Ursache für dieses Problem ist, dass das Homeverzeichnis nicht für den Domänenadministrator erstellt wurde.

Lösen des Problems:

1. Geben Sie an einer Befehlszeile **pam-auth-update** ein.
2. Überprüfen Sie im angezeigten Popupfenster, ob **Create home directory login** ausgewählt ist.



Sitzung kann nicht gestartet werden oder wird mit dbus-Fehler schnell beendet

/var/log/messages (für RHEL oder CentOS):

```
1 Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
     CITRIXLAB\ctxadmin.
2
3 Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
     ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0
4
5 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...
6
7 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)
8
9 Oct 27 04:17:18 CentOS7 gnome-session: aborting...
```



```
10
11 Oct 27 04:17:18 CentOS7 citrix-ctxgfx[18981]: Exiting normally.
12
13 Oct 27 04:17:18 CentOS7 citrix-ctxhdx[8978]: Session stopped for user
       CITRIXLAB\ctxadmin.
14 <!--NeedCopy-->
```

Für Ubuntu-Distributionen können Sie auch das Protokoll /var/log/syslog verwenden:

```
1  Nov  3 11:03:52 user01-HVM-domU pulseaudio[25326]: [pulseaudio] pid.c:
       Stale PID file, overwriting.
2
3  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.
4
5  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.
6
7  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.
8
9  Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
       times: [ [pulseaudio] core-util.c: Failed to connect to system bus:
       Did not receive a reply. Possible causes include: the remote
       application did not send a reply, the message bus security policy
       blocked the reply, the reply timeout expired, or the network
       connection was broken.]
10
11 Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
       Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-ctxgfx
       [24693]: Exiting normally
12 <!--NeedCopy-->
```

Einige Gruppen oder Module werden erst nach einem Neustart wirksam. Wenn im Protokoll Fehlermeldungen zu **dbus** angezeigt werden, empfiehlt Citrix, das System neu zu starten und den Vorgang zu wiederholen.

SELinux verhindert den Zugriff auf das Homeverzeichnis durch SSHD

Der Benutzer kann eine Sitzung starten, er kann sich jedoch nicht anmelden.

/var/log/ctxinstall.log:


```
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

Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/
    sbin/sshd from setattr access on the directory /root.

*****  Plugin catchall_boolean (89.3 confidence) suggests
    ******************

If you want to allow polyinstantiation to enabled

   Then you must tell SELinux about this by enabling the '
    polyinstantiation_enabled' boolean.

You can read 'None' man page for more details.

    Do

       setsebool -P polyinstantiation_enabled 1

*****  Plugin catchall (11.6 confidence) suggests
    **************************

If you believe that sshd should be allowed setattr access on the root
    directory by default.

Then you should report this as a bug.

You can generate a local policy module to allow this access.

      Do

       allow this access for now by executing:

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

# semodule -i mypol.pp
<!--NeedCopy-->
```

Lösen des Problems:

1. Deaktivieren Sie SELinux, indem Sie die folgende Änderung an /etc/selinux/config vornehmen:

   SELINUX=disabled

2. Starten Sie den VDA neu.

Installieren von Linux Virtual Delivery Agent für RHEL/CentOS

June 16, 2022

Mit den Schritten in diesem Artikel können Sie die Installation manuell durchführen, oder verwenden Sie Easy Install für die automatische Installation und Konfiguration. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die manuelle Installation.

> **Hinweis:**
>
> Verwenden Sie Easy Install bei Neuinstallationen. Zum Aktualisieren von vorhandenen Installationen eignet Easy Install sich nicht.

Schritt 1: Vorbereiten von RHEL 7/CentOS 7 oder RHEL 6/CentOS 6 für die VDA-Installation

Schritt 1a: Überprüfen der Netzwerkkonfiguration

Citrix empfiehlt, dass Netzwerk zu verbinden und richtig zu konfigurieren, bevor Sie fortfahren.

Schritt 1b: Festlegen des Hostnamens

> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit nicht das Abschneiden von NetBIOS-Namen. Der Name darf daher nicht länger als 15 Zeichen sein.

Damit der Hostname der Maschine richtig gemeldet wird, ändern Sie die Datei **/etc/hostname**, sodass sie nur den Hostnamen der Maschine enthält.

`HOSTNAME`=**hostname**

Schritt 1c: Zuweisen einer Loopbackadresse für den Hostnamen

> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit nicht das Abschneiden von NetBIOS-Namen. Der Name darf daher nicht länger als 15 Zeichen sein.

Damit der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine richtig gemeldet werden, ändern Sie die folgende Zeile in der Datei **/etc/hosts**, sodass der FQDN und der Hostname die ersten zwei Einträge sind:

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

Beispiel:

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

Entfernen Sie alle anderen Verweise auf **hostname-fqdn** oder **hostname** aus anderen Einträgen in der Datei.

> **Tipp:**
>
> Verwenden Sie nur Buchstaben (a-z oder A-Z), Ziffern (0-9) und Bindestriche (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Hostnamen sollten nicht mit einer Zahl beginnen und nicht mit einem Bindestrich enden. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Schritt 1d: Überprüfen des Hostnamens

Stellen Sie sicher, dass der Hostname richtig festgelegt ist:

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

Mit diesem Befehl wird nur der Hostname der Maschine und nicht der vollqualifizierte Domänenname (FQDN) zurückgegeben.

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

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

Dieser Befehl gibt den FQDN der Maschine zurück.

Schritt 1e: Überprüfen von Namensauflösung und Diensterreichbarkeit

Stellen Sie sicher, dass Sie den FQDN auflösen können und pingen Sie den Domänencontroller und den Delivery Controller:

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

Wenn Sie den FQDN nicht auflösen und eine der beiden Maschinen nicht pingen können, überprüfen Sie die vorherigen Schritte, bevor Sie fortfahren.

Schritt 1f: Konfigurieren der Uhrsynchronisierung

Es ist wichtig, dass die Uhrsynchronisierung zwischen den VDAs, den Delivery Controllern und den Domänencontrollern genau ist. Beim Hosten eines Linux VDAs als virtuelle Maschine kann es zu Zeitabweichungen kommen. Aus diesem Grund sollte die Zeit remote von einem Zeitdienst synchronisiert werden.

RHEL 6.x und frühere Releases verwenden den NTP-Daemon (`ntpd`) zum Synchronisieren der Uhr, während in einer RHEL 7.x-Standardumgebung der neuere Chrony-Daemon (`chronyd`) verwendet wird. Die Konfiguration und Betriebsprozesse zwischen den beiden Diensten sind ähnlich.

Konfigurieren des NTP-Diensts (nur für RHEL 6/CentOS 6) Bearbeiten Sie als Root-Benutzer die Datei **/etc/ntp.conf** und fügen Sie pro Remote-Zeitserver einen Servereintrag hinzu:

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

server peer2-fqdn-or-ip-address iburst
<!--NeedCopy-->
```

In einer typischen Bereitstellung synchronisieren Sie die Zeit von den lokalen Domänencontrollern und nicht direkt von öffentlichen NTP-Poolservern. Fügen Sie pro Active Directory-Domänencontroller in der Domäne einen Servereintrag hinzu.

Entfernen Sie alle anderen **Servereinträge**, einschließlich Einträge für Loopback-IP-Adresse, Localhost und öffentliche Servereinträge wie ***.pool.ntp.org**.

Speichern Sie die Änderungen und starten Sie den NTP-Daemon neu:

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

Konfigurieren des Chrony-Diensts (nur für RHEL 7/CentOS 7) Bearbeiten Sie als Root-Benutzer die Datei **/etc/chrony.conf** und fügen Sie pro Remote-Zeitserver einen Servereintrag hinzu:

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

server peer2-fqdn-or-ip-address iburst
<!--NeedCopy-->
```

In einer typischen Bereitstellung synchronisieren Sie die Zeit von den lokalen Domänencontrollern und nicht direkt von öffentlichen NTP-Poolservern. Fügen Sie pro Active Directory-Domänencontroller in der Domäne einen Servereintrag hinzu.

Entfernen Sie alle anderen Servereinträge, einschließlich Einträge für Loopback-IP-Adresse, Localhost und öffentliche Servereinträge wie ***.pool.ntp.org**.

Speichern Sie die Änderungen und starten Sie den Chrony-Daemon neu:


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

Schritt 1g: Installieren von OpenJDK

Der Linux VDA ist von OpenJDK abhängig. Üblicherweise wird die Laufzeitumgebung als Teil der Betriebssysteminstallation installiert.

Bestätigen Sie die richtige Version:

- RHEL 7/CentOS 7:

```
sudo yum info java-1.8.0-openjdk
<!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
sudo yum info java-1.7.0-openjdk
<!--NeedCopy-->
```

Das OpenJDK-Paket ist möglicherweise eine frühere Version. Aktualisieren Sie ggf. auf die aktuelle Version:

- RHEL 7/CentOS 7:

```
sudo yum -y update java-1.8.0-openjdk
<!--NeedCopy-->
```

- RHEL 6/CentOS 6:

```
sudo yum -y update java-1.7.0-openjdk
<!--NeedCopy-->
```

Legen Sie die Umgebungsvariable **JAVA_HOME** fest, indem Sie der Datei **~/.bashrc** folgende Zeile hinzufügen:

```
export JAVA\\_HOME=/usr/lib/jvm/java
```

Öffnen Sie eine neue Shell und prüfen Sie die Java-Version:

```
java -version
<!--NeedCopy-->
```

> **Tipp:**
>
> Stellen Sie zum Vermeiden von Problemen sicher, dass bei RHEL 6/CentOS 6 nur die OpenJDK-Version 1.7.0 oder 1.8.0 installiert ist und bei RHEL 7/CentOS 7 nur die OpenJDK-Version 1.8.0.

> Entfernen Sie alle anderen Java-Versionen vom System.

Schritt 1h: Installieren von PostgreSQL

Der Linux VDA erfordert auf RHEL 6 PostgreSQL 8.4 oder höher und auf RHEL 7 PostgreSQL 9.2 oder höher.

Installieren Sie die folgenden Pakete:

```
sudo yum -y install postgresql-server

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

Anschließend ist der folgende Schritt erforderlich, um die Datenbank zu initialisieren und zu gewährleisten, dass der Dienst beim Systemstart startet. Mit der Aktion werden unter **/var/lib/pgsql/-data** Datenbankdateien erstellt. Der Befehl ist für PostgreSQL 8 und PostgreSQL 9 unterschiedlich:

- Nur RHEL 7: PostgreSQL 9

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

- Nur RHEL 6: PostgreSQL 8

```
sudo /sbin/service postgresql initdb
<!--NeedCopy-->
```

Schritt 1i: Starten von PostgreSQL

Konfigurieren Sie den Dienst so, dass er beim Systemstart der Maschine startet und sofort startet:

- Nur RHEL 7: PostgreSQL 9

```
sudo systemctl enable postgresql

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

- Nur RHEL 6: PostgreSQL 8

```
sudo /sbin/chkconfig postgresql on

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

Überprüfen Sie die Version von PostgreSQL mit folgendem Befehl:


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

Stellen Sie mit dem **psql**-Befehlszeilenprogramm sicher, dass das Datenverzeichnis festgelegt ist:

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

> **Wichtig:**
>
> Diesem Release wurde eine neue Abhängigkeit für gperftools-libs hinzugefügt, die im ursprünglichen Repository nicht vorhanden ist. Fügen Sie mit dem Befehl `sudo rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-6.noarch.rpm` ein neues Repository hinzu.
> Nur RHEL 6/CentOS 6 ist betroffen. Führen Sie vor der Installation des Linux VDA-Pakets folgenden Befehl aus:

Schritt 2: Vorbereiten des Hypervisors

Wenn Sie den Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausführen, sind einige Änderungen erforderlich. Nehmen Sie entsprechend der verwendeten Hypervisorplattform die folgenden Änderungen vor. Wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen, sind keine Änderungen erforderlich.

Festlegen der Zeitsynchronisierung auf Citrix XenServer

Wenn das Zeitsynchronisierungsfeature auf XenServer aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und XenServer gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen, auf denen ein paravirtualisierter Linux-Kernel mit installierten XenServer Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das XenServer-Zeitsynchronisierungsfeature vorhanden und aktiviert ist:

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

Dieser Befehl gibt 0 oder 1 zurück:

- 0: Das Zeitsynchronisierungsfeature ist aktiviert und muss deaktiviert werden.

- 1: Das Zeitsynchronisierungsfeature ist deaktiviert und keine weitere Aktion ist erforderlich.

Wenn die Datei /proc/sys/xen/indepent_wallclock nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

Wenn das Zeitsynchronisierungsfeature aktiviert ist, deaktivieren Sie es, indem Sie 1 in die Datei eingeben:

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

Damit die Änderung permanent wird und nach dem Neustart erhalten bleibt, fügen Sie in der Datei **/etc/sysctl.conf** die folgende Zeile hinzu:

```
xen.independent_wallclock = 1
```

Starten Sie das System neu, um die Änderungen zu überprüfen:

```
su -

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

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

Linux-VMs, auf denen Hyper-V Linux-Integrationsdienste installiert sind, können mit dem Hyper-V-Zeitsynchronisierungsfeature die Systemzeit des Hostbetriebssystems verwenden. Um sicherzustellen, dass die Betriebssystemzeit korrekt ist, müssen Sie das Feature zusätzlich zu den NTP-Diensten aktivieren.

Auf dem verwaltenden Betriebssystem:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Wählen Sie für die Einstellungen einer Linux-VM **Integration Services** aus.
3. Stellen Sie sicher, dass **Time synchronization** ausgewählt ist.

> **Hinweis:**
>
> Diese Methode unterscheidet sich von VMware und XenServer, wo die Hostzeitsynchronisierung deaktiviert ist, um Konflikte mit dem NTP zu vermeiden. Hyper-V-Zeitsynchronisierung kann gleichzeitig mit der NTP-Zeitsynchronisierung bestehen und sie ergänzen.

Festlegen der Zeitsynchronisierung auf ESX und ESXi

Wenn das VMware-Zeitsynchronisierungsfeature aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und der Hypervisor gleichzeitig versuchen, die Systemuhr zu synchronisieren. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel ausführen und VMware-Tools installiert sind:

1. Öffnen Sie den vSphere-Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Virtual Machine Properties** die Registerkarte **Options**.
4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Advanced** das Kontrollkästchen **Synchronize guest time with host**.

Schritt 3: Hinzufügen der virtuellen Linux-Maschine zur Windows-Domäne

Der Linux VDA unterstützt mehrere Methoden zum Hinzufügen von Linux-Maschinen zur Active Directory-Domäne:

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

Folgen Sie den Anweisungen für die von Ihnen gewählte Methode.

> **Hinweis:**
>
> Der Sitzungsstart kann fehlschlagen, wenn für das lokale Konto auf dem Linux VDA und das AD-Konto derselbe Benutzername verwendet wird.

Samba Winbind

Installieren oder aktualisieren Sie die erforderlichen Pakete:

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

Starten des Winbind-Daemon beim Booten Der Winbind-Daemon muss beim Systemstart gestartet werden:


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

Konfigurieren der Winbind-Authentifizierung Konfigurieren Sie die Maschine für die Kerberos-Authentifizierung mit Winbind:

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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **domain** ist der NetBIOS-Name der Domäne.

Wenn eine DNS-basierte Suche nach dem KDC-Server und -Bereichsnamen erforderlich ist, fügen Sie dem vorherigen Befehl die folgenden beiden Optionen hinzu:

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

Ignorieren Sie alle Fehler hinsichtlich des `winbind`-Dienststarts, die vom Befehl `authconfig` zurückgegeben wurden. Diese Fehler können auftreten, wenn `authconfig` versucht, den `winbind`-Dienst zu starten, bevor die Maschine mit einer Domäne verbunden wurde.

Öffnen Sie die Datei **/etc/samba/smb.conf** und fügen Sie im Abschnitt [Global] nach dem von dem Tool `authconfig` erstellten Abschnitt die folgenden Einträge hinzu:

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

Der Linux VDA benötigt die Systemdatei für die Schlüsseltabelle "/etc/krb5.keytab", um sich beim Delivery Controller zu authentifizieren und zu registrieren. Die vorherige Einstellung "kerberos method"zwingt Winbind zum Erstellen der Systemdatei für die Schlüsseltabelle, wenn die Maschine der Domäne beitritt.

Beitreten zu einer Windows-Domäne Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

Konfigurieren von PAM für Winbind Standardmäßig wird bei der Konfiguration des Winbind PAM-Moduls (pam_winbind) nicht das Zwischenspeichern von Kerberos-Tickets und das Erstellen von Basisverzeichnissen aktiviert. Öffnen Sie die Datei `/etc/security/pam_winbind.conf` und ändern Sie die folgenden Einträge im Abschnitt [Global] oder fügen Sie sie hinzu:

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

Entfernen Sie ggf. den Einstellungen vorangehende Semikolons. Diese Änderungen erfordern den Neustart des Winbind-Daemon:

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

> **Tipp:**
>
> Der Winbind-Daemon wird nur weiterhin ausgeführt, wenn die Maschine zu einer Domäne gehört.

Öffnen Sie die Datei **/etc/krb5.conf** und ändern Sie im Abschnitt [libdefaults] die folgende Einstellung von KEYRING in FILE:

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

Überprüfen der Domäneneigentümerschaft Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen(Windows und Linux VDAs) ein Computerobjekt in Active Directory haben.

Führen Sie den Samba-Befehl **net ads** aus, um zu prüfen, ob die Maschine zu einer Domäne gehört:

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

Führen Sie den folgenden Befehl aus, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen:

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

Überprüfen der Kerberos-Konfiguration Um sicherzustellen, dass Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, überprüfen Sie, ob die Systemdatei für die Schlüsseltabelle erstellt wurde und gültige Schlüssel enthält:

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


Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller mit diesen Schlüsseln zu authentifizieren:

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

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

Überprüfen der Benutzerauthentifizierung Überprüfen Sie mit dem **wbinfo**-Tool, dass Domänenbenutzer sich bei der Domäne authentifizieren können:

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

Die hier angegebene Domäne ist der AD-Domänenname und nicht der Kerberos-Bereichsname. Für die Bash-Shell muss der umgekehrte Schrägstrich (\) durch einen weiteren umgekehrten Schrägstrich geschützt werden. Bei diesem Befehl wird eine Erfolgs- oder Fehlermeldung zurückgegeben.

Um sich zu vergewissern, dass das Winbind-PAM-Modul fehlerfrei konfiguriert ist, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
ssh localhost -l domain\username

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

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache gültig und nicht abgelaufen sind:


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

Beenden Sie die Sitzung:

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

Quest Authentication Service

Konfigurieren von Quest auf dem Domänencontroller Es wird vorausgesetzt, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und über Administratorrechte zum Erstellen von Computerobjekten in Active Directory verfügen.

Domänenbenutzern die Anmeldung an Linux VDA-Maschinen ermöglichen Führen Sie folgende Schritte aus, damit Domänenbenutzer HDX-Sitzungen auf einer Linux VDA-Maschine herstellen können:

1. Öffnen Sie in der Verwaltungskonsole für Active Directory-Benutzer und -Computer die Active Directory-Eigenschaften für das jeweilige Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix Account** aus.
3. Aktivieren Sie das Kontrollkästchen **Unix-enabled**.
4. Legen Sie **Primary GID Number** auf die Gruppen-ID einer vorhandenen Domänenbenutzergruppe fest.

> **Hinweis:**
>
> Mit diesen Anleitungen können Domänenbenutzer für die Anmeldung mit der Konsole, RDP, SSH oder anderen Remotingprotokollen eingerichtet werden.

Konfigurieren von Quest auf Linux VDA

Workaround bei SELinux-Richtlinienerzwingung In der RHEL-Standardumgebung wird SELinux vollständig erzwungen. Das beeinträchtigt die von Quest verwendeten IPC-Methoden der Unix-Domänensockets und verhindert, dass Domänenbenutzer sich anmelden.

Der bequeme Weg, dieses Problem zu umgehen, ist die Deaktivierung von SELinux. Bearbeiten Sie als Root-Benutzer die Datei **/etc/selinux/config** und ändern Sie die **SELinux**-Einstellung:

`SELINUX=permissive`

Diese Änderung erfordert einen Neustart der Maschine:

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

> **Wichtig:**
>
> Seien Sie vorsichtig beim Verwenden dieser Einstellung. Das erneute Aktivieren der SELinux-Richtlinienerzwingung nach ihrer Deaktivierung kann selbst für den Root-Benutzer und anderen lokale Benutzer zu einer vollständigen Sperrung führen.

Konfigurieren eines VAS-Daemons Die automatische Erneuerung von Kerberos-Tickets muss aktiviert und getrennt sein. Authentifizierung (für Offlineanmeldung) muss deaktiviert sein.

```
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-->
```

Mit diesem Befehl wird das Verlängerungsintervall auf neun Stunden (32.400 Sekunden) festgelegt. Das ist eine Stunde weniger als die Standardgültigkeitsdauer (10 Stunden) eines Tickets. Bei Systemen mit einer kürzeren Ticketgültigkeitsdauer legen Sie diesen Parameter auf einen niedrigeren Wert fest.

Konfigurieren von PAM und NSS Um die Domänenbenutzeranmeldung über HDX und andere Dienste wie su, ssh und RDP zu aktivieren, führen Sie die folgenden Befehle aus, um PAM und NSS manuell zu konfigurieren:

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

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

Beitreten zu einer Windows-Domäne Machen Sie die Linux-Maschine mit dem Quest-Befehl `vastool` zu einem Mitglied der Active Directory-Domäne:

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

user ist ein beliebiger Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern der Active Directory-Domäne zu machen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Überprüfen der Domäneneigentümerschaft Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen(Windows und Linux VDAs) ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Quest angemeldete Linux-Maschine zur Domäne gehört:

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

Wenn die Maschine zu einer Domäne gehört, wird mit diesem Befehl der Domänenname zurückgegeben. Wenn die Maschine zu keiner Domäne gehört, wird die folgende Fehlermeldung angezeigt:

```
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
```

Überprüfen der Benutzerauthentifizierung Um sicherzustellen, dass Quest Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
ssh localhost -l domain\username

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

Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

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

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung:

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

Centrify DirectControl

Beitreten zu einer Windows-Domäne Wenn der Centrify DirectControl Agent installiert ist, machen Sie die Linux-Maschine mit dem Centrify-Befehl `adjoin` zu einem Mitglied der Active Directory-Domäne:

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

Der Parameter "user"ist ein beliebiger Active Directory-Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern der Active Directory-Domäne zu machen. **domain-name** ist der Name der Domäne, der die Linux-Maschine beitritt.

Überprüfen der Domäneneigentümerschaft Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen(Windows und Linux VDAs) ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Centrify hinzugefügte Linux-Maschine Mitglied der Domäne ist:

```
su -

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

Stellen Sie sicher, dass der Wert Joined to domain gültig ist und dass CentrifyDC mode den Wert connected zurückgibt. Wenn der Modus im Startzustand stecken bleibt, hat der Centrify-Client Serververbindungs- oder Authentifizierungsprobleme.

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all

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

Testen Sie die Verbindung mit den verschiedenen Active Directory- und Kerberos-Diensten. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

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

SSSD

Beim Einsatz von SSSD folgen Sie den Anweisungen in diesem Abschnitt. Dieser Abschnitt enthält Anweisungen zum Beitritt einer Linux VDA-Maschine zu einer Windows-Domäne und zum Konfigurieren der Kerberos-Authentifizierung.

Das Einrichten von SSSD unter RHEL und CentOS umfasst die folgenden Schritte:

1. Domänenbeitritt und Erstellen einer Hostschlüsseltabelle mit Samba
2. Einrichten von SSSD
3. Konfigurieren von NSS/PAM
4. Überprüfen der Kerberos-Konfiguration
5. Überprüfen der Benutzerauthentifizierung

Erforderliche Software Der Active Directory-Anbieter wurde mit SSSD Version 1.9.0 eingeführt. Wenn Sie eine ältere Version verwenden, folgen Sie den Anweisungen unter Configuring the LDAP provider with Active Directory.

Die folgenden Umgebungen wurden gemäß den Anweisungen in diesem Artikel getestet:

- RHEL 7.3 oder höher/CentOS 7.3 oder höher
- Linux VDA-Version 1.3 oder höher

Domänenbeitritt und Erstellen einer Hostschlüsseltabelle mit Samba SSSD bietet keine Active Directory-Clientfunktionen für den Domänenbeitritt und die Verwaltung der Systemschlüsseltabelle. Sie können stattdessen `adcli`, `realmd`, `Winbind` oder `Samba` verwenden.

Die Informationen in diesem Abschnitt basieren auf der Verwendung von `Samba`. Informationen über `realmd` finden Sie in der Dokumentation zu RHEL oder CentOS. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

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

Konfigurieren Sie die Maschine für die Authentifizierung mit Samba und Kerberos:

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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **domain** ist der kurze NetBIOS-Name der Active Directory-Domäne.

Wenn eine DNS-basierte Suche nach dem KDC-Server und -Bereichsnamen erforderlich ist, fügen Sie dem vorherigen Befehl die folgenden beiden Optionen hinzu:

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

Öffnen Sie die Datei **/etc/samba/smb.conf** und fügen Sie im Abschnitt **[Global]** nach dem von dem Tool **authconfig** erstellten Abschnitt die folgenden Einträge hinzu:


```
kerberos method = secrets and keytab
```

Treten Sie der Windows-Domäne bei. Stellen Sie sicher, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

Einrichten von SSSD Die Einrichtung von SSSD umfasst die folgenden Schritte:

- Installieren des Pakets **sssd-ad** auf dem Linux VDA
- Ändern der Konfiguration verschiedener Dateien (z. B. sssd.conf).
- Starten des Diensts **sssd**.

Muster einer **sssd.conf**-Konfiguration (zusätzliche Optionen können bei Bedarf hinzugefügt werden):

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

Ersetzen Sie **ad.example.com** und **server.ad.example.com** durch den jeweils gültigen Wert. Weitere Informationen finden Sie unter sssd-ad(5) - Linux man page.

Legen Sie Dateieigentümer und Berechtigungen für sssd.conf fest:

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

Konfigurieren von NSS/PAM RHEL/CentOS:

Aktivieren Sie SSSD mit `authconfig`. Installieren Sie **oddjob-mkhomedir**, damit die Erstellung des Homeverzeichnisses mit SELinux kompatibel ist:

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

sudo service sssd start

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

Überprüfen der Kerberos-Konfiguration Überprüfen Sie, ob die **Schlüsseltabelle**-Systemdatei erstellt wurde und gültige Schlüssel enthält:

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

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl **kinit** aus, um die Maschine mit dem Domänencontroller zu authentifizieren, die diese Schlüssel verwendet:

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

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen (**$**) muss durch einen umgekehrten Schrägstrich (****) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

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

Überprüfen der Benutzerauthentifizierung Prüfen Sie mit dem Befehl **getent**, ob das Anmeldeformat unterstützt wird und NSS funktioniert:

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

Der Parameter **DOMAIN** ist die kurze Version des Domänennamens. Wenn ein anderes Anmeldeformat von erforderlich ist, überprüfen Sie dies zunächst mit dem Befehl **getent**.

Unterstützte Anmeldeformate:

- Down-Level-Anmeldename: `DOMAIN\username`
- UPN: `username@domain.com`
- NetBIOS-Suffix-Format: `username@DOMAIN`

Um sich zu vergewissern, dass das SSSD-PAM-Modul fehlerfrei konfiguriert wurde, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
sudo ssh localhost  – l DOMAIN\username

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

Stellen Sie sicher, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **uid** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind: Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

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


Schritt 4: Installieren des Linux VDA

Schritt 4a: Deinstallieren der alten Version

Wenn bereits eine ältere Version des Linux VDA installiert ist, deinstallieren Sie diese Version, bevor Sie die neue Version installieren.

1. Halten Sie die Linux VDA-Dienste an:

```
sudo /sbin/service ctxvda stop

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

2. Deinstallieren Sie das Paket:

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

> **Hinweis:**
>
> Upgrades von den letzten zwei Versionen werden unterstützt.
>
> **Hinweis:**
>
> Ab Version 1.3 wurde der Installationspfad geändert. In vorherigen Releases waren die Installationskomponenten unter **/usr/local/**. Der neue Speicherort ist **/opt/Citrix/VDA/**.
>
> Zum Ausführen eines Befehls ist der vollständige Pfad erforderlich. Alternativ können Sie dem Systempfad **/opt/Citrix/VDA/sbin** und **/opt/Citrix/VDA/bin** hinzufügen.

Schritt 4b: Herunterladen des Linux VDA-Pakets

Rufen Sie die Citrix-Website auf und laden Sie das entsprechende Linux VDA-Paket herunter, je nach Linux-Distribution.

Schritt 4c: Installieren des Linux VDA

Installieren Sie die Linux VDA-Software mit `Yum`:

Für RHEL 7/CentOS 7:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.9:


```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

Installieren Sie die Linux VDA-Software mit dem RPM-Paketmanager. Vorher müssen folgende Abhängigkeiten aufgelöst werden:

Für RHEL 7/CentOS 7:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.9:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

RPM-Abhängigkeitsliste für RHEL 7:

```
postgresql-server >= 9.2

postgresql-jdbc >= 9.2

java-1.8.0-openjdk >= 1.8.0

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

libXpm >= 3.5.10

libXrandr >= 1.4.1

```



```
libXtst >= 1.2.2

motif >= 2.3.4

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

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

python-requests >= 2.6.0

gperftools-libs >= 2.4

xorg-x11-server-Xorg >= 1.17

xorg-x11-server-Xorg < 1.18

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
<!--NeedCopy-->
```

RPM-Abhängigkeitsliste für RHEL 6.9:

```
postgresql-jdbc >= 8.4

postgresql-server >= 8.4

java-1.7.0-openjdk >= 1.7.0

```



```
ImageMagick >= 6.5.4.7

GConf2 >= 2.28.0

system-config-firewall-base >= 1.2.27

policycoreutils-python >= 2.0.83

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.0.9

ConsoleKit >= 0.4.1

dbus >= 1.2.24

dbus-x11 >= 1.2.24

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

openmotif >= 2.3.3

pam >= 1.1.1

util-linux-ng >= 2.17.2

bash >= 4.1

findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.6.0

gperftools-libs >= 2.0
```



```
60
61 xorg-x11-server-Xorg >= 1.17
62
63 xorg-x11-server-Xorg < 1.18
64
65 rpmlib(FileDigests) <= 4.6.0-1
66
67 rpmlib(PayloadFilesHavePrefix) <= 4.0-1
68
69 rpmlib(CompressedFileNames) <= 3.0.4-1
70
71 rpmlib(PayloadIsXz) <= 5.2-1
72 <!--NeedCopy-->
```

RPM-Abhängigkeitsliste für RHEL 6.6/CentOS 6.6:

```
1  postgresql-jdbc >= 8.4
2
3  postgresql-server >= 8.4
4
5  java-1.7.0-openjdk >= 1.7.0
6
7  ImageMagick >= 6.5.4.7
8
9  GConf2 >= 2.28.0
10
11 system-config-firewall-base >= 1.2.27
12
13 policycoreutils-python >= 2.0.83
14
15 xorg-x11-server-utils >= 7.7
16
17 xorg-x11-xinit >= 1.0.9
18
19 ConsoleKit >= 0.4.1
20
21 dbus >= 1.2.24
22
23 dbus-x11 >= 1.2.24
24
25 libXpm >= 3.5.10
26
27 libXrandr >= 1.4.1
28
29 libXtst >= 1.2.2
30
31 openmotif >= 2.3.3
32
33 pam >= 1.1.1
34
35 util-linux-ng >= 2.17.2
36
37 bash >= 4.1
```



```
findutils >= 4.4

gawk >= 3.1

sed >= 4.2

cups >= 1.4.0

foomatic >= 4.0.0

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.6.0

gperftools-libs >= 2.0

xorg-x11-server-Xorg >= 1.15

xorg-x11-server-Xorg < 1.16

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
<!--NeedCopy-->
```

Schritt 4d: Upgrade des Linux VDA (optional)

Sie können die Versionen 7.14 und 7.13 der Linux VDA-Software mit `Yum` aktualisieren:

Für RHEL 7/CentOS 7:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.9:

```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6:


```
sudo yum install -y XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

Führen Sie ein Upgrade der Linux VDA-Software mit dem RPM-Paketmanager durch:

Für RHEL 7/CentOS 7:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el7_3.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.9:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_9.x86_64.rpm
<!--NeedCopy-->
```

RHEL 6.6/CentOS 6.6:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.el6_6.x86_64.rpm
<!--NeedCopy-->
```

> **Wichtig:**
>
> Starten Sie die Linux VDA-Maschine nach der Softwareaktualisierung neu.

Schritt 5: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro sind zusätzliche Installationsschritte erforderlich, um die erforderlichen Grafiktreiber auf dem Hypervisor und auf den VDA-Maschinen zu installieren.

Konfigurieren Sie Folgendes:

1. Citrix XenServer
2. VMware ESX

Folgen Sie den Anweisungen für den von Ihnen gewählten Hypervisor.

Citrix XenServer:

In diesem Abschnitt wird die Installation und Konfiguration von NVIDIA GRID-Treibern unter Citrix XenServer detailliert beschrieben.

VMware ESX:

Installieren und konfigurieren Sie die NVIDIA GRID-Treiber für VMware ESX entsprechend den Informationen in diesem Dokument.

VDA-Maschinen:

Führen Sie die folgenden Schritte aus, um die Treiber für die Linux-VM-Gäste zu installieren und zu konfigurieren:

1. Stellen Sie zu Beginn sicher, dass die Linux-VM heruntergefahren ist.
2. Fügen Sie in XenCenter der VM eine GPU im GPU-Passthroughmodus hinzu.
3. Starten Sie die RHEL-VM.

Zum Vorbereiten der Maschine für die NVIDIA GRID-Treiber müssen Sie folgende Befehle ausführen:

```
yum install gcc

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

systemctl set-default multi-user.target
<!--NeedCopy-->
```

Führen Sie die in den Anleitungen im Red Hat Enterprise Linux-Dokument aufgeführte Schrittfolge zum Installieren des NVIDIA GRID-Treibers aus.

> **Hinweis:**
>
> Wählen Sie während der GPU-Treiberinstallation für jede Frage den Standardwert (“no”).
>
> **Wichtig:**
>
> Nach dem Aktivieren des GPU-Passthrough kann auf die Linux-VM nicht mehr über XenCenter zugegriffen werden. Verwenden Sie SSH, um eine Verbindung herzustellen.

```
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                                                 |
+-----------------------------------------------------------------------------+
```

Legen Sie die richtige Konfiguration für die Karte fest:

`etc/X11/ctx-nvidia.sh`

Um die hohen Auflösungen und Multimonitorfunktionen nutzen zu können, benötigen Sie eine gültige NVIDIA-Lizenz. Anleitungen zum Anfordern der Lizenz finden Sie in der Produktdokumentation in “GRID Licensing Guide.pdf - DU-07757-001 September 2015”.

Schritt 6: Konfigurieren des Linux VDA

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Das Skript überprüft die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Führen Sie Änderungen erst danach durch. Sie können das Skript nach Bedarf jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell unter Reaktion auf Aufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript durch, bevor Sie fortfahren:

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

Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

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

Automatische Konfiguration

Bei einer automatischen Installation geben Sie die für das Setupskript erforderlichen Optionen mit Umgebungsvariablen an. Wenn alle erforderlichen Variablen vorhanden sind, werden von dem Skript keine Eingabeaufforderungen für Informationen angezeigt.

Unterstützte Umgebungsvariablen umfassen u. a.:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME** = **Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Standardeinstellung ist N.
- **CTX_XDL_DDC_LIST** = **list-ddc-fqdns** –Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT** = **port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist standardmäßig Port 80.
- **CTX_XDL_REGISTER_SERVICE** = **Y | N** –Die Linux Virtual Desktop-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES** = **Y | N** –Für die Linux Virtual Desktop-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen. Die Standardeinstellung ist Y.

- **CTX_XDL_AD_INTEGRATION** = **1 | 2 | 3 | 4** –Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt. Geben Sie die zu verwendende Active Directory-Integrationsmethode an:
  - 1 –Samba Winbind
  - 2 –Quest-Authentifizierungsdienst
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO** = **Y | N** –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Wenn HDX 3D Pro aktiviert ist, muss der Virtual Delivery Agent für VDI-Desktopmodus (Einzelsitzungen) konfiguriert werden (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE** = **Y | N** –Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Legen Sie dies bei Umgebungen mit HDX 3D Pro auf "Y"fest. Standardmäßig ist diese Variable auf N festgelegt.
- **CTX_XDL_SITE_NAME** = **dns-name** –Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_LDAP_LIST** = **list-ldap-servers** –Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE**= **search-base-set** –Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_START_SERVICE** = **Y | N** –Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Die Standardeinstellung ist Y.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

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



```
export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

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

Sie müssen die Option **-E** mit dem Befehl “sudo”angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Citrix empfiehlt, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y|N \

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


Entfernen von Konfigurationsänderungen

In einigen Fällen müssen die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernt werden, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

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

Entfernen von Konfigurationsänderungen:

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

> **Wichtig:**
>
> Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank, sodass der Linux VDA nicht funktionsfähig ist.

Konfigurationsprotokolle

Die Skripts **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an und schreiben weitere Informationen in die Konfigurationsprotokolldatei **/tmp/xdl.configure.log**.

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

Schritt 7: Ausführen des Linux VDA

Nachdem Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, können Sie den Linux VDA mit den folgenden Befehlen steuern.

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start

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

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

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


Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

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

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status

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

Schritt 8: Erstellen des Maschinenkatalogs in XenApp oder XenDesktop

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt der traditionellen Windows VDA-Methode. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.

Beim Erstellen von Maschinenkatalogen mit Linux VDA-Maschinen gibt es einige Einschränkungen, durch die sich der Prozess von der Maschinenkatalogerstellung für Windows VDA-Maschinen unterscheidet:

- Auswahl des Betriebssystems:
  - Das Serverbetriebssystem für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Das Desktopbetriebssystem für ein VDI-dediziertes Desktopbereitstellungsmodell.
- Stellen Sie sicher, dass für die Maschinen keine Energieverwaltung festgelegt ist.
- Da MCS für Linux VDAs nicht unterstützt wird, wählen Sie die Bereitstellungsmethode PVS oder **Anderer Dienst oder andere Technologie** (vorhandene Images).
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

> **Hinweis:**
>
> In früheren Citrix Studio-Versionen wurde Linux als Betriebssystem nicht unterstützt. Durch die Auswahl von Windows-Serverbetriebssystem oder Serverbetriebssystem wird jedoch ein äquivalentes gehostetes, freigegebenes Desktopbereitstellungsmodell bereitgestellt. Durch

> die Auswahl von Windows-Desktopbetriebssystem oder Desktopbetriebssystem wird ein Bereitstellungsmodell für Einzelbenutzermaschinen bereitgestellt.
>
> **Tipp:**
>
> Wenn Sie eine Maschine aus einer Active Directory-Domäne entfernen und sie ihr dann wieder hinzufügen, muss die Maschine auch aus dem Maschinenkatalog entfernt und ihm dann erneut hinzugefügt werden.

Schritt 9: Erstellen der Bereitstellungsgruppe in XenApp oder XenDesktop

Die Prozesse zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen mit Linux VDA- bzw. Windows VDA-Maschinen sind fast identisch. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Bereitstellungsgruppen.

Beim Erstellen von Bereitstellungsgruppen mit Linux VDA-Maschinenkatalogen gelten die folgenden Einschränkungen:

- Wählen Sie als Bereitstellungstyp “Desktops”oder “Anwendungen”aus.
- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.
- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

> **Wichtig:**
>
> Die Veröffentlichung von Anwendungen wird unter Linux VDA-Version 1.4 und höher unterstützt. Der Linux VDA unterstützt jedoch keine Bereitstellung von Desktops und Anwendungen für dieselbe Maschine.

Installieren von Linux Virtual Delivery Agent für SUSE

February 9, 2024

Mit den Schritten in diesem Artikel können Sie die Installation manuell durchführen, oder verwenden Sie Easy Install für die automatische Installation und Konfiguration. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die manuelle Installation.

> **Hinweis:**

> Verwenden Sie Easy Install bei Neuinstallationen. Zum Aktualisieren von vorhandenen Installationen eignet Easy Install sich nicht.

Schritt 1: Vorbereiten der Installation

Schritt 1a: Starten des YaST-Tools

Mit dem SUSE Linux Enterprise YaST-Tool können alle Aspekte des Betriebssystems konfiguriert werden.

Starten des textbasierten YaST-Tools:

```
su -

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

Sie können auch das YaST-Tool mit Benutzeroberfläche starten:

```
su -

yast2 &
<!--NeedCopy-->
```

Schritt 1b: Konfigurieren des Netzwerks

In den folgenden Abschnitten finden Sie Informationen zum Konfigurieren der verschiedenen Netzwerkeinstellungen und Dienste, die der Linux VDA verwendet. Die Konfiguration des Netzwerks wird mit dem YaST-Tool ausgeführt und nicht mit anderen Methoden wie Network Manager. Die Anleitungen beziehen sich auf das YaST-Tool mit Benutzeroberfläche. Sie können das textbasierte YaST-Tool verwenden, aber es erfordert eine andere Navigationsweise, die hier nicht dokumentiert ist.

Konfigurieren von Hostnamen und DNS

1. Öffnen Sie “YaST Network Settings”.
2. Nur in SLED 12: Ändern Sie auf der Registerkarte **Global Options** die Einstellung unter **Network Setup Method** in **Wicked Service**.
3. Öffnen Sie die Registerkarte **Hostname/DNS**.
4. Deaktivieren Sie das Kontrollkästchen **Change hostname via DHCP**.
5. Aktivieren Sie das Kontrollkästchen **Assign Hostname to Loopback IP**.
6. Geben Sie die folgenden Informationen entsprechend Ihrer Netzwerkeinstellungen an:

    - Host name: Geben Sie den DNS-Hostnamen der Maschine an.
    - Domain Name: Geben Sie den DNS-Domänennamen der Maschine an.

- Name server: Geben Sie die IP-Adresse des DNS-Servers an. Dies ist in der Regel die IP-Adresse des Active Directory-Domänencontrollers.
- Domain Search list: Geben Sie den DNS-Domänennamen an.

> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit nicht das Abschneiden von NetBIOS-Namen. Der Hostname darf daher nicht länger als 15 Zeichen sein.
>
> **Tipp:**
>
> Verwenden Sie nur Buchstaben (a-z oder A-Z), Ziffern (0-9) und Bindestriche (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Hostnamen sollten nicht mit einer Zahl beginnen und nicht mit einem Bindestrich enden. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Deaktivieren von Multicast-DNS In SLED ist standardmäßig Multicast-DNS (mDNS) aktiviert, was zu inkonsistenten Ergebnissen bei der Namensauflösung führen kann. In SLES ist mDNS nicht standardmäßig aktiviert, daher ist keine Aktion erforderlich.

Um mDNS zu deaktivieren, bearbeiten Sie **/etc/nsswitch.conf** und ändern Sie folgende Zeile:

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

In:

```
hosts: files dns
```

Überprüfen des Hostnamens Stellen Sie sicher, dass der Hostname richtig festgelegt ist:

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

Mit diesem Befehl wird nur der Hostname der Maschine und nicht der vollqualifizierte Domänenname (FQDN) zurückgegeben.

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

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

Mit diesem Befehl wird der FQDN der Maschine zurückgegeben.

Überprüfen von Namensauflösung und Diensterreichbarkeit Stellen Sie sicher, dass Sie den FQDN auflösen können und pingen Sie den Domänencontroller und den Delivery Controller:

```
1 nslookup domain-controller-fqdn
2
```



```
ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

Wenn Sie den FQDN nicht auflösen und eine der beiden Maschinen nicht pingen können, überprüfen Sie die vorherigen Schritte, bevor Sie fortfahren.

Schritt 1c: Konfigurieren des NTP-Diensts

Es ist wichtig, dass die Uhrsynchronisierung zwischen den VDAs, den Delivery Controllern und den Domänencontrollern genau ist. Beim Hosten eines Linux VDAs als virtuelle Maschine kann es zu Zeitabweichungen kommen. Aus diesem Grund sollte die Zeit remote von einem NTP-Dienst verwaltet werden. Möglicherweise müssen einige Änderungen an den NTP-Standardeinstellungen vorgenommen werden:

1. Öffnen Sie "YaST NTP Configuration"und wählen Sie die Registerkarte **General Settings**.
2. Aktivieren Sie im Abschnitt "Start NTP Daemon"das Kontrollkästchen **Now and on Boot**.
3. Wählen Sie das Element **Undisciplined Local Clock (LOCAL)** aus, wenn es vorhanden ist, und klicken Sie auf **Delete**.
4. Fügen Sie einen Eintrag für einen NTP-Server hinzu, indem Sie auf **Add** klicken.
5. Wählen Sie unter **Server Type** den Servertyp aus und klicken Sie auf **Next**.
6. Geben Sie den DNS-Namen des NTP-Servers in das Adressfeld ein. Dieser Dienst wird normalerweise auf dem Active Directory-Domänencontroller gehostet.
7. Lassen Sie das Feld "Options"unverändert.
8. Klicken Sie auf **Test**, um zu prüfen, ob der NTP-Dienst erreichbar ist.
9. Klicken Sie in den folgenden Fenstern auf **OK**, um die Änderungen zu speichern.

> **Hinweis:**
>
> Falls der NTP-Daemon in SLES 12-Implementierungen nicht startet, ist dies möglicherweise auf ein bekanntes SUSE-Problem mit AppArmor-Richtlinien zurückzuführen. Weitere Informationen und eine Lösung des Problems finden Sie hier.

Schritt 1d: Installieren von Linux VDA-abhängigen Paketen

Die Linux VDA-Software für SUSE Linux Enterprise ist von den folgenden Paketen abhängig:

- PostgreSQL
  - SLED/SLES 11: Version 9.1 oder höher

  - SLED/SLES 12: Version 9.3 oder höher

- OpenJDK 1.7.0
- OpenMotif Runtime Environment 2.3.1 oder höher
- Cups
  - SLED/SLES 11: Version 1.3.7 oder höher
  - SLED/SLES 12: Version 1.6.0 oder höher
- Foomatic-Filter
  - SLED/SLES 11: Version 3.0.0 oder höher
  - SLED/SLES 12: Version 1.0.0 oder höher
- ImageMagick
  - SLED/SLES 11: Version 6.4.3.6 oder höher
  - SLED/SLES 12: Version 6.8 oder höher

Hinzufügen von Repositorys Einige der erforderlichen Pakete sind nicht in allen SUSE Linux Enterprise-Repositorys verfügbar:

- SLED 11: PostgreSQL ist für SLES 11, aber nicht für SLED 11 verfügbar.
- SLES 11: OpenJDK und OpenMotif sind für SLED 11, aber nicht SLES 11 verfügbar.
- SLED 12: PostgreSQL ist für SLES 12, aber nicht für SLED 12 verfügbar. ImageMagick ist mit dem SLE 12 SDK ISO oder dem Online-Repository verfügbar.
- SLES 12: Es gibt keine Probleme. Alle Pakete sind verfügbar. ImageMagick ist mit dem SLE 12 SDK ISO oder dem Online-Repository verfügbar.

Laden Sie fehlende Pakete für die Edition, die Sie installieren, vom Medium für die alternative SLE-Edition herunter. Das bedeutet, für SLED können Sie fehlende Pakete vom SLES-Medium installieren und für SLES können Sie fehlende Pakete vom SLED-Medium installieren. Mit der folgenden Methode werden die ISO-Dateien und Repositorys sowohl für SLED als auch SLES bereitgestellt.

- Führen Sie für SLED 11 die Befehle aus:

```
sudo mkdir -p /mnt/sles

sudo mount -t iso9660 path-to-iso/SLES-11-SP4-DVD-x86_64-GM-DVD1.iso /
   mnt/sles

sudo zypper ar -f /mnt/sles sles
<!--NeedCopy-->
```

- Führen Sie für SLES 11 die Befehle aus:


```
sudo mkdir -p /mnt/sled

sudo mount -t iso9660 path-to-iso/SLED-11-SP4-DVD-x86_64-GM-DVD1.iso /
   mnt/sled

sudo zypper ar -f /mnt/sled sled
<!--NeedCopy-->
```

- Führen Sie für SLED 12 die Befehle aus:

```
sudo mkdir -p /mnt/sles

sudo mount -t iso9660 path-to-iso/SLES-12-SP2-DVD-x86_64-GM-DVD1.iso /
   mnt/sles

sudo zypper ar -f /mnt/sles sles
<!--NeedCopy-->
```

- Führen Sie für SLED/SLES 12 die Befehle aus:

```
sudo mkdir -p /mnt/sdk

sudo mount -t iso9660 path-to-iso/SLE-12-SP3-SDK-DVD-x86_64-GM-DVD1.iso
    /mnt/sdk

sudo zypper ar -f /mnt/sdk sdk
<!--NeedCopy-->
```

Installieren des Kerberos-Clients Installieren Sie den Kerberos-Client für die gegenseitige Authentifizierung des Linux VDA und der Delivery Controller:

```
sudo zypper install krb5-client
<!--NeedCopy-->
```

Die Kerberos-Clientkonfiguration ist abhängig von der verwendeten Active Directory-Integrationsmethode. Dies wird im Folgenden beschrieben.

Installieren von OpenJDK Der Linux VDA ist von OpenJDK 1.7.0 abhängig.

> **Tipp:**
>
> Stellen Sie zum Vermeiden von Problemen sicher, dass nur die OpenJDK-Version 1.7.0 installiert ist. Entfernen Sie alle anderen Java-Versionen vom System.

- **SLED:**

1. Unter SLED wird Java Runtime Environment normalerweise mit dem Betriebssystem installiert. Überprüfen Sie, ob es installiert ist:


```
sudo zypper info java-1_7_0-openjdk
<!--NeedCopy-->
```

2. Aktualisieren Sie auf die aktuelle Version, wenn der Status als veraltet gemeldet wird:

```
sudo zypper update java-1_7_0-openjdk
<!--NeedCopy-->
```

3. Überprüfen Sie die Java-Version:

```
java -version
<!--NeedCopy-->
```

- **SLES:**

1. Unter SLES muss Java Runtime Environment installiert werden:

```
sudo zypper install java-1_7_0-openjdk
<!--NeedCopy-->
```

2. Überprüfen Sie die Java-Version:

```
java -version
<!--NeedCopy-->
```

Installieren von PostgreSQL

- Installieren Sie für SLED/SLES 11 die Pakete:

```
 sudo zypper install libecpg6

 sudo zypper install postgresql-init

 sudo zypper install postgresql

 sudo zypper install postgresql-server

 sudo zypper install postgresql-jdbc
 <!--NeedCopy-->
```

Nach der Installation sind folgende Schritte erforderlich, um den Datenbankdienst zu initialisieren und zu gewährleisten, dass PostgreSQL beim Systemstart startet:

```
 sudo /sbin/insserv postgresql

 sudo /etc/init.d/postgresql restart
 <!--NeedCopy-->
```

- Installieren Sie für SLED/SLES 12 die Pakete:


```
sudo zypper install postgresql-init

sudo zypper install postgresql-server

sudo zypper install postgresql-jdbc
<!--NeedCopy-->
```

Nach der Installation sind folgende Schritte erforderlich, um den Datenbankdienst zu initialisieren und zu gewährleisten, dass PostgreSQL beim Systemstart startet:

```
sudo systemctl enable postgresql

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

Datenbankdateien finden Sie unter /var/lib/pgsql/data.

Entfernen von Repositorys Nach der Installation der abhängigen Pakete können nun die zuvor eingerichteten Repositorys der alternativen Edition entfernt und die Bereitstellung der Medien aufgehoben werden:

- Führen Sie für SLED 11 die Befehle aus, um die Pakete zu entfernen:

```
sudo zypper rr sles

sudo umount /mnt/sles

sudo rmdir /mnt/sles
<!--NeedCopy-->
```

- Führen Sie für SLES 11 die Befehle aus, um die Pakete zu entfernen:

```
sudo zypper rr sled

sudo umount /mnt/sled

sudo rmdir /mnt/sled
<!--NeedCopy-->
```

- Führen Sie für SLED 12 die Befehle aus, um die Pakete zu entfernen:

```
sudo zypper rr sles

sudo umount /mnt/sles

sudo rmdir /mnt/sles
<!--NeedCopy-->
```

- Führen Sie für SLED/SLES 12 die Befehle aus, um die Pakete zu entfernen:


```
sudo zypper rr sdk

sudo umount /mnt/sdk

sudo rmdir /mnt/sd
<!--NeedCopy-->
```

Schritt 2: Vorbereiten der Linux-VM für den Hypervisor

Wenn Sie den Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausführen, sind einige Änderungen erforderlich. Nehmen Sie entsprechend der verwendeten Hypervisorplattform die folgenden Änderungen vor. Wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen, sind keine Änderungen erforderlich.

Festlegen der Zeitsynchronisierung auf Citrix XenServer

Wenn das Zeitsynchronisierungsfeature auf XenServer aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und XenServer gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeit-synchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen, auf denen ein paravirtualisierter Linux-Kernel mit installierten XenServer Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das XenServer-Zeitsynchronisierungsfeature vorhanden und aktiviert ist:

```
su -



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

Dieser Befehl gibt 0 oder 1 zurück:

- 0: Das Zeitsynchronisierungsfeature ist aktiviert und muss deaktiviert werden.
- 1: Das Zeitsynchronisierungsfeature ist deaktiviert und keine weitere Aktion ist erforderlich.

Wenn die Datei **/proc/sys/xen/indepent_wallclock** nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

Deaktivieren Sie gegebenenfalls das Zeitsynchronisierungsfeature, indem Sie **1** in die Datei schreiben:


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

Damit die Änderung permanent wird und nach dem Neustart erhalten bleibt, fügen Sie in der Datei **/etc/sysctl.conf** die folgende Zeile hinzu:

```
xen.independent_wallclock = 1
```

Starten Sie das System neu, um die Änderungen zu überprüfen:

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

Überprüfen Sie nach dem Neustart, ob die Einstellung korrekt ist:

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

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

Linux-VMs, auf denen Hyper-V Linux-Integrationsdienste installiert sind, können mit dem Hyper-V-Zeitsynchronisierungsfeature die Systemzeit des Hostbetriebssystems verwenden. Aktivieren Sie das Feature zusätzlich zu den NTP-Diensten, um sicherzustellen, dass die Betriebssystemzeit korrekt ist.

Auf dem verwaltenden Betriebssystem:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Wählen Sie für die Einstellungen einer Linux-VM **Integration Services** aus.
3. Stellen Sie sicher, dass **Time synchronization** ausgewählt ist.

> **Hinweis:**
>
> Diese Methode unterscheidet sich von VMware und XenServer, wo die Hostzeitsynchronisierung deaktiviert ist, um Konflikte mit dem NTP zu vermeiden. Hyper-V-Zeitsynchronisierung kann gleichzeitig mit der NTP-Zeitsynchronisierung bestehen und sie ergänzen.

Festlegen der Zeitsynchronisierung auf ESX und ESXi

Wenn das VMware-Zeitsynchronisierungsfeature aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und der Hypervisor gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel ausführen und VMware-Tools installiert sind:

1. Öffnen Sie den vSphere-Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Virtual Machine Properties** die Registerkarte **Options**.
4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Advanced** das Kontrollkästchen **Synchronize guest time with host**.

Schritt 3: Hinzufügen der virtuellen Linux-Maschine zur Windows-Domäne

Der Linux VDA unterstützt mehrere Methoden zum Hinzufügen von Linux-Maschinen zur Active Directory-Domäne:

- Samba Winbind
- Quest Authentication Service
- Centrify DirectControl

Folgen Sie den Anweisungen für die von Ihnen gewählte Methode.

Samba Winbind

Windows-Domäne beitreten Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Maschinen zur Domäne verfügen:

1. Öffnen Sie "YaST Windows Domain Membership".
2. Nehmen Sie die folgenden Änderungen vor:
    - Legen Sie die **Domäne oder Arbeitsgruppe** auf den Namen der Active Directory-Domäne oder auf die IP-Adresse des Domänencontrollers fest. Stellen Sie sicher, dass der Domänenname in Großbuchstaben angegeben wurde.
    - Aktivieren Sie **Also Use SMB information for Linux Authentication**.
    - Aktivieren Sie **Create Home Directory on Login**.
    - Aktivieren Sie **Single Sign-on for SSH**.
    - Stellen Sie sicher, dass die Option **Offline Authentication** nicht aktiviert ist. Diese Option ist mit dem Linux VDA nicht kompatibel.
3. Klicken Sie auf **OK**. Wenn Sie zum Installieren einiger Pakete aufgefordert werden, klicken Sie auf **Install**.
4. Wenn ein Domänencontroller gefunden wird, werden Sie gefragt, ob Sie der Domäne beitreten möchten. Klicken Sie auf **Ja**.

5. Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen eines Domänenbenutzers ein, der über Berechtigungen zum Hinzufügen von Computern zur Domäne verfügt, und klicken Sie auf **OK**.
6. Eine Erfolgsmeldung wird angezeigt.
7. Wenn Sie zum Installieren von samba- und krb5-Paketen aufgefordert werden, klicken Sie auf **Install**.

YaST hat Sie möglicherweise davon unterrichtet, dass für diese Änderungen einige Dienste oder die Maschine neu gestartet werden müssen. Wir empfehlen Ihnen, den Computer neu zu starten:

```
su -

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

Nur SLED/SLES 12: Patch für Cachenamen für Kerberos-Anmeldeinformationen SLED/SLES 12 hat die standardmäßige Kerberos-Cachenamenspezifikation für Kerberos-Anmeldeinformationen von **FILE:/tmp/krb5cc_%{uid}** in **DIR:/run/user/%{uid}/krb5cc** geändert. Diese neue DIR-Zwischenspeichermethode ist nicht mit dem Linux VDA kompatibel und muss manuell geändert werden. Bearbeiten Sie als Root-Benutzer die Datei **/etc/krb5.conf** und fügen Sie die folgende Einstellung im Abschnitt **[libdefaults]** hinzu, falls sie nicht festgelegt ist:

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

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux VDAs) ein Computerobjekt in Active Directory haben.

Führen Sie den Samba-Befehl **net ads** aus, um zu prüfen, ob die Maschine zu einer Domäne gehört:

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

Führen Sie den folgenden Befehl aus, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen:

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

Kerberos-Konfiguration überprüfen Um sicherzustellen, dass Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, überprüfen Sie, ob die Systemdatei für die Schlüsseltabelle erstellt wurde und gültige Schlüssel enthält:


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

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller mit diesen Schlüsseln zu authentifizieren:

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

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

Benutzerauthentifizierung überprüfen Überprüfen Sie mit dem `wbinfo`-Tool, dass Domänenbenutzer sich bei der Domäne authentifizieren können:

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

Die hier angegebene Domäne ist der AD-Domänenname und nicht der Kerberos-Bereichsname. Für die Bash-Shell muss der umgekehrte Schrägstrich (\) durch einen weiteren umgekehrten Schrägstrich geschützt werden. Bei diesem Befehl wird eine Erfolgs- oder Fehlermeldung zurückgegeben.

Um sich zu vergewissern, dass das Winbind-PAM-Modul fehlerfrei konfiguriert ist, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
ssh localhost -l domain\username

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


Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

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

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

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

Sitzung beenden

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

Quest Authentication Service

Quest auf dem Domänencontroller konfigurieren Es wird vorausgesetzt, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und über Administratorrechte zum Erstellen von Computerobjekten in Active Directory verfügen.

Domänenbenutzern die Anmeldung an Linux VDA-Maschinen ermöglichen Führen Sie folgende Schritte aus, damit Domänenbenutzer HDX-Sitzungen auf einer Linux VDA-Maschine herstellen können:

1. Öffnen Sie in der Verwaltungskonsole für Active Directory-Benutzer und -Computer die Active Directory-Eigenschaften für das jeweilige Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix Account** aus.
3. Aktivieren Sie das Kontrollkästchen **Unix-enabled**.
4. Legen Sie **Primary GID Number** auf die Gruppen-ID einer vorhandenen Domänenbenutzergruppe fest.

> **Hinweis:**
>
> Mit diesen Anleitungen können Domänenbenutzer für die Anmeldung mit der Konsole, RDP, SSH oder anderen Remotingprotokollen eingerichtet werden.

Quest auf Linux VDA konfigurieren

VAS-Daemon konfigurieren Die automatische Erneuerung von Kerberos-Tickets muss aktiviert und getrennt sein. Authentifizierung (für Offlineanmeldung) muss deaktiviert sein.

```
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-->
```

Mit diesem Befehl wird das Verlängerungsintervall auf neun Stunden (32.400 Sekunden) festgelegt. Das ist eine Stunde weniger als die Standardgültigkeitsdauer (10 Stunden) eines Tickets. Bei Systemen mit einer kürzeren Ticketgültigkeitsdauer legen Sie diesen Parameter auf einen niedrigeren Wert fest.

PAM und NSS konfigurieren Um die Domänenbenutzeranmeldung über HDX und andere Dienste wie su, ssh und RDP zu aktivieren, führen Sie die folgenden Befehle aus, um PAM und NSS manuell zu konfigurieren:

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

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

Windows-Domäne beitreten Machen Sie die Linux-Maschine mit dem Quest-Befehl `vastool` zu einem Mitglied der Active Directory-Domäne:

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

user ist ein beliebiger Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern der Active Directory-Domäne zu machen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux VDAs) ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Quest angemeldete Linux-Maschine zur Domäne gehört:

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

Wenn die Maschine zu einer Domäne gehört, wird mit diesem Befehl der Domänenname zurückgegeben. Wenn die Maschine zu keiner Domäne gehört, wird die folgende Fehlermeldung angezeigt:


```
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
```

Benutzerauthentifizierung überprüfen Um sicherzustellen, dass Quest Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
ssh localhost -l domain\username

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

Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

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

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

Centrify DirectControl

Windows-Domäne beitreten Wenn der Centrify DirectControl Agent installiert ist, machen Sie die Linux-Maschine mit dem Centrify-Befehl **adjoin** zu einem Mitglied der Active Directory-Domäne:

```
su -

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


user ist ein beliebiger Active Directory-Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern der Active Directory-Domäne zu machen. **domain-name** ist der Name der Domäne, der die Linux-Maschine beitritt.

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux VDAs) ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Centrify hinzugefügte Linux-Maschine Mitglied der Domäne ist:

```
su -

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

Stellen Sie sicher, dass der Wert **Joined to domain** gültig ist und dass **CentrifyDC mode** den Wert **connected** zurückgibt. Wenn der Modus im Startzustand stecken bleibt, hat der Centrify-Client Serververbindungs- oder Authentifizierungsprobleme.

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all

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

Testen Sie die Verbindung mit den verschiedenen Active Directory- und Kerberos-Diensten.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

Schritt 4: Installieren des Linux VDA

Schritt 4a: Deinstallieren der alten Version

Wenn eine Version installiert ist, die älter ist als die beiden vorigen Versionen und keine LTSR-Version ist, deinstallieren Sie diese Version, bevor Sie die neue Version installieren.

1. Halten Sie die Linux VDA-Dienste an:

   ```
   sudo /sbin/service ctxvda stop

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

2. Deinstallieren Sie das Paket:


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

> **Wichtig:**
>
> Upgrades von den letzten zwei Versionen werden unterstützt.
>
> **Hinweis:**
>
> Die Installationskomponenten befinden sich in **/opt/Citrix/VDA/**.
>
> Zum Ausführen eines Befehls ist der vollständige Pfad erforderlich. Alternativ können Sie dem Systempfad **/opt/Citrix/VDA/sbin** und **/opt/Citrix/VDA/bin** hinzufügen.

Schritt 4b: Herunterladen des Linux VDA-Pakets

Rufen Sie die Citrix-Website auf und laden Sie das entsprechende Linux VDA-Paket herunter, je nach Linux-Distribution.

Schritt 4c: Installieren des Linux VDA

Installieren der Linux VDA-Software mit Zypper:

SUSE 12:

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
<!--NeedCopy-->
```

SUSE 11:

```
sudo zypper install XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

Installieren Sie die Linux VDA-Software mit dem RPM-Paketmanager. Vorher müssen folgende Abhängigkeiten aufgelöst werden:

SUSE 12:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
<!--NeedCopy-->
```

SUSE 11:

```
sudo rpm -i XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```


Schritt 4d: Upgrade des Linux VDA (optional)

Sie können die Versionen 7.14 und 7.13 der Linux VDA-Software mit RPM Package Manager aktualisieren:

SUSE 12:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle12_2.x86_64.rpm
<!--NeedCopy-->
```

SUSE 11:

```
sudo rpm -U XenDesktopVDA-7.15.0.404-1.sle11_4.x86_64.rpm
<!--NeedCopy-->
```

RPM-Abhängigkeitsliste für SUSE 12:

```
postgresql-server >= 9.3

postgresql-jdbc >= 9.2

java-1.7.0-openjdk >= 1.7.0

ImageMagick >= 6.8

dbus-1 >= 1.8.8

dbus-1-x11 >= 1.8.8

libXpm4 >= 3.5.11

libXrandr2 >= 1.4.2

libXtst6 >= 1.2.2

motif >= 2.3

pam >= 1.1.8

bash >= 4.2

findutils >= 4.5

gawk >= 4.1

sed >= 4.2

cups >= 1.6.0

cups-filters-foomatic-rip >= 1.0.0

openldap2 >= 2.4

```



```
cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

python-requests >= 2.8.1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsLzma) <= 4.4.6-1
<!--NeedCopy-->
```

RPM-Abhängigkeitsliste für SUSE 11:

```
postgresql-server >= 9.1.

postgresql-jdbc >= 9.1

java-1_7_0-openjdk >= 1.7.0.6

ImageMagick >= 6.4.3.6

ConsoleKit >= 0.2.10

dbus-1 >= 1.2.10

dbus-1-x11 >= 1.2.10

xorg-x11-libXpm >= 7.4

xorg-x11-libs >= 7.4

openmotif-libs >= 2.3.1

pam >= 1.1.5

libdrm >= 2.4.41

libpixman-1-0 >= 0.24.4

Mesa >= 9.0

openssl >= 0.9.8j

xorg-x11 >= 7.4

xorg-x11-fonts-core >= 7.4

xorg-x11-libXau >= 7.4

```



```
xorg-x11-libXdmcp >= 7.4

bash >= 3.2

findutils >= 4.4

gawk >= 3.1

sed >= 4.1

cups >= 1.3.7

foomatic-filters >= 3.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.7

python-requests >= 2.0.1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsLzma) <= 4.4.6-1
<!--NeedCopy-->
```

> **Wichtig:**
>
> Starten Sie die Linux VDA-Maschine nach dem Upgrade neu.

Schritt 5: Konfigurieren des Linux VDA

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Das Skript überprüft die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Führen Sie Änderungen erst danach durch. Sie können das Skript nach Bedarf jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell unter Reaktion auf Aufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript durch, bevor Sie fortfahren:

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


Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

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

Automatische Konfiguration

Bei einer automatischen Installation geben Sie die für das Setupskript erforderlichen Optionen mit Umgebungsvariablen an. Wenn alle erforderlichen Variablen vorhanden sind, werden von dem Skript keine Eingabeaufforderungen für Informationen angezeigt.

Unterstützte Umgebungsvariablen umfassen u. a.:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Standardeinstellung ist N.
- **CTX_XDL_DDC_LIST = list-ddc-fqdns** –Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT = port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist standardmäßig Port 80.
- **CTX_XDL_REGISTER_SERVICE = Y | N** –Die Linux Virtual Desktop-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES = Y | N** –Für die Linux Virtual Desktop-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION = 1 | 2 | 3 | 4** –Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt. Geben Sie die zu verwendende Active Directory-Integrationsmethode an:
  - 1 –Samba Winbind
  - 2 –Quest-Authentifizierungsdienst
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO = Y | N** –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Wenn HDX 3D Pro aktiviert ist, muss der Virtual Delivery Agent für VDI-Desktopmodus (Einzelsitzungen) konfiguriert werden (d. h. CTX_XDL_VDI_MODE=Y).

- **CTX_XDL_VDI_MODE = Y | N** –Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Legen Sie dies bei Umgebungen mit HDX 3D Pro auf "Y"fest. Standardmäßig ist diese Variable auf N festgelegt.
- **CTX_XDL_SITE_NAME = dns-name** –Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_LDAP_LIST = list-ldap-servers** –Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE = search-base-set** –Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_START_SERVICE = Y | N** –Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Die Standardeinstellung ist Y.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

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

Sie müssen die Option **-E** mit dem Befehl "sudo"angeben, damit die vorhandenen Umgebungsvari-

ablen an die neu erstellte Shell weitergegeben werden. Citrix empfiehlt, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y|N \

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

Entfernen von Konfigurationsänderungen

In einigen Fällen müssen die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernt werden, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

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

Entfernen von Konfigurationsänderungen:

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

> **Wichtig:**
>
> Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank, sodass der Linux VDA nicht

> funktionsfähig ist.

Konfigurationsprotokolle

Die Skripts **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an und schreiben weitere Informationen in eine Konfigurationsprotokolldatei:

`/tmp/xdl.configure.log`

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

Schritt 6: Ausführen des Linux VDA

Nachdem Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, können Sie den Linux VDA mit den folgenden Befehlen steuern.

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start

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

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

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

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

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

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:


```
sudo /sbin/service ctxvda status

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

Schritt 7: Erstellen des Maschinenkatalogs in XenApp oder XenDesktop

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt der traditionellen Windows VDA-Methode. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.

Beim Erstellen von Maschinenkatalogen mit Linux VDA-Maschinen gibt es einige Einschränkungen, durch die sich der Prozess von der Maschinenkatalogerstellung für Windows VDA-Maschinen unterscheidet:

- Auswahl des Betriebssystems:
  - Das Serverbetriebssystem für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Das Desktopbetriebssystem für ein VDI-dediziertes Desktopbereitstellungsmodell.
- Stellen Sie sicher, dass für die Maschinen keine Energieverwaltung festgelegt ist.
- Da MCS für Linux VDAs nicht unterstützt wird, wählen Sie die Bereitstellungsmethode PVS oder **Anderer Dienst oder andere Technologie** (vorhandene Images).
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

> **Hinweis:**
>
> In früheren Citrix Studio-Versionen wurde Linux als Betriebssystem nicht unterstützt. Durch die Auswahl von Windows-Serverbetriebssystem oder Serverbetriebssystem wird jedoch ein äquivalentes gehostetes, freigegebenes Desktopbereitstellungsmodell bereitgestellt. Durch die Auswahl von Windows-Desktopbetriebssystem oder Desktopbetriebssystem wird ein Bereitstellungsmodell für Einzelbenutzermaschinen bereitgestellt.
>
> **Tipp:**
>
> Wenn Sie eine Maschine aus einer Active Directory-Domäne entfernen und sie ihr dann wieder hinzufügen, muss die Maschine auch aus dem Maschinenkatalog entfernt und ihm dann erneut hinzugefügt werden.

Schritt 8: Erstellen der Bereitstellungsgruppe in XenApp oder XenDesktop

Die Prozesse zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen mit Linux VDA- bzw. Windows VDA-Maschinen sind fast identisch. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Bereitstellungsgruppen.

Beim Erstellen von Bereitstellungsgruppen mit Linux VDA-Maschinenkatalogen gelten die folgenden Einschränkungen:

- Wählen Sie als Bereitstellungstyp "Desktops"oder "Anwendungen"aus.
- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.
- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

> **Wichtig:**
>
> Die Veröffentlichung von Anwendungen wird unter Linux VDA-Version 1.4 und höher unterstützt. Der Linux VDA unterstützt jedoch keine Bereitstellung von Desktops und Anwendungen für dieselbe Maschine.

Installieren von Linux Virtual Delivery Agent für Ubuntu

June 16, 2022

Mit den Schritten in diesem Artikel können Sie die Installation manuell durchführen, oder verwenden Sie Easy Install für die automatische Installation und Konfiguration. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die manuelle Installation.

> **Hinweis:**
>
> Verwenden Sie Easy Install bei Neuinstallationen. Zum Aktualisieren von vorhandenen Installationen eignet Easy Install sich nicht.

Schritt 1: Vorbereiten von Ubuntu für die VDA-Installation

Schritt 1a: Überprüfen der Netzwerkkonfiguration

Stellen Sie sicher, dass das Netzwerk verbunden und richtig konfiguriert ist, bevor Sie fortfahren.

Schritt 1b: Festlegen des Hostnamens

Damit der Hostname der Maschine richtig gemeldet wird, ändern Sie die Datei **/etc/hostname**, sodass sie nur den Hostnamen der Maschine enthält.

```
hostname
```

Schritt 1c: Zuweisen einer Loopbackadresse für den Hostnamen

Damit der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine richtig gemeldet werden, ändern Sie die folgende Zeile in der Datei **/etc/hosts**, sodass der FQDN und der Hostname die ersten zwei Einträge sind:

```
127.0.0.1 hostname-fqdn hostname localhost
```

Beispiel:

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

Entfernen Sie alle anderen Verweise auf **hostname-fqdn** oder **hostname** aus anderen Einträgen in der Datei.

> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit nicht das Abschneiden von NetBIOS-Namen. Der Name darf daher nicht länger als 15 Zeichen sein.
>
> **Tipp:**
>
> Verwenden Sie nur Buchstaben (a-z oder A-Z), Ziffern (0-9) und Bindestriche (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Hostnamen sollten nicht mit einer Zahl beginnen und nicht mit einem Bindestrich enden. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Schritt 1d: Überprüfen des Hostnamens

Stellen Sie sicher, dass der Hostname richtig festgelegt ist:

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

Dieser Befehl gibt nur den Hostnamen der Maschine zurück und nicht den vollqualifizierten Domänennamen (FQDN).

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

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


Dieser Befehl gibt den FQDN der Maschine zurück.

Schritt 1e: Deaktivieren von Multicast-DNS

In den Standardeinstellungen ist Multicast-DNS (**mDNS**) aktiviert, was zu inkonsistenten Ergebnissen bei der Namensauflösung führen kann.

Um **mDNS** zu deaktivieren, bearbeiten Sie **/etc/nsswitch.conf** und ändern die Zeile:

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

In:

```
hosts: files dns
```

Schritt 1f: Überprüfen von Namensauflösung und Diensterreichbarkeit

Stellen Sie sicher, dass Sie den FQDN auflösen können und pingen Sie den Domänencontroller und den Delivery Controller:

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

Wenn Sie den FQDN nicht auflösen und eine der beiden Maschinen nicht pingen können, überprüfen Sie die vorherigen Schritte, bevor Sie fortfahren.

Schritt 1g: Konfigurieren der Uhrsynchronisierung (Chrony)

Es ist wichtig, dass die Uhrsynchronisierung zwischen den VDAs, den Delivery Controllern und den Domänencontrollern genau ist. Beim Hosten eines Linux VDAs als virtuelle Maschine kann es zu Zeitabweichungen kommen. Aus diesem Grund sollte die Zeit remote von einem Zeitdienst synchronisiert werden.

Installieren Sie chrony:

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

Bearbeiten Sie als Root-Benutzer die Datei **/etc/chrony/chrony.conf** und fügen Sie pro Remote-Zeitserver einen Servereintrag hinzu:


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

In einer typischen Bereitstellung synchronisieren Sie die Zeit von den lokalen Domänencontrollern und nicht direkt von öffentlichen NTP-Poolservern. Fügen Sie pro Active Directory-Domänencontroller in der Domäne einen Servereintrag hinzu.

Entfernen Sie alle **server**- oder **pool**-Einträge, , einschließlich Einträge für Loopback-IP-Adressen, Localhost und öffentliche Servereinträge wie ***.pool.ntp.org**.

Speichern Sie die Änderungen und starten Sie den Chrony-Daemon neu:

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

Schritt 1h: Installieren von OpenJDK

Der Linux VDA ist von OpenJDK abhängig. Üblicherweise wird die Laufzeitumgebung als Teil der Betriebssysteminstallation installiert. Überprüfen Sie, ob es installiert ist:

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

Schritt 1i: Installieren von PostgreSQL

Der Linux VDA erfordert PostgreSQL 9.x unter Ubuntu 16.04:

```
sudo apt-get install -y postgresql

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

Schritt 1j: Installieren von Motif

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

Schritt 1k: Installieren weiterer Pakete

```
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
```



```
6
7  sudo apt-get install -y krb5-user
8
9  sudo apt-get install -y cups
10 <!--NeedCopy-->
```

Schritt 2: Vorbereiten des Hypervisors

Wenn Sie den Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausführen, sind einige Änderungen erforderlich. Nehmen Sie entsprechend der verwendeten Hypervisorplattform die folgenden Änderungen vor. Wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen, sind keine Änderungen erforderlich.

Festlegen der Zeitsynchronisierung auf Citrix XenServer

Wenn das Zeitsynchronisierungsfeature auf XenServer aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und XenServer gleichzeitig versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeit-synchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen, auf denen ein paravirtualisierter Linux-Kernel mit installierten XenServer Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das XenServer-Zeitsynchronisierungsfeature vorhanden und aktiviert ist:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--NeedCopy-->
```

Dieser Befehl gibt 0 oder 1 zurück:

- 0: Das Zeitsynchronisierungsfeature ist aktiviert und muss deaktiviert werden.
- 1: Das Zeitsynchronisierungsfeature ist deaktiviert und keine weitere Aktion ist erforderlich.

Wenn die Datei /proc/sys/xen/indepent_wallclock nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

Wenn das Zeitsynchronisierungsfeature aktiviert ist, deaktivieren Sie es, indem Sie 1 in die Datei eingeben:

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


Damit die Änderung permanent wird und nach dem Neustart erhalten bleibt, fügen Sie in der Datei **/etc/sysctl.conf** die folgende Zeile hinzu:

```
xen.independent_wallclock = 1
```

Starten Sie das System neu, um die Änderungen zu überprüfen:

```
su -

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

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

Linux-VMs, auf denen Hyper-V Linux-Integrationsdienste installiert sind, können mit dem Hyper-V-Zeitsynchronisierungsfeature die Systemzeit des Hostbetriebssystems verwenden. Um sicherzustellen, dass die Betriebssystemzeit korrekt ist, muss das Feature zusätzlich zu den NTP-Diensten aktiviert sein.

Auf dem verwaltenden Betriebssystem:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Wählen Sie für die Einstellungen einer Linux-VM **Integration Services** aus.
3. Stellen Sie sicher, dass **Time synchronization** ausgewählt ist.

> **Hinweis:**
>
> Diese Methode unterscheidet sich von VMware und XenServer, wo die Hostzeitsynchronisierung deaktiviert ist, um Konflikte mit dem NTP zu vermeiden. Hyper-V-Zeitsynchronisierung kann gleichzeitig mit der NTP-Zeitsynchronisierung bestehen und sie ergänzen.

Festlegen der Zeitsynchronisierung auf ESX und ESXi

Wenn das VMware-Zeitsynchronisierungsfeature aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme auf, da NTP und der Hypervisor gleichzeitig versuchen, die Systemuhr zu synchronisieren. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel ausführen und VMware-Tools installiert sind:

1. Öffnen Sie den vSphere-Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.

3. Öffnen Sie im Dialogfeld **Virtual Machine Properties** die Registerkarte **Options**.
4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Advanced** das Kontrollkästchen **Synchronize guest time with host**.

Schritt 3: Hinzufügen der virtuellen Linux-Maschine zur Windows-Domäne

Der Linux VDA unterstützt mehrere Methoden zum Hinzufügen von Linux-Maschinen zur Active Directory-Domäne:

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

Folgen Sie den Anweisungen für die von Ihnen gewählte Methode.

Samba Winbind

Installieren oder aktualisieren Sie die erforderlichen Pakete

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

Starten des Winbind-Daemon beim Booten Der Winbind-Daemon muss beim Systemstart gestartet werden:

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

Konfigurieren von Kerberos Öffnen Sie als Root-Benutzer `/etc/krb5.conf` und nehmen Sie folgende Einstellungen vor:

```
[libdefaults]

default_realm = REALM

dns_lookup_kdc = false



[realms]

REALM = {


```



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

Die Eigenschaft **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. **example.com**. **REALM** ist der Kerberos-Bereichsname in Großbuchstaben, z. B. **EXAMPLE.COM**.

Konfigurieren der Winbind-Authentifizierung Führen Sie eine manuelle Konfiguration durch, denn Ubuntu verfügt nicht über Tools wie `authconfig` in RHEL und yast2 in SUSE.

Öffnen Sie `/etc/samba/smb.conf` und nehmen Sie folgende Einstellungen vor:

```
1  [global]
2
3  workgroup = WORKGROUP
4
5  security = ADS
6
7  realm = REALM
8
9  encrypt passwords = yes
10
11 idmap config *:range = 16777216-33554431
12
13 winbind trusted domains only = no
14
15 kerberos method = secrets and keytab
16
17 winbind refresh tickets = yes
18
19 template shell = /bin/bash
20 <!--NeedCopy-->
```

WORKGROUP ist das erste Feld in **REALM** und REALM ist der Kerberos-Bereichsname in Großbuchstaben.

Konfigurieren von nsswitch Öffnen Sie `/etc/nsswitch.conf` und fügen Sie `winbind` in den folgenden Zeilen hinzu:


```
passwd: compat winbind
group: compat winbind
```

Beitreten zu einer Windows-Domäne Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

Neustarten von winbind

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

Konfigurieren von PAM für Winbind Führen Sie den folgenden Befehl aus. Stellen Sie sicher, dass die Optionen **Winbind NT/Active Directory authentication** und **Create home directory on login** aktiviert sind:

```
sudo pam-auth-update
<!--NeedCopy-->
```

> **Tipp:**
>
> Der Winbind-Daemon wird nur weiterhin ausgeführt, wenn die Maschine zu einer Domäne gehört.

Überprüfen der Domäneneigentümerschaft Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben.

Führen Sie den Samba-Befehl `net ads` aus, um zu prüfen, ob die Maschine zu einer Domäne gehört:

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

Führen Sie den folgenden Befehl aus, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen:

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


Überprüfen der Kerberos-Konfiguration Überprüfen Sie, ob Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, indem Sie sicherstellen, dass die Systemdatei für die **Schlüsseltabelle** erstellt wurde und gültige Schlüssel enthält:

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

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller mit diesen Schlüsseln zu authentifizieren:

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

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

Überprüfen der Benutzerauthentifizierung Überprüfen Sie mit dem **wbinfo**-Tool, dass Domänenbenutzer sich bei der Domäne authentifizieren können:

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

Die hier angegebene Domäne ist der AD-Domänenname und nicht der Kerberos-Bereichsname. Für die Bash-Shell muss der umgekehrte Schrägstrich (\) durch einen weiteren umgekehrten Schrägstrich geschützt werden. Bei diesem Befehl wird eine Erfolgs- oder Fehlermeldung zurückgegeben.

Um sich zu vergewissern, dass das Winbind-PAM-Modul fehlerfrei konfiguriert ist, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

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



```
2
3 id -u
4 <!--NeedCopy-->
```

Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

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

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

> **Tipp:**
>
> Wenn die Benutzerauthentifizierung erfolgreich ist, aber der Desktop nach der Anmeldung mit einem Domänenkonto nicht angezeigt wird, starten Sie die Maschine neu und wiederholen Sie die Anmeldung.

Quest Authentication Service

Konfigurieren von Quest auf dem Domänencontroller Es wird vorausgesetzt, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und über Administratorrechte zum Erstellen von Computerobjekten in Active Directory verfügen.

Domänenbenutzern die Anmeldung an Linux VDA-Maschinen ermöglichen Führen Sie folgende Schritte aus, damit Domänenbenutzer HDX-Sitzungen auf einer Linux VDA-Maschine herstellen können:

1. Öffnen Sie in der Verwaltungskonsole für Active Directory-Benutzer und -Computer die Active Directory-Eigenschaften für das jeweilige Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix Account** aus.
3. Aktivieren Sie das Kontrollkästchen **Unix-enabled**.

4. Legen Sie **Primary GID Number** auf die Gruppen-ID einer vorhandenen Domänenbenutzergruppe fest.

> **Hinweis:**
>
> Mit diesen Anleitungen können Domänenbenutzer für die Anmeldung mit der Konsole, RDP, SSH oder anderen Remotingprotokollen eingerichtet werden.

Konfigurieren von Quest auf Linux VDA

Workaround bei SELinux-Richtlinienerzwingung In der RHEL-Standardumgebung wird SELinux vollständig erzwungen. Das beeinträchtigt die von Quest verwendeten IPC-Methoden der Unix-Domänensockets und verhindert, dass Domänenbenutzer sich anmelden.

Der bequeme Weg, dieses Problem zu umgehen, ist die Deaktivierung von SELinux. Bearbeiten Sie als Root-Benutzer die Datei **/etc/selinux/config** und ändern Sie die **SELinux**-Einstellung:

```
SELINUX=disabled
```

Diese Änderung erfordert einen Neustart der Maschine:

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

> **Wichtig:**
>
> Seien Sie vorsichtig beim Verwenden dieser Einstellung. Das erneute Aktivieren der SELinux-Richtlinienerzwingung nach ihrer Deaktivierung kann selbst für den Root-Benutzer und anderen lokale Benutzer zu einer vollständigen Sperrung führen.

Konfigurieren eines VAS-Daemons Die automatische Erneuerung von Kerberos-Tickets muss aktiviert und getrennt sein. Authentifizierung (für Offlineanmeldung) muss deaktiviert sein.

```
1 sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-
     interval 32400
2
3 sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
     auth false
4 <!--NeedCopy-->
```

Mit diesem Befehl wird das Verlängerungsintervall auf neun Stunden (32.400 Sekunden) festgelegt. Das ist eine Stunde weniger als die Standardgültigkeitsdauer (10 Stunden) eines Tickets. Bei Systemen mit einer kürzeren Ticketgültigkeitsdauer legen Sie diesen Parameter auf einen niedrigeren Wert fest.

Konfigurieren von PAM und NSS Um die Domänenbenutzeranmeldung über HDX und andere Dienste wie su, ssh und RDP zu aktivieren, führen Sie die folgenden Befehle aus, um PAM und NSS manuell zu konfigurieren:

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

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

Beitreten zu einer Windows-Domäne Machen Sie die Linux-Maschine mit dem Quest-Befehl `vastool` zu einem Mitglied der Active Directory-Domäne:

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

Der Benutzer ist ein beliebiger Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern der Active Directory-Domäne zu machen. domain-name ist der DNS-Name der Domäne, z. B. example.com.

Überprüfen der Domäneneigentümerschaft Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Quest angemeldete Linux-Maschine zur Domäne gehört:

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

Wenn die Maschine zu einer Domäne gehört, wird mit diesem Befehl der Domänenname zurückgegeben. Wenn die Maschine zu keiner Domäne gehört, wird die folgende Fehlermeldung angezeigt:

```
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
```

Überprüfen der Benutzerauthentifizierung Um sicherzustellen, dass Quest Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
ssh localhost -l domain\username

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


Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

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

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

Centrify DirectControl

Beitreten zu einer Windows-Domäne Wenn der Centrify DirectControl Agent installiert ist, machen Sie die Linux-Maschine mit dem Centrify-Befehl `adjoin` zu einem Mitglied der Active Directory-Domäne:

```
su -

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

Der Parameter **user** ist ein Active Directory-Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern von Active Directory-Domänen zu machen. Der Parameter **domain-name** ist der Name der Domäne, der die Linux-Maschine beitritt.

Überprüfen der Domäneneigentümerschaft Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Centrify hinzugefügte Linux-Maschine Mitglied der Domäne ist:

```
su -

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

Stellen Sie sicher, dass der Wert **Joined to domain** gültig ist und dass **CentrifyDC mode** den Wert **connected** zurückgibt. Wenn der Modus im Startzustand stecken bleibt, hat der Centrify-Client Serververbindungs- oder Authentifizierungsprobleme.

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all

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

Testen Sie die Verbindung mit den verschiedenen Active Directory- und Kerberos-Diensten.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

SSSD

Konfigurieren von Kerberos Führen Sie zum Installieren von Kerberos den folgenden Befehl aus:

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

Zum Konfigurieren von Kerberos öffnen Sie als Root-Benutzer `/etc/krb5.conf` und nehmen folgende Einstellungen vor:

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


Die Eigenschaft `domain-dns-name` ist in diesem Kontext der DNS-Domänenname, z. B. `example.com`. `REALM` ist der Kerberos-Bereichsname in Großbuchstaben, z. B. `EXAMPLE.COM`.

Beitreten zu einer Domäne SSSD muss für die Verwendung von Active Directory als Identitätsanbieter und Kerberos zur Authentifizierung konfiguriert werden. SSSD bietet keine AD-Clientfunktionen für den Domänenbeitritt und die Verwaltung der Systemschlüsseltabelle. Sie können stattdessen `adcli`, `realmd`, oder `Samba` verwenden.

> **Hinweis:**
>
> Dieser Abschnitt enthält nur Informationen zu `adcli` und `Samba`.

Verwenden Sie adcli für den Beitritt zur Domäne:

Installieren Sie adcli:

Installieren Sie das erforderliche Paket:

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

Domänenbeitritt mit adcli:

Entfernen Sie die alte Systemdatei für die Schlüsseltabelle und treten Sie der Domäne mit folgenden Befehl bei:

```
su -

rm -rf /etc/krb5.keytab

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

user ist ein Domänenbenutzer mit der Berechtigung zum Hinzufügen von Maschinen zur Domäne. **hostname-fqdn** ist der Hostname für die Maschine im FQDN-Format.

Die Option **-H** ist erforderlich, damit adcli SPN im folgenden, vom Linux VDA benötigten Format erstellen kann: host/hostname-fqdn@REALM.

Überprüfen der Systemschlüsseltabelle:

Die Möglichkeiten des **adcli**-Tools sind begrenzt und bieten keine Möglichkeit zu testen, ob eine Maschine mit der Domäne verbunden ist. Führen Sie als Alternative folgenden Befehl aus, um sicherzustellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde:

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

Prüfen Sie, ob die Zeitstempel der einzelnen Schlüssel mit der Zeit übereinstimmen, zu der der Domänenbeitritt der Maschine erfolgte.

Verwenden von samba für den Domänenbeitritt:

Installieren Sie das Paket:

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

Konfigurieren Sie samba:

Öffnen Sie `/etc/samba/smb.conf` und nehmen Sie folgende Einstellungen vor:

```
[global]

   workgroup = WORKGROUP

   security = ADS

   realm = REALM

   client signing = yes

   client use spnego = yes

   kerberos method = secrets and keytab
<!--NeedCopy-->
```

WORKGROUP ist das erste Feld in **REALM** und REALM ist der Kerberos-Bereichsname in Großbuchstaben.

Domänenbeitritt mit samba:

Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Windows-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen.

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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

Einrichten von SSSD Installieren oder aktualisieren Sie die erforderlichen Pakete:

Installieren Sie ggf. die erforderlichen SSSD- und Konfigurationspakete:

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

Wenn die Pakete bereits installiert sind, wird die Aktualisierung empfohlen:

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


> **Hinweis:**
>
> Beim Installationsvorgang in Ubuntu werden **nsswitch.conf** und das PAM-Anmeldemodul automatisch konfiguriert.

Konfigurieren von SSSD Vor dem Start des SSSD-Daemon sind SSSD-Konfigurationsänderungen erforderlich. Für einige Versionen von SSSD ist die Konfigurationsdatei **/etc/sssd/sssd.conf** nicht standardmäßig installiert und muss manuell erstellt werden. Öffnen oder erstellen Sie als Root-Benutzer **/etc/sssd/sssd.conf** und nehmen Sie folgende Einstellungen vor:

```
[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
```



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

> **Hinweis:**
>
> ldap_id_mapping ist auf **true** festgelegt, sodass SSSD die Zuordnung von Windows SIDs zu Unix UIDs selbst vornimmt. Andernfalls muss Active Directory POSIX-Erweiterungen bereitstellen können. Der PAM-Dienst `ctxhdx` wird ad_gpo_map_remote_interactive hinzugefügt.

Die Eigenschaft **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. example.com. **REALM** ist der Kerberos-Bereichsname in Großbuchstaben, z. B. EXAMPLE.COM. Die Konfiguration des NetBIOS-Domänennamens ist nicht erforderlich.

> **Tipp:**
>
> Weitere Informationen zu diesen Konfigurationseinstellungen finden Sie auf den Manpages über sssd.conf und sssd-ad.

Für den SSSD-Daemon muss die Konfigurationsdatei Besitzer-Leseberechtigung haben:

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

Starten des SSSD-Daemon Führen Sie die folgenden Befehle aus, um den SSSD-Daemon zu starten und den Daemon beim Systemstart der Maschine zu aktivieren:

```
sudo systemctl start sssd

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

PAM-Konfiguration Führen Sie den folgenden Befehl aus. Stellen Sie sicher, dass die Optionen **SSS authentication** und **Create home directory on login** aktiviert sind:

```
sudo pam-auth-update
<!--NeedCopy-->
```

Überprüfen der Domäneneigentümerschaft Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen(Windows und Linux VDAs) ein Computerobjekt in Active Directory haben.

Überprüfen Sie die Domänenmitgliedschaft mit adcli:

Zeigen Sie die Domäneninformationen an, indem Sie folgenden Befehl ausführen:

```
sudo adcli info domain-dns-name
<!--NeedCopy-->
```


Überprüfen Sie die Domänenmitgliedschaft mit samba:

Führen Sie den Samba-Befehl `net ads` aus, um zu prüfen, ob die Maschine zu einer Domäne gehört:

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

Führen Sie den folgenden Befehl aus, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen:

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

Überprüfen der Kerberos-Konfiguration Überprüfen Sie, ob Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, indem Sie sicherstellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde und gültige Schlüssel enthält:

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

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller mit diesen Schlüsseln zu authentifizieren:

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

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

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

Überprüfen der Benutzerauthentifizierung SSSD bietet kein Befehlszeilentool zum direkten Testen der Authentifizierung mit dem Daemon, daher kann der Test nur mit PAM ausgeführt werden.

Um sich zu vergewissern, dass das SSSD-PAM-Modul fehlerfrei konfiguriert wurde, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
ssh localhost -l domain\username

id -u

klist

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

Stellen Sie sicher, dass die vom Befehl **klist** zurückgegebenen Kerberos-Tickets für den Benutzer richtig und nicht abgelaufen sind.

Überprüfen Sie als Root-Benutzer, dass eine entsprechende Ticketcachedatei für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt am KDE- oder Gnome-Anzeigemanager anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 4: Installieren des Linux VDA fort.

Schritt 4: Installieren des Linux VDA

Schritt 4a: Herunterladen des Linux VDA-Pakets

Rufen Sie die Citrix-Website auf und laden Sie das entsprechende Linux VDA-Paket herunter, je nach Linux-Distribution.

Schritt 4b: Installieren des Linux VDA

Installieren Sie die Linux VDA-Software mit dem Debian-Paketmanager:

```
sudo dpkg -i xendesktopvda_7.15.0.404-1.ubuntu16.04_amd64.deb
<!--NeedCopy-->
```

Debian-Abhängigkeitsliste für Ubuntu:

```
postgresql >= 9.5

libpostgresql-jdbc-java >= 9.2

default-jdk >= 2:1.8
```



```
imagemagick >= 8:6.8.9.9

ufw >= 0.35

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42

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

python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~
<!--NeedCopy-->
```

Schritt 4c: Konfigurieren des Linux VDA

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Das Skript überprüft die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Führen Sie Änderungen erst danach durch. Sie können das Skript nach Bedarf jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell unter Reaktion auf Aufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript durch, bevor Sie fortfahren:

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

Konfiguration mit Aufforderungen Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:


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

Automatische Konfiguration Bei einer automatischen Installation können die für das Setupskript erforderlichen Optionen mit Umgebungsvariablen angegeben werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript keine weiteren Informationen vom Benutzer und der Installationsvorgang wird per Skript ausgeführt.

Unterstützte Umgebungsvariablen umfassen u. a.:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME = Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Standardeinstellung ist N.
- **CTX_XDL_DDC_LIST** = **list-ddc-fqdns** –Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT** = **port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist standardmäßig Port 80.
- **CTX_XDL_REGISTER_SERVICE = Y | N** –Die Linux Virtual Desktop-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES** = **Y | N** –Für die Linux Virtual Desktop-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION** = **1 | 2 | 3 | 4** –Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt. Geben Sie die zu verwendende Active Directory-Integrationsmethode an:
  - 1 –Samba Winbind
  - 2 –Quest-Authentifizierungsdienst
  - 3 –Centrify DirectControl
  - 4 –SSSD
- **CTX_XDL_HDX_3D_PRO** = **Y | N** –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Wenn HDX 3D Pro aktiviert ist, muss der Virtual Delivery Agent für VDI-Desktopmodus (Einzelsitzungen) konfiguriert werden (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE** = **Y | N** –Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Legen Sie dies bei Umgebungen mit HDX 3D Pro auf "Y"fest. Standardmäßig ist diese Variable auf N festgelegt.

- **CTX_XDL_SITE_NAME** = **dns-name** –Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_LDAP_LIST** = **list-ldap-servers** –Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE** = **search-base-set** –Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI, DC=mycompany,DC=com). Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_START_SERVICE** = **Y | N** –Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Die Standardeinstellung ist Y.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST=list-ddc-fqdns

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-name

export CTX_XDL_LDAP_LIST=list-ldap-servers

export CTX_XDL_SEARCH_BASE=search-base-set

export CTX_XDL_START_SERVICE=Y|N

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

Sie müssen die Option **-E** mit dem Befehl “sudo”angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Citrix empfiehlt, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:


```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=list-ddc-fqdns \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=list-ldap-servers \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_START_SERVICE=Y|N \

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

Entfernen von Konfigurationsänderungen In einigen Fällen müssen die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernt werden, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

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

Entfernen von Konfigurationsänderungen:

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

> **Wichtig:**
>
> Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank, sodass der Linux VDA nicht funktionsfähig ist.

Konfigurationsprotokolle Die Skripts **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an und schreiben weitere Informationen in die Konfigurationsprotokolldatei **/tm-**

p/xdl.configure.log.

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

Deinstallieren der Linux VDA-Software Überprüfen, ob der Linux VDA installiert ist, und Anzeigen der Version des installierten Pakets:

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

Anzeigen weiterer Details:

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

Deinstallieren der Linux VDA-Software:

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

> **Hinweis:**
>
> Beim Deinstallieren der Linux VDA-Software werden die damit verknüpften PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden nicht gelöscht.
>
> **Tipp:**
>
> Die Informationen in diesem Abschnitt beziehen sich nicht auf das Entfernen von abhängigen Paketen einschließlich PostgreSQL.

Schritt 5: Ausführen des Linux VDA

Wenn Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, können Sie den Linux VDA mit den folgenden Befehlen steuern.

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo systemctl start ctxhdx

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

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:


```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

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

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```

Schritt 6: Erstellen des Maschinenkatalogs in XenApp oder XenDesktop

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt der traditionellen Windows VDA-Methode. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.

Beim Erstellen von Maschinenkatalogen mit Linux VDA-Maschinen gibt es einige Einschränkungen, durch die sich der Prozess von der Maschinenkatalogerstellung für Windows VDA-Maschinen unterscheidet:

- Auswahl des Betriebssystems:
  - Das Serverbetriebssystem für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Das Desktopbetriebssystem für ein VDI-dediziertes Desktopbereitstellungsmodell.
- Stellen Sie sicher, dass für die Maschinen keine Energieverwaltung festgelegt ist.
- Da MCS für Linux VDAs nicht unterstützt wird, wählen Sie die Bereitstellungsmethode PVS oder **Anderer Dienst oder andere Technologie** (vorhandene Images).
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

> **Hinweis:**
>
> In früheren Citrix Studio-Versionen wurde Linux als Betriebssystem nicht unterstützt. Durch die Auswahl von Windows-Serverbetriebssystem oder Serverbetriebssystem wird jedoch ein äquivalentes gehostetes, freigegebenes Desktopbereitstellungsmodell bereitgestellt. Durch die Auswahl von Windows-Desktopbetriebssystem oder Desktopbetriebssystem wird ein Bereitstellungsmodell für Einzelbenutzermaschinen bereitgestellt.
>
> **Tipp:**
>
> Wenn Sie eine Maschine aus einer Active Directory-Domäne entfernen und sie ihr dann wieder hinzufügen, muss die Maschine auch aus dem Maschinenkatalog entfernt und ihm dann erneut hinzugefügt werden.

Schritt 7: Erstellen der Bereitstellungsgruppe in XenApp oder XenDesktop

Die Prozesse zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen mit Linux VDA- bzw. Windows VDA-Maschinen sind fast identisch. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Bereitstellungsgruppen.

Beim Erstellen von Bereitstellungsgruppen mit Linux VDA-Maschinenkatalogen gelten die folgenden Einschränkungen:

- Wählen Sie als Bereitstellungstyp **Desktops** aus. Linux VDA für Ubuntu unterstützt keine Bereitstellung von Anwendungen.
- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.
- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

Konfigurieren des Linux VDA

November 21, 2020

In diesem Abschnitt werden die Features des Linux VDA, ihre Konfiguration und die Problembehandlung beschrieben.

Integrieren von NIS in Active Directory

November 30, 2022

In diesem Artikel wird beschrieben, wie NIS in Windows Active Directory (AD) auf dem Linux VDA mithilfe von SSSD integriert wird. Der Linux VDA ist eine Komponente von Citrix XenApp und XenDesktop. Daher passt er eng in die Windows AD-Umgebung.

Zur Verwendung von NIS statt AD als UID- und GID-Anbieter müssen die Kontoinformationen (Benutzernamen/Kennwortkombinationen) in AD und NIS identisch sein.

> **Hinweis:**
>
> Die Authentifizierung findet weiterhin auf dem Active Directory-Server statt. NIS+ wird nicht unterstützt. Wenn Sie NIS als UID- und GID-Anbieter verwenden, werden die POSIX-Attribute des Windows-Servers nicht mehr verwendet.
>
> **Tipp:**
>
> Diese Methode ist eine veraltete Methode zum Bereitstellen des Linux VDA und wird nur in besonderen Fällen verwendet Für eine RHEL/CentOS-Distribution folgen Sie den Anweisungen unter Install Linux Virtual Delivery Agent for RHEL/CentOS. Für eine Ubuntu-Distribution folgen Sie den Anweisungen unter Install Linux Virtual Delivery Agent for Ubuntu.

SSSD:

SSSD ist ein System-Daemon. Seine primäre Funktion ist die Bereitstellung des Zugriffs zur Identifizierung und Authentifizierung von Remoteressourcen über ein gemeinsames Framework, das Zwischenspeicherung und Offlineunterstützung für das System liefert. Es bietet PAM- und NSS-Module und soll künftig D-BUS-Schnittstellen für erweiterte Benutzerinformationen unterstützen. Es bietet zudem eine bessere Datenbank für lokale Benutzerkonten und erweiterte Benutzerdaten.

Erforderliche Software

Der AD-Anbieter wurde mit SSSD Version 1.9.0 eingeführt.

Die folgenden Umgebungen wurden gemäß den Anweisungen in diesem Artikel getestet:

- RHEL 7.3 oder höher/CentOS 7.3 oder höher
- Linux VDA-Version 1.3 oder höher

Integrieren von NIS in Active Directory

Um NIS mit AD zu integrieren, gehen Sie wie folgt vor:

1. Fügen Sie den Linux VDA als NIS-Client hinzu
2. Treten Sie der Domäne bei und erstellen Sie eine Hostschlüsseltabelle mit Samba
3. Einrichten von SSSD
4. Konfigurieren von NSS/PAM
5. Überprüfen der Kerberos-Konfiguration
6. Überprüfen der Benutzerauthentifizierung

Fügen Sie den Linux VDA als NIS-Client hinzu

Konfigurieren Sie den NIS-Client:

```
yum –y install ypbind rpcbind oddjob-mkhomedir
<!--NeedCopy-->
```

Legen Sie die NIS-Domäne fest:

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
<!--NeedCopy-->
```

Fügen Sie die IP-Adresse des NIS-Servers/-Clients zu **/etc/hosts** hinzu:

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

Konfigurieren Sie NIS über authconfig:

```
sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
   nis.domain --enablemkhomedir --update
<!--NeedCopy-->
```

nis.domain ist der Name der NIS-Serverdomäne. **server.nis.domain** ist der Hostname des NIS-Servers (bzw. dessen IP-Adresse).

Konfigurieren Sie die NIS-Dienste:

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
<!--NeedCopy-->
```

Vergewissern Sie sich, dass die NIS-Konfiguration richtig ist:

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

Prüfen Sie, ob die Kontoinformationen über den NIS-Server zur Verfügung stehen:

```
getent passwd nisaccount
<!--NeedCopy-->
```


> **Hinweis:**
>
> **nisaccount**ist das tatsächliche NIS-Konto auf dem NIS-Server. Stellen Sie sicher, dass UID/GID, Homeverzeichnis und Anmeldeshell richtig konfiguriert sind.

Treten Sie der Domäne bei und erstellen Sie eine Hostschlüsseltabelle mit Samba

SSSD bietet keine AD-Clientfunktionen für den Domänenbeitritt und die Verwaltung der Systemschlüsseltabelle. Zum Ausführen dieser Funktionen gibt es mehrere Methoden:

- adcli
- realmd
- Winbind
- Samba

Die Informationen in diesem Abschnitt basieren auf der Verwendung von Samba. Informationen über **realmd** finden Sie in der Dokumentation zu RHEL oder CentOS. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

Treten Sie der Domäne bei und erstellen Sie eine Hostschlüsseltabelle mit Samba:

Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

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

Konfigurieren Sie die Maschine für die Authentifizierung mit Samba und Kerberos:

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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **domain** ist der NetBIOS-Name der Domäne.

Wenn eine DNS-basierte Suche nach dem KDC-Server und -Bereichsnamen erforderlich ist, fügen Sie dem vorherigen Befehl die folgenden beiden Optionen hinzu:

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

Öffnen Sie die Datei **/etc/samba/smb.conf** und fügen Sie im Abschnitt **[Global]** nach dem von dem Tool **authconfig** erstellten Abschnitt die folgenden Einträge hinzu:

```
kerberos method = secrets and keytab
```

Zum Beitritt zur Windows-Domäne muss der Domänencontroller erreichbar sein und Sie müssen ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zu der Domäne haben:


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

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

Einrichten von SSSD

Die Einrichtung von SSSD umfasst die folgenden Schritte:

- Installieren der Pakete **sssd-ad** und **sssd-proxy** auf der Linux-Clientmaschine.
- Ändern der Konfiguration verschiedener Dateien (z. B. **sssd.conf**).
- Starten des Diensts **sssd**.

/etc/sssd/sssd.conf Muster einer **sssd.conf**-Konfiguration (weitere Optionen können bei Bedarf hinzugefügt werden):

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

Ersetzen Sie **ad.domain.com**, **server.ad.example.com** durch den jeweils gültigen Wert. Weitere Informationen finden Sie unter sssd-ad(5) - Linux man page.

Legen Sie Dateieigentümer und Berechtigungen für **sssd.conf** fest:

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

Konfigurieren von NSS/PAM

RHEL/CentOS:

Aktivieren Sie SSSD mit **authconfig**. Installieren Sie **oddjob-mkhomedir**, damit die Erstellung des Homeverzeichnisses mit SELinux kompatibel ist:

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

sudo systemctl start sssd

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

> **Tipp:**
>
> Berücksichtigen Sie bei der Konfiguration der Linux VDA-Einstellungen, dass es für SSSD keine besonderen Einstellungen für den Linux VDA-Client gibt. Verwenden Sie als weitere Lösung im Skript **ctxsetup.sh** den Standardwert.

Überprüfen der Kerberos-Konfiguration

Um sicherzustellen, dass Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, überprüfen Sie, ob die Systemdatei für die **Schlüsseltabelle** erstellt wurde und gültige Schlüssel enthält:

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

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl **kinit** aus, um die Maschine mit dem Domänencontroller zu authentifizieren, die diese Schlüssel verwendet:


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

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

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

Überprüfen der Benutzerauthentifizierung

Prüfen Sie mit dem Befehl **getent**, ob das Anmeldeformat unterstützt wird und ob NSS funktioniert:

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

Der Parameter **DOMAIN** ist die kurze Version des Domänennamens. Wenn ein anderes Anmeldeformat von erforderlich ist, überprüfen Sie dies zunächst mit dem Befehl **getent**.

Unterstützte Anmeldeformate:

- Down-Level-Anmeldename: `DOMAIN\username`
- UPN: `username@domain.com`
- NetBIOS-Suffix-Format: `username@DOMAIN`

Um sich zu vergewissern, dass das SSSD-PAM-Modul fehlerfrei konfiguriert wurde, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
sudo localhost  – l DOMAIN\username

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

Stellen Sie sicher, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **uid** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```


Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

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

Veröffentlichen von Anwendungen

July 8, 2022

Mit Linux VDA-Version 7.13 hat Citrix das Feature Seamlessanwendungen auf allen unterstützten Linux-Plattformen hinzugefügt. Zum Verwenden dieses Features sind keine besonderen Installationsmaßnahmen erforderlich.

> **Tipp:**
>
> Für Version 1.4 des Linux VDA hat Citrix die Unterstützung für veröffentlichte Nicht-Seamlessanwendungen und die Sitzungsfreigabe hinzugefügt.

Veröffentlichen von Anwendungen mit Citrix Studio

Sie können die auf einem Linux VDA installierten Anwendungen beim Erstellen einer Bereitstellungsgruppe veröffentlichen oder einer vorhandenen Bereitstellungsgruppe hinzufügen. Dies ist vergleichbar mit dem Veröffentlichen von auf einem Windows VDA installierten Anwendungen. Weitere Informationen finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation(basierend auf der verwendeten Version von Citrix Virtual Apps and Desktops).

> **Tipp:**
>
> Achten Sie beim Konfigurieren von Bereitstellungsgruppen darauf, als Bereitstellungstyp **Desktop und Anwendungen** oder **Anwendungen** festzulegen.
>
> **Wichtig:**
>
> Die Veröffentlichung von Anwendungen wird unter Linux VDA-Version 1.4 und höher unterstützt. Der Linux VDA unterstützt jedoch keine Bereitstellung von Desktops und Anwendungen für dieselbe Maschine. Um dieses Problem zu lösen, empfiehlt Citrix, für App- und Desktop-Bereitstellungen separate Bereitstellungsgruppen zu erstellen.
>
> **Hinweis:**
>
> Um Seamlessanwendungen zu verwenden, deaktivieren Sie den Seamlessmodus nicht auf StoreFront. Der Seamlessmodus ist standardmäßig aktiviert. Wenn Sie den Modus

> durch "TWIMode=Off"bereits deaktiviert haben, entfernen Sie diese Einstellung, statt sie in "TWIMode=On"zu ändern. Andernfalls können Sie u. U. keine veröffentlichten Desktops starten.

Problembehandlung

Es kann vorkommen, dass der Start einer veröffentlichten Anwendung länger als zwei Minuten dauert und Fenster nicht im Seamlessmodus angezeigt werden. Stellen Sie in diesem Fall sicher, dass der Seamlessmodus auf dem Linux VDA und in StoreFront aktiviert wurde.

Der Befehl zum Prüfen, ob der Seamlessmodus auf dem Linux VDA aktiviert ist:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg list -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix"  |  grep "SeamlessEnabled"
2 <!--NeedCopy-->
```

Wenn "SeamlessEnabled = 0x00000000"angezeigt wird, ist der Seamlessmodus deaktiviert. Um ihn zu aktivieren, führen Sie den folgenden Befehl aus:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update  -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix"  -v "SeamlessEnabled" -d "0
     x00000001"
2 <!--NeedCopy-->
```

Bekannte Probleme

Beim Veröffentlichen von Anwendungen sind folgende Probleme bekannt:

- Anwendungen, die im Nicht-Seamlessmodus veröffentlicht wurden, werden nicht gestartet, wenn der Seamlessmodus auf StoreFront deaktiviert, auf dem Linux VDA jedoch weiterhin aktiviert ist. Aktivieren bzw. deaktivieren Sie den Seamlessmodus auf dem Linux VDA und auf StoreFront.
- Nicht-rechteckige Fenster werden nicht unterstützt. Die Ecken eines Fensters zeigen möglicherweise den serverseitigen Hintergrund an.
- Die Vorschau des Inhalts eines Fensters aus einer veröffentlichten Anwendung wird nicht unterstützt.
- Der Seamlessmodus unterstützt zurzeit folgende Fenstermanager: Mutter (CentOS7.3\RHEL7.3\SUSE12.2), Metacity (CentOS6.6\RHEL6.6\SUSE 11.4) und Compiz (Ubuntu 16.04). Kwin und andere Fenstermanager werden nicht unterstützt. Stellen Sie sicher, dass Ihr Fenstermanager unterstützt wird.
- Wenn Sie mehrere LibreOffice-Anwendungen ausführen, wird nur die zuerst gestartete in Citrix Studio angezeigt, da diese Anwendungen denselben Prozess verwenden.

- Veröffentlichte, auf Qt5 basierende Anwendungen wie "Dolphin"zeigen u. U. keine Symbole an. Um das Problem zu beheben, lesen Sie den Artikel unter https://wiki.archlinux.org/index.php/Qt.
- Alle Taskleistenschaltflächen veröffentlichter Anwendungen, die in der gleichen ICA-Sitzung ausgeführt werden, werden in der gleichen Gruppe zusammengefasst. Um dieses Problem zu beheben, legen Sie über die Eigenschaft "Taskleiste"fest, dass die Taskleistenschaltflächen nicht zusammengefasst werden.

Drucken

November 21, 2020

Dieser Artikel enthält Informationen zu bewährten Druckmethoden.

Installation

Der Linux VDA benötigt die Filter **cups** und **foomatic**. Führen Sie, je nach Linux-Distribution, die folgenden Befehle aus:

Druckunterstützung für RHEL 7:

```
sudo yum –y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```

Druckunterstützung für RHEL 6:

```
sudo yum –y install cups

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

Verwendung

Sie können aus veröffentlichten Desktops und veröffentlichten Anwendungen drucken. Nur der clientseitige Standarddrucker wird in einer Linux VDA-Sitzung zugeordnet. Der Druckername muss für Desktops und Anwendungen unterschiedlich sein. Beachten Sie Folgendes:

- Veröffentlichte Desktops:
  `CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`

- Veröffentlichte Anwendungen
  `CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

> **Hinweis:**
>
> Wenn ein Benutzer einen veröffentlichten Desktop und eine veröffentlichte Anwendung öffnet, stehen in der Sitzung beide Drucker zur Verfügung. Das Drucken auf einem Desktopdrucker in einer veröffentlichten Anwendung und auf einem Anwendungsdrucker über einen veröffentlichten Desktop schlägt fehl.

Problembehandlung

Fehler beim Drucken

Sie können verschiedene Elemente überprüfen, wenn der Druckvorgang nicht richtig funktioniert. Der Druckdaemon ist ein pro Sitzung ausgeführter Vorgang, der für die gesamte Sitzungsdauer ausgeführt werden muss. Prüfen Sie, ob der Druck-Daemon ausgeführt wird.

```
ps –ef | grep ctxlpmngt
<!--NeedCopy-->
```

Wenn der Prozess **ctxlpmngt** nicht ausgeführt wird, starten Sie **ctxlpmngt** manuell über eine Befehlszeile. Wenn der Druck immer noch nicht funktioniert, überprüfen Sie das CUPS-Framework. Der Dienst **ctxcups** dient zur Druckerverwaltung und kommuniziert mit dem Linux CUPS-Framework. Es gibt jeweils einen Prozess pro Maschine, der mit folgendem Befehl überprüft werden kann:

```
service ctxcups status
<!--NeedCopy-->
```

Zusätzliches Protokoll beim Drucken von CUPS

Als Komponente des Linux VDA ist die Methode zum Abrufen des Protokolls einer Druckkomponente anderen Komponenten ähnlich.

Bei RHEL sind einige zusätzliche Schritte erforderlich, um die CUPS-Dienstdatei zu konfigurieren. Andernfalls werden einige Protokolle nicht in **hdx.lo** protokolliert:

```
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-->
```

> **Hinweis:**
>
> Das vollständige Druckprotokoll sollte mit dieser Konfiguration nur bei einem Problem abgerufen werden. Normalerweise wird diese Konfiguration nicht empfohlen, da sie die CUPS-Sicherheit verletzt.

Druckausgabe ist verzerrt

Eine fehlerhafte Ausgabe kann durch einen nicht kompatiblen Druckertreiber verursacht werden. Pro Benutzer ist eine Treiberkonfiguration verfügbar und kann durch das Bearbeiten der Konfigurationsdatei **~/.CtxlpProfile$CLIENT_NAME** konfiguriert werden:

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
<!--NeedCopy-->
```

> **Wichtig:**
>
> Das Feld **printername** enthält den Namen des aktuellen Clientstandarddruckers. Dieser Wert ist schreibgeschützt. Bearbeiten Sie ihn nicht.
>
> Nehmen Sie nicht gleichzeitig Eingaben in den Feldern **ppdpath**, **model** und **drivertype**, da nur eines für den zugeordneten Drucker wirksam ist.

Wenn der universelle Druckertreiber mit dem Clientdrucker nicht kompatibel ist, konfigurieren Sie das Modell des nativen Druckertreibers mit der Option **model=**. Sie finden den aktuellen Modellnamen des Druckers mit dem Befehl **lpinfo**:

```
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-->
```


Sie können dann das Modell gemäß dem Drucker festlegen:

```
Model=xerox/ph3115.ppd.gz
<!--NeedCopy-->
```

Wenn der universelle Druckertreiber nicht mit dem Clientdrucker kompatibel ist, konfigurieren Sie den PPD-Dateipfad für den nativen Druckertreiber. Der Wert von **ppdpath** ist der absolute Pfad der nativen Druckertreiberdatei.

Beispielsweise ist ein **ppd-Treiber** unter /home/tester/NATIVE_PRINTER_DRIVER.ppd vorhanden.

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
<!--NeedCopy-->
```

Citrix bietet drei universelle Druckertreibertypen: postscript, pcl5 und pcl6. Sie können den Treibertyp konfigurieren, wenn kein nativer Druckertreiber verfügbar ist.

Beispiel: Der Standarddruckertreibertyp des Client ist PCL5.

```
drivertype=pcl5
<!--NeedCopy-->
```

Ausgabegröße ist Null

Versuchen Sie es mit anderen Druckertypen. Versuchen Sie es auch mit einem virtuellen Drucker wie CutePDF oder PDFCreator, um zu ermitteln, ob das Problem mit dem Druckertreiber zusammenhängt.

Der Druckauftrag hängt vom Druckertreiber und dem Standarddrucker des Clients ab. Es ist wichtig, den Typ des aktuell aktiven Treibers zu identifizieren. Wenn der Clientdrucker einen PCL5-Treiber verwendet, der Linux VDA jedoch einen PostScript-Treiber auswählt, kann ein Problem auftreten.

Wenn der Druckertreibertyp richtig ist, können Sie das Problem mit folgenden Schritten finden:

Problemdiagnose

1. Melden Sie sich bei dem ICA-Sitzungsdesktop an.
2. vi ~/.CtxlProfile$CLIENT_NAME
3. Fügen Sie auf dem Linux VDA das folgende Feld hinzu, um die Spooldatei zu speichern:

   ```
   deletespoolfile=no
   <!--NeedCopy-->
   ```

4. Melden Sie sich ab und wieder an, um die Konfigurationsänderungen zu laden.
5. Drucken Sie das Dokument zum Reproduzieren des Problems. Nach dem Druckvorgang wird unter **/var/spool/cups-ctx/$logon_user/$spool_file** eine Spooldatei gespeichert.

6. Prüfen Sie, ob die Spooldatei leer ist. Wenn die Spooldatei NULL ist, liegt ein Problem vor. Wenden Sie sich mit dem Druckprotokoll an den Citrix Support.
7. Wenn die Spooldatei nicht NULL ist, kopieren Sie die Datei auf den Client. Der Inhalt der Spooldatei hängt vom Druckertreibertyp und dem Standarddrucker des Clients ab. Wenn der zugeordnete (native) Druckertreiber ein PostScript-Treiber ist, kann die Spooldatei direkt im Linux-Betriebssystem geöffnet werden. Prüfen Sie den Inhalt auf Korrektheit.

   Bei einer PCL-Spooldatei oder einem Windows-Betriebssystem auf dem Client kopieren Sie die Spooldatei auf den Client und drucken Sie sie auf dem clientseitigen Drucker. Testen Sie sie anschließend mit dem anderen Druckertreiber.
8. Zum Wechseln des zugeordneten Druckers zu einem anderen Drittanbieter-Druckertreiber verwenden Sie den PostScript-Clientdrucker als Beispiel:

   a) Melden Sie sich bei einer aktiven Sitzung an und öffnen Sie einen Browser auf dem Clientdesktop.

   b) Öffnen Sie das Druckverwaltungsportal:

   ```
   localhost:631
   <!--NeedCopy-->
   ```

   c) Wählen Sie den zugeordneten Drucker **CitrixUniversalPrinter:$ClientName:app/dek$SESSION_ID** und dann **Modify Printer** aus. Hierfür sind Administratorprivilegien erforderlich.

   d) Behalten Sie die cups-ctx-Verbindung bei und klicken Sie auf "Continue", um den Druckertreiber zu ändern.

   e) Wählen Sie auf der Seite "Make and Model"einen anderen PostScript-Treiber als den Citrix UPD-Treiber aus (z. B. Citrix Universal Driver Postscript). Wenn beispielsweise der virtuelle CUPS-PDF-Drucker installiert ist, wählen Sie den Drucker "Generic CUPS-PDF Printer". Speichern Sie die Änderung.

   f) Wenn der Vorgang Erfolg hat, konfigurieren Sie den PPD-Dateipfad des Treibers in **.CtxlpProfile$CLIENT_NAME** so, dass der zugeordnete Drucker einen Drittanbietertreiber verwenden darf.

Bekannte Probleme

Die folgenden Probleme beim Drucken mit dem Linux VDA sind bekannt:

CTXPS-Treiber ist mit einigen PLC-Druckern nicht kompatibel

Wenn Sie Druckausgabestörungen bemerken, legen Sie als Druckertreiber den nativen Druckertreiber des Herstellers fest.

Langsame Druckleistung bei großen Dokumenten

Wenn Sie ein großes Dokument auf einem lokalen Clientdrucker drucken, wird das Dokument über die Serververbindung übertragen. Bei langsamen Verbindungen kann die Übertragung sehr lange dauern.

Drucker- und Druckauftragsbenachrichtigungen aus anderen Sitzungen werden angezeigt

Linux hat nicht das gleiche Sitzungskonzept wie das Windows-Betriebssystem. Daher erhalten alle Benutzer systemweite Benachrichtigungen. Durch Ändern der CUPS-Konfigurationsdatei **/etc/cups/cupsd.conf** können Sie diese Benachrichtigungen deaktivieren.

Suchen Sie den aktuellen, in der Datei konfigurierten Richtliniennamen:

```
DefaultPolicy default
```

Wenn der Richtlinienname *default* lautet, fügen Sie dem XML-Block der Standardrichtlinie die folgenden Zeilen hinzu:

```
<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-Druck

November 5, 2021

Mit einer Version der Citrix Workspace-App, die PDF-Druck unterstützt, können Sie PDF-Dateien aus Linux VDA-Sitzungen heraus drucken. Druckaufträge aus der Sitzung werden an den lokalen Computer gesendet, auf dem die Citrix Workspace-App installiert ist. Auf dem lokalen Computer können Sie PDFs mit Ihrem bevorzugten PDF-Viewer öffnen und auf dem Drucker Ihrer Wahl ausdrucken.

Der Linux VDA unterstützt den PDF-Druck auf folgenden Versionen der Citrix Workspace-App:

- Citrix Receiver für HTML5 Versionen 2.4 bis 2.6.9, Citrix Workspace-App 1808 für HTML5 und höher
- Citrix Receiver für Chrome Versionen 2.4 bis 2.6.9, Citrix Workspace-App 1808 für Chrome und höher
- Citrix Workspace-App 1905 für Windows und höher

Konfiguration

Sie müssen eine Version der Citrix Workspace-App verwenden, die den PDF-Druck unterstützt, und außerdem die folgenden Richtlinien in Citrix Studio aktivieren:

- **Clientdruckerumleitung** (standardmäßig aktiviert)
- **Universellen PDF-Drucker automatisch erstellen** (standardmäßig deaktiviert)

Wenn diese Richtlinien aktiviert sind und Sie in einer aktiven Sitzung auf **Drucken** klicken, wird auf der lokalen Maschine eine Druckvorschau angezeigt, sodass Sie einen Drucker auswählen können. Informationen zum Festlegen von Standarddruckern finden Sie in der Dokumentation für die Citrix Workspace-App.

Konfigurieren von Grafiken

November 30, 2022

Dieser Artikel enthält eine Anleitung zur Grafikkonfiguration und -optimierung für den Linux VDA.

Weitere Informationen finden Sie unter Systemanforderungen und Installationsübersicht.

Konfigurationsparameter

Es gibt mehrere Grafikkonfigurationsparameter in **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control** die Sie mit dem Hilfsprogramm **ctxreg** optimieren können.

Aktivieren von ThinWire Plus

ThinWire Plus ist für den Standard-VDA und 3D Pro standardmäßig aktiviert.

Aktivieren von H.264

Neben dem Betriebssystem gilt für H.264 eine Mindestanforderung an die Version der Citrix Workspace-App (früher Citrix Receiver). Erfüllt der Client die Anforderungen nicht, erfolgt ein Fallback auf ThinWire Plus.

Betriebssystem	Mindestanforderung für H.264
Windows	3.4 oder höher
Mac OS X	11.8 oder höher
Linux	13.0 oder höher
Android	3.5
iOS	5.9
Chrome OS	1.4

Die aktuelle Featurematrix für die Citrix Workspace-App finden Sie unter https://docs.citrix.com/de-de/citrix-workspace-app/citrix-workspace-app-feature-matrix.html.

Führen Sie den folgenden Befehl aus, um die H.264-Codierung auf dem VDA anzukündigen:

```
1 sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\
     Thinwire" -t "REG_DWORD" -v "AdvertiseH264" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Aktivieren der Hardwarecodierung in HDX 3D Pro

Für HDX 3D Pro aktiviert die Einstellung **AdvertiseH264** nur die H.264-Softwarecodierung.
Führen Sie folgenden Befehl aus, um die Hardwarecodierung zu aktivieren:


```
sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\
    Thinwire" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000001" --
    force
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn der Fehler "`ctxreg command can't be found`"angezeigt wird, verwenden Sie den Befehl "`ctxreg`"mit einem vollständigen Pfad. Verwenden Sie zum Beispiel `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "REG_DWORD"-v "AdvertiseH264"-d "0x00000001"–force` anstelle von `sudo ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-t "REG_DWORD"-v "AdvertiseH264"-d "0x00000001"–force`.

Einstellen von ThinWire Plus für geringere Bandbreiten

- MaxColorDepth

  ```
  Default 0x20, type DWORD
  <!--NeedCopy-->
  ```

  Mit dieser Option wird die Farbtiefe von Grafiken festgelegt, die mit dem ThinWire-Protokoll an den Client übertragen werden.

  Zum Einsparen von Bandbreite legen Sie 0x10 (bevorzugte Farbtiefe für einfache Grafiken) oder auf 0x8 (experimenteller Modus für geringe Bandbreiten) fest.

- Qualität

  Bildqualität

  ```
  Default: 0x1(medium), type: DWORD, valid values: 0x0(low), 0x1(
      medium), 0x2(high), 0x3(build to lossless), 0x4 always
      lossless.
  <!--NeedCopy-->
  ```

  Zum Einsparen von Bandbreite legen Sie 0x0(low) fest.

- Mehr Parameter

  - TargetFPS

    Frameratesollwert

    ```
    Default: 0x1e (30), Type: DWORD
    <!--NeedCopy-->
    ```


- MinFPS

  Mindestframeratesollwert

  ```
  Default: 0xa (10), Type: DWORD
  <!--NeedCopy-->
  ```

- MaxScreenNum

  Maximale Anzahl Monitore, die der Client haben kann

  ```
  Default: 0x2, Type: DWORD
  <!--NeedCopy-->
  ```

  Für einen Standard-VDA können Sie maximal 10 festlegen. Für 3D Pro können Sie maximal 4 festlegen.

Problembehandlung

Ermitteln der verwendeten Codierung

Verwenden Sie den folgenden Befehl, um zu ermitteln, ob die H.264-Codierung verwendet wird (**1** = H.264, **0** = TW+):

```
sudo ctxreg dump | grep H264
<!--NeedCopy-->
```

Das Ergebnis sieht in etwa wie folgt aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force
```

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

Ermitteln, ob die Hardwarecodierung für 3D Pro verwendet wird

Führen Sie folgenden Befehl aus (**0** = nicht verwendet; **1** = verwendet):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
<!--NeedCopy-->
```

Das Ergebnis sieht in etwa wie folgt aus:

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

Alternativ können Sie den Befehl **nvidia-smi** verwenden. Wird die Hardwarecodierung verwendet, sieht die Ausgabe in etwa wie folgt aus:


```
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-->
```

Prüfung auf fehlerfreie Installation des NVIDIA GRID-Grafiktreibers

Um die korrekte Installation des NVIDIA GRID-Grafiktreibers zu überprüfen, führen Sie **nvidia-smi** aus. Das Ergebnis sieht in etwa wie folgt aus:

```
+-----------------------------------------------------+
| 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-->
```

Legen Sie die richtige Konfiguration für die Karte fest:

`etc/X11/ctx-nvidia.sh`

HDX 3D Pro - Probleme bei der Darstellungsaktualisierung bei mehreren Monitoren

Wenn beim Verwenden mehrerer Monitore Probleme bei der Darstellungsaktualisierung auf den sekundären Monitoren auftreten, prüfen Sie, ob die NVIDIA GRID-Lizenz verfügbar ist.

Überprüfen der Xorg-Fehlerprotokolle

Die Xorg-Protokolldatei heißt **Xorg.{DISPLAY}.log** (oder ähnlich) und ist im Ordner **/var/log/**.

Bekannte Probleme und Einschränkungen

Für vGPU wird auf der lokalen XenServer-Konsole der ICA-Desktopsitzungsbildschirm angezeigt

Workaround: Deaktivieren Sie die lokale VGA-Konsole der VM, indem Sie den folgenden Befehl ausführen:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
<!--NeedCopy-->
```


NVENC-API wird in anderen vGPU-Profilen als 8Q nicht unterstützt

Andere vGPU-Profile für die NVIDIA Tesla M60-Karte als 8Q unterstützen cuda nicht. Daher stehen die NVENC-API und Citrix 3D Pro-Hardwarecodierung nicht zur Verfügung.

NVIDIA K2-Grafikkarten unterstützen nicht die YUV444-Hardwarecodierung im Passthroughmodus

Dies ist eine Einschränkung der NVIDIA K2-Grafikkarte.

Gnome 3-Desktoppopups bei Anmeldung langsam

Dies ist eine Einschränkung im Gnome 3-Desktopsitzungsstart.

Einige OpenGL/WebGL-Anwendungen werden nach einer Änderung der Größe des Citrix Receiver-Fensters nicht einwandfrei gerendert

Beim Ändern der Größe des Citrix Receiver-Fensters wird die Bildschirmauflösung geändert. Damit ändern sich einige interne Zustände des proprietären NVIDIA-Treibers, wodurch Anwendungen möglicherweise entsprechend reagieren müssen. Zum Beispiel das WebGL-Bibliothekselement **lightgl.js** könnte einen Fehler zeigen: ‘`Rendering to this texture is not supported (incomplete frame buffer)`’.

Nicht-GRID 3D-Grafiken

March 13, 2024

Übersicht

Mit dieser Funktionserweiterung unterstützt der Linux VDA nicht nur NVIDIA GRID 3D-Karten, sondern auch nicht-GRID 3D-Karten.

Installation

Um Nicht-GRID 3D-Grafiken verwenden zu können:

- Installieren Sie XDamage als Voraussetzung. Normalerweise ist XDamage als eine Erweiterung von XServer vorhanden.
- Setzen Sie `CTX_XDL_HDX_3D_PRO` auf `Y` bei der Installation des Linux VDA. Informationen zu Umgebungsvariablen finden Sie unter Schritt 3: Einrichten der Laufzeitumgebung für die Installation.

Konfiguration

Xorg-Konfigurationsdateien

Wenn der 3D-Kartentreiber NVIDIA ist, werden die Konfigurationsdateien automatisch installiert und eingerichtet.

Andere 3D-Karten

Wenn der Treiber Ihrer 3D-Karte nicht NVIDIA ist, müssen Sie die vier unter `/etc/X11/` installierten Vorlagenkonfigurationsdateien ändern:

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf
- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

Verwenden Sie die Datei **ctx-driver_name-1.conf** als Beispiel, um die folgenden Änderungen an den Vorlagenkonfigurationsdateien zu machen:

1. Ersetzen Sie ***driver_name*** durch den Namen Ihres Treibers.

   Wenn der Treibername beispielsweise `intel` ist, ändern Sie den Namen der Konfigurationsdatei in `ctx-intel-1.conf`.

2. Fügen Sie die Videotreiberinformationen hinzu.

   Jede Vorlagenkonfigurationsdatei enthält einen Abschnitt "Device", der auskommentiert ist. Dieser Abschnitt beschreibt die Informationen zum Videotreiber. Aktivieren Sie in diesen Abschnitt, bevor Sie die Videotreiberinformationen hinzufügen. Sie aktivieren den Abschnitt wie folgt:

   a) Sie finden Konfigurationsinformationen in der Dokumentation des Herstellers Ihrer 3D-Karte. Es wird eine native Konfigurationsdatei erstellt. Stellen Sie sicher, dass Ihre 3D-Karte in einer lokalen Umgebung mit der nativen Konfigurationsdatei funktioniert, wenn Sie keine über den Linux VDA hergestellte ICA-Sitzung verwenden.

b) Kopieren Sie den Abschnitt “Device”aus der nativen Konfigurationsdatei nach **ctx-driver_name-1.conf**

3. Führen Sie den folgenden Befehl aus, um den Registrierungsschlüssel festzulegen, mit dem der Linux VDA den in Schritt 1 festgelegten Konfigurationsdateinamen erkennt.

```
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-->
```

Aktivieren des Features für nicht-GRID 3D-Grafiken

Das Feature für rasterlose 3D-Grafiken ist standardmäßig deaktiviert. Führen Sie zum Aktivieren folgenden Befehl aus, mit dem XDamageEnabled auf 1 festgelegt wird.

```
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-->
```

Problembehandlung

Keine oder fehlerhafte Grafikausgabe

Wenn Sie 3D-Anwendungen lokal ausführen können und alle Konfigurationen richtig sind, ist keine oder eine fehlerhafte Grafikausgabe das Ergebnis eines Fehlers. Verwenden Sie /opt/Citrix/VDA/bin/setlog und legen Sie GFX_X11 auf “verbose”fest, um die Ablaufverfolgungsinformationen für das Debuggen zu sammeln.

Hardwarecodierung funktioniert nicht

Dieses Feature unterstützt nur die Softwarecodierung.

Konfigurieren von Richtlinien

November 5, 2021

Installation

Folgen Sie den Anleitungen zur Installation, um den Linux VDA vorzubereiten.

Abhängigkeiten

Installieren Sie vor der Installation des Linux VDA-Pakets die nachfolgend aufgeführte erforderliche Software.

RHEL/CentOS:

```
sudo yum -y install openldap

sudo yum -y install libxml2

sudo yum -y install cyrus-sasl

sudo yum -y install cyrus-sasl-gssapi
<!--NeedCopy-->
```

SLES/SELD:

```
sudo zypper install openldap2

sudo zypper install libxml2

sudo zypper install cyrus-sasl

sudo zypper install cyrus-sasl-gssapi
<!--NeedCopy-->
```

Ubuntu:

```
sudo apt-get install -y libldap-2.4-2

sudo apt-get install -y libsasl2-2

sudo apt-get install -y libsasl2-modules-gssapi-mit
<!--NeedCopy-->
```

Konfiguration

Richtlinieneinstellungen in Citrix Studio

Zum Festlegen von Richtlinien in Citrix Studio führen Sie folgende Schritte aus:

1. Öffnen Sie **Citrix Studio**.
2. Wählen Sie den Bereich **Richtlinien**.

3. Klicken Sie auf **Richtlinie erstellen**.
4. Legen Sie die Richtlinie gemäß der Liste der unterstützten Richtlinien fest.

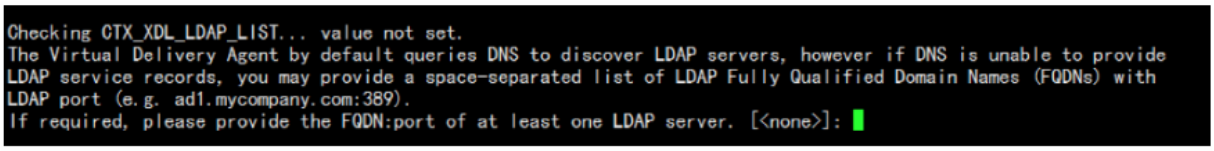
LDAP-Servereinstellung auf dem VDA

Die LDAP-Servereinstellung für den Linux VDA ist in Umgebungen mit einer Domäne optional. In Umgebungen mit mehreren Domänen oder mehreren Gesamtstrukturen ist sie obligatorisch. Die Einstellung ist für den Richtliniendienst zum Ausführen der LDAP-Suche in diesen Umgebungen erforderlich.

Führen Sie nach der Installation des Linux VDA-Pakets folgenden Befehl aus:

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

Geben Sie alle LDAP-Server im empfohlenen Format ein: durch Leerzeichen getrennte Liste der vollqualifizierten Domänennamen (FQDN) der LDAP-Server mit LDAP-Port (z. B. ad1.mycompany.com:389 ad2.mycomany.com:389).



Sie können diese Einstellung auch mit dem Befehl **ctxreg** direkt in die Registrierung schreiben:

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

Die folgenden Richtlinien gelten nur für den Linux VDA und können nur in Citrix Studio Version 7.12 und höher konfiguriert werden:

- ClipboardSelectionUpdateMode
- PrimarySelectionUpdateMode
- MaxSpeexQuality

Die Liste der unterstützten Richtlinien enthält Beschreibungen der Richtlinien. Wenn Sie Citrix Studio Version 7.11 oder früher verwenden, müssen Sie diese Richtlinien lokal auf dem Linux VDA mit dem Befehl **ctxreg** konfigurieren:

> **Hinweis:**
>
> Die Werte sind auf einen bestimmten Bereich beschränkt. Ausführliche Beschreibungen finden Sie in der Liste der unterstützten Richtlinien.

Liste der unterstützten Richtlinien

November 5, 2021

Liste der für Linux VDA unterstützten Richtlinien

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
ICA-Keep-Alives	SendICAKeepAlives	ComputerA	ICA\Keep Alive	Keine ICA-Keep-Alive-Meldungen senden (0)
ICA-Keep-Alive - Timeout	ICAKeepAliveTimeout	ComputerA	ICA\Keep Alive	60 Sekunden
ICA-Listenerportnummer	IcaListenerPortNumber	ComputerA	ICA	1494
Bandbreitenlimit für die Audioumleitung	LimitAudioBandwidth	BenutzerA	Audio	0 KBit/s
Clientaudioumleitung	AllowAudioRedirection	BenutzerA	Audio	Zugelassen (1)
Clientdruckerumleitung	AllowPrinterRedirection	BenutzerA	Drucken	Zugelassen (1)
Clientzwischenablageumleitung	AllowClipboardRedirection	BenutzerA	Zwischenablage	Zulässig (1)
Client-USB-Geräteumleitung	AllowUSBRedirection	BenutzerA	USB	Nicht zugelassen (0)

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert						
Regeln für die Client-USB-Geräteumleitung	USBDeviceRules	Benutzer	USB	”	Regeln für die Client-USB-Geräteumleitung	USBDeviceRules	Benutzer	USB	“\0”	”
Bewegtbildkomprimierung	MovingImageCompressionConfiguration	Benutzer	Thinwire	Aktiviert (1)						
Mindestframerate für Bewegtbildkomprimierung	TargetedMinimumFramesPerSecond	Benutzer	Thinwire	10 f/s						
Framerate für Bewegtbildkomprimierung	SoftwarePBSecond	Benutzer	Thinwire	30 f/s						
Bildqualität	VisualQuality	Benutzer	Thinwire	Mittel (3)						
Verwenden von Videocodec für die Komprimierung	VideoCodec	Benutzer	Thinwire	Bevorzugt verwenden (3)						
Verwenden der Hardwarecodierung für Videocodec	UseHardwareEncodingForVideoCodec	Benutzer	Thinwire	Aktiviert (1)						
Bevorzugte Farbtiefe für einfache Grafiken	PreferredColorDepth	Benutzer	Thinwire	24 Bit pro Pixel (1)						

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Audioqualität	SessionAudioQuality	Benutzer	Audio	Hoch - High Definition Audio (2)
Clientmikrofonumleitung zulassen	AllowMicrophoneRedirection	Benutzer	Audio	Zugelassen (1)
Sitzungsverwaltung	MaximumNumberOfSessions	Computer	Sitzungsverwaltung	250
Toleranzwert für gleichzeitige Anmeldungen	ConcurrentLogonTolerance	Computer	Sitzungsverwaltung	2
Automatische Controllerupdates aktivieren	EnableAutoUpdateOfController	Computer	Virtual Delivery Agent-Einstellungen	Zugelassen (1)
Aktualisierungsmodus für die Zwischenablageauswahl	ClipboardSelectionUpdateMode	Sitzung	Zwischenablage	
Aktualisierungsmodus für die Primärauswahl	PrimarySelectionUpdateMode	Sitzung	Zwischenablage	
Max. Speex-Qualität	MaxSpeexQuality	Computer	Audio	5

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Clientlaufwerke automatisch verbinden	AutoConnectDrives	BenDrives	ICA\File	Aktiviert (1)
Optische Clientlaufwerke	AllowCdromDrives	BenDrives	ICA\File	Zugelassen (1)
Lokale Clientfestplattenlaufwerke	AllowFixedDrives	BenDrives	ICA\File	Zugelassen (1)
Clientdiskettenlaufwerke	AllowFloppyDrives	BenDrives	ICA\File	Zugelassen (1)
Clientnetzwerklaufwerke	AllowNetworkDrives	BenDrives	ICA\File	Zugelassen (1)
Clientwechselmedienlaufwerke	AllowRemovableDrives	BenDrives	ICA\File	Zugelassen (1)
Clientlaufwerkumleitung	AllowDriveRedir	BenDrives	ICA\File	Zugelassen (1)
Schreibgeschützter Zugriff auf Clientlaufwerke	ReadOnlyMappedDrive	BenDrives	ICA\File	Deaktiviert (0)

Die folgenden Richtlinien können in Citrix Studio Version 7.12 und höher konfiguriert werden.

- MaxSpeexQuality

  Wert (Ganzzahl): [0–10]

  Standardwert: 5

Details:

Die Audioumleitung codiert Audiodaten mit dem Speex-Codec, wenn die Audioqualität mittelmäßig oder niedrig ist (siehe Richtlinie "Audioqualität"). Speex ist ein verlustbehafteter Codec, d. h. die Komprimierung geht auf Kosten der Genauigkeit des Eingabesprachsignals. Im Gegensatz zu anderen Sprachencodecs kann das Verhältnis zwischen Qualität und Bitrate gesteuert werden. Der Speex-Codierungsprozess wird meist über einen Qualitätsparameter mit einem Wertebereich von 0 bis 10 gesteuert. Je höher die Qualität, desto höher ist die Bitrate.

Die maximale Speex-Qualität wählt die beste Speex-Qualität für die Audiodatencodierung gemäß Audioqualität und Bandbreitenlimit (siehe Richtlinie "Bandbreitenlimit für die Audioumleitung"). Bei mittlerer Audioqualität erfolgt die Codierung im Breitbandmodus mit einer höheren Samplingrate. Bei niedriger Audioqualität erfolgt die Codierung im Schmalbandmodus mit einer niedrigeren Samplingrate. Bei gleicher Speex-Qualität ist die Bitrate in verschiedenen Modi unterschiedlich. Die beste Speex-Qualität wird erreicht, wenn für den höchsten Wert folgende Bedingungen zutreffen:

- Es ist kleiner oder gleich der maximalen Speex-Qualität.
- Die Bitrate ist kleiner oder gleich dem Bandbreitenlimit.

Verwandte Einstellungen: Audioqualität, Bandbreitenlimit für die Audioumleitung

- PrimarySelectionUpdateMode

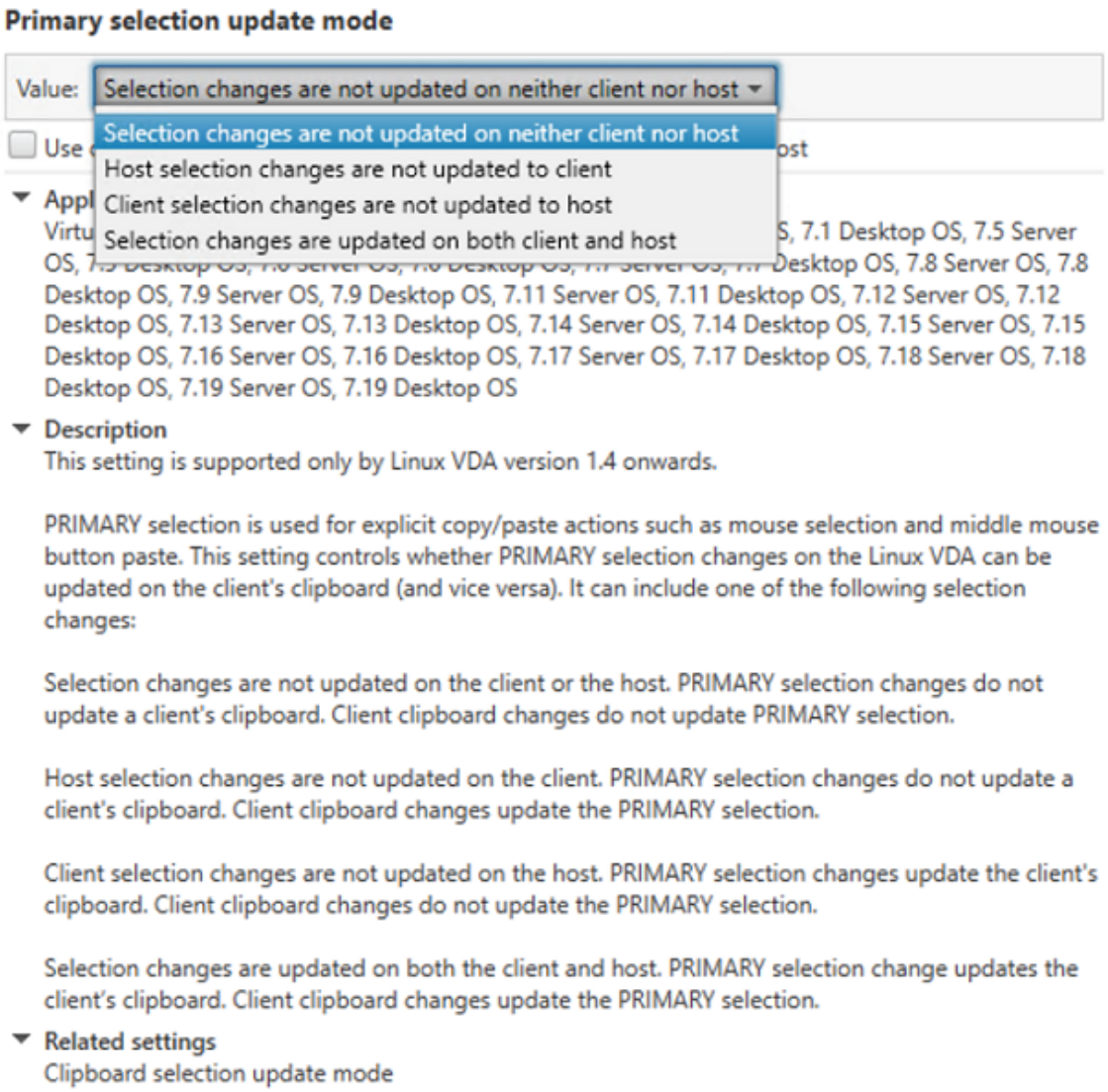
  Wert (Aufzählung): [0, 1, 2, 3]

  Standardwert: 3

  Details:

  Mit der Primärauswahl können Sie ausgewählte Daten durch Drücken der mittleren Maustaste einfügen.

  Diese Richtlinie steuert, ob bei einer Änderung der Primärauswahl auf dem Linux VDA bzw. Client die Zwischenablage des jeweils anderen aktualisiert werden kann. Es gibt vier mögliche Werte:



- **Auswahländerungen werden weder auf Client noch auf Host aktualisiert**
  Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.
- **Auswahländerungen auf dem Host werden nicht auf dem Client aktualisiert**
  Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert.
- **Auswahländerungen auf dem Client werden nicht auf dem Host aktualisiert**
  Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.

– **Auswahländerungen werden auf Client und Host aktualisiert**
Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert. Diese Option ist der Standardwert.

Verwandte Einstellung: Aktualisierungsmodus für die Zwischenablageauswahl

- ClipboardSelectionUpdateMode

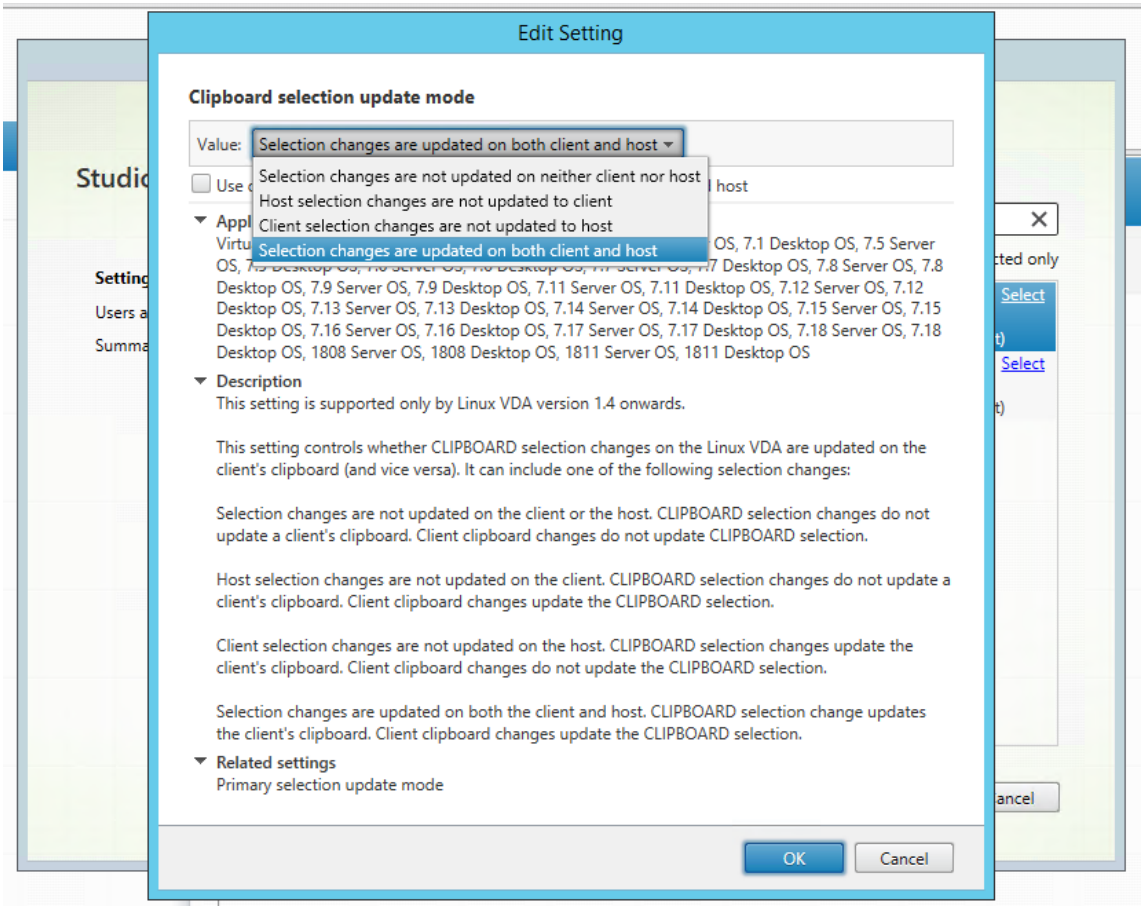
Wert (enum): [0, 1, 2, 3]

Standardwert: 3

Details:

Die Zwischenablageauswahl wird verwendet, um ausgewählte Daten explizit in die Zwischenablage zu kopieren (z. B. durch Auswahl von "Kopieren"aus dem Kontextmenü). Die Zwischenablageauswahl wird vor allem mit der Zwischenablage in Microsoft Windows verwendet, während die Primärauswahl nur in Linux genutzt werden kann.

Diese Richtlinie steuert, ob bei Zwischenablageänderungen auf dem Linux VDA bzw. Client die Zwischenablage des jeweils anderen aktualisiert werden kann. Es gibt vier mögliche Werte:



- **Auswahländerungen werden weder auf Client noch auf Host aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.
- **Auswahländerungen auf dem Host werden nicht auf dem Client aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert.
- **Auswahländerungen auf dem Client werden nicht auf dem Host aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.
- **Auswahländerungen werden auf Client und Host aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert. Diese Option ist der Standardwert.

Verwandte Einstellung: Aktualisierungsmodus für die Primärauswahl

> **Hinweis:**
>
> Der Linux VDA unterstützt die Zwischenablageauswahl und die Primärauswahl. Um das Kopier- und Einfügeverhalten zwischen Linux VDA und Client zu steuern, empfehlen wir, dass Sie den Aktualisierungsmodus für Zwischenablage- und Primärauswahl auf denselben Wert festzulegen.

Konfigurieren von IPv6

May 13, 2020

Der Linux VDA bietet Unterstützung für IPv6, um die Funktionalität an XenApp und XenDesktop anzugleichen. Beachten Sie bei der Verwendung dieses Features Folgendes:

- Für Umgebungen mit dualem Stapel wird IPv4 verwendet, es sei denn, IPv6 wurde explizit aktiviert.
- Wenn IPv6 in einer IPv4-Umgebung aktiviert ist, funktioniert der Linux VDA nicht.

> **Wichtig:**
>
> - Die gesamte Netzwerkumgebung muss IPv6 sein, nicht nur der Linux VDA.
> - Centrify unterstützt reines IPv6 nicht.

Bei der Installation des Linux VDA ist für IPv6 keine spezielle Einrichtung erforderlich.

Konfigurieren von IPv6 für den Linux VDA

Bevor Sie die Konfiguration für den Linux VDA ändern, stellen Sie sicher, dass die virtuelle Linux-Maschine zuvor in einem IPv6-Netzwerk funktioniert hat. Für die IPv6-Konfiguration müssen zwei Registrierungsschlüssel festgelegt werden:

```
1 “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
    -v “OnlyUseIPv6ControllerRegistration”
2
3 “HKLM\Software\Policies\Citrix\VirtualDesktopAgent” -t “REG_DWORD”
    -v “ControllerRegistrationIPv6Netmask”
4 <!--NeedCopy-->
```

OnlyUseIPv6ControllerRegistration muss auf 1 festgelegt werden, damit IPv6 auf dem Linux VDA aktiviert ist:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
    OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Wenn der Linux VDA mehrere Netzwerkschnittstellen hat, kann mit **ControllerRegistrationIPv6Netmask** angegeben werden, welche für die Linux VDA-Registrierung verwendet wird:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
    Citrix\VirtualDesktopAgent" -t "REG_SZ" -v "
    ControllerRegistrationIPv6Netmask " -d "{
2  IPv6 netmask }
3  " --force
4 <!--NeedCopy-->
```

Ersetzen Sie **{IPv6 netmask}** mit der echten Netzwerkmaske (z. B. 2000::/64).

Weitere Informationen zur Bereitstellung von IPv6 in XenApp und XenDesktop finden Sie unter Unterstützung für IPv4/IPv6.

Problembehandlung

Überprüfen Sie die grundlegende IPv6-Netzwerkumgebung und prüfen Sie mit ping6, ob AD und Delivery Controller erreichbar sind.

Konfigurieren des Citrix-Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP)

February 11, 2021

Wenn Sie an dem Programm teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, um die Qualität und Leistung der Citrix Produkte zu verbessern.

Registrierungseinstellungen

Standardmäßig nehmen Sie bei der Installation des Linux VDA automatisch am CEIP teil. Der erste Datenupload erfolgt ca. sieben Tage nach der Installation des Linux VDAs. Sie können die Standardeinstellung über eine Registrierungseinstellung ändern.

- **CEIPSwitch**

Die Registrierungseinstellung, mit der das CEIP aktiviert oder deaktiviert wird (Standardwert = 0):

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: CEIPSwitch

Wert: 1 = deaktiviert , 0 = aktiviert

Wenn nicht angegeben, ist CEIP aktiviert.

Sie können auf einem Client den folgenden Befehl ausführen, um das CEIP zu deaktivieren:

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

- **DataPersistPath**

Die Registrierungseinstellung zur Steuerung des Datenspeicherpfads (Standard = /var/xdl/ceip):

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: DataPersistPath

Wert: Zeichenfolge

Legen Sie den Pfad mit folgendem Befehl fest:

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

Wenn der konfigurierte Pfad nicht vorhanden ist oder nicht darauf zugegriffen werden kann, werden die Daten im Standardpfad gespeichert.

Vom Linux VDA gesammelte CEIP-Daten

In der folgende Tabelle sehen Sie Beispiele für die Art der anonymen Informationen, die gesammelt werden. Die Daten enthalten keine Informationen, die Sie als Kunden identifizieren.

Datenpunkt	Schlüsselname	Beschreibung
Maschinen-GUID	machine_guid	Identifiziert die Maschine, von der die Daten stammen.
AD-Lösung	ad_solution	Textzeichenfolge, die die Domänenbeitrittsmethode der Maschine angibt.
Linux-Kernelversion	kernel_version	Textzeichenfolge, die die Kernelversion der Maschine angibt.
LVDA-Version	vda_version	Textzeichenfolge, die die installierte Version des Linux VDA angibt.
LVDA-Update oder Neuinstallation	update_or_fresh_install	Textzeichenfolge, die das aktuelle Linux VDA-Paket angibt, das installiert oder aktualisiert wird.
LVDA-Installiermethode	install_method	Textzeichenfolge, die angibt, wie das aktuelle Linux VDA-Paket installiert wurde: MCS, PVS, einfache oder manuelle Installation.
HDX 3D Pro aktiviert oder nicht	hdx_3d_pro	Textzeichenfolge, die angibt, ob HDX 3D Pro auf der Maschine aktiviert ist.
VDI-Modus aktiviert oder nicht	vdi_mode	Textzeichenfolge, die angibt, ob der VDI-Modus aktiviert ist.
Letzter Neustart der LVDA-Schlüsseldienste	ctxhdx ctxvda	Die Zeit des letzten Neustarts der `ctxhdx`- und `ctxvda`-Dienste im Format tt-hh:mm:ss, z. B. 10-17:22:19
GPU-Typ	gpu_type	Der GPU-Typ der Maschine.
CPU-Kerne	cpu_cores	Ganzzahl, die die Anzahl der CPU-Kerne des Computers angibt.

Datenpunkt	Schlüsselname	Beschreibung
CPU-Frequenz	cpu_frequency	Die CPU-Frequenz in MHz.
Größe des physischen Speichers	memory_size	Ganzzahl, die die Größe des physischen Speichers in KB angibt.
Anzahl der aktiven Sitzungen	active_session_number	Ganzzahl, die die Anzahl der aktiven Sitzungen auf der Maschine zum Zeitpunkt der Datenerfassung angibt.
Linux-OS-Name und -Version	os_name_version	Textzeichenfolge, die Namen und Version des Linux-OS auf der Maschine angibt.
Sitzungsschlüssel	session_key	Identifiziert die Sitzung, aus der die Daten stammen.
Benötigte Wiederverbindungszeit	econnect_time_cost	Speichert die benötigte Wiederverbindungszeit einer Sitzung. Die Größe des Arrays ist 5. Damit verfolgen wir den aktuellen Wert, den Mindestwert, den maximalen Wert, die laufende Summe und die Anzahl der Updates des Datenpunkts.
Aktive Sitzungszeiten	active_session_time	Speichert die aktiven Zeiten der Sitzung. Eine Sitzung kann mehrere aktive Zeiten haben, da die Sitzung getrennt und wieder verbunden werden kann.
Sitzungsdauer	session_duration_time	Speichert die Sitzungsdauer von der Anmeldung bis zur Abmeldung.
Receiver-Clienttyp	receiver_type	Ganzzahl, die den zum Starten der Sitzung verwendeten Citrix Receiver-Typ angibt.
Receiver-Clientversion	receiver_version	Textzeichenfolge, die die zum Starten der Sitzung verwendete Citrix Receiver-Version angibt.

Datenpunkt	Schlüsselname	Beschreibung
Druckzähler	printing_count	Ganzzahl, die angibt, wie oft die Druckfunktion in der Sitzung verwendet wurde.
USB-Umleitungszähler	usb_redirecting_count	Ganzzahl, die angibt, wie oft ein USB-Gerät in der Sitzung verwendet wurde.

Konfigurieren der USB-Umleitung

November 5, 2021

USB-Geräte werden von Citrix Receiver und Linux VDA-Desktop gemeinsam verwendet. Wenn ein USB-Gerät an einen Desktop umgeleitet wird, kann es wie ein lokal verbundenes Gerät verwendet werden.

Die USB-Umleitung umfasst drei hauptsächliche Funktionalitätsbereiche:

- Open-Source-Projektimplementierung (VHCI)
- VHCI-Dienst
- USB-Dienst

Open-Source-VHCI:

Dieser Teil der USB-Umleitung besteht aus der Entwicklung eines allgemeinen Systems zur USB-Gerätefreigabe über ein IP-Netzwerk. Er umfasst einen Linux-Kerneltreiber und einige Benutzermodusbibliotheken für die Kommunikation mit dem Kerneltreiber zum Abruf aller USB-Daten. In der Linux VDA-Implementierung hat Citrix den VHCI-Kerneltreiber wiederverwendet. Alle USB-Datenübertragungen zwischen Linux VDA und Citrix Receiver erfolgen jedoch gekapselt im Citrix ICA-Protokollpaket.

VHCI-Dienst:

Der VHCI-Dienst ist ein von Citrix zur Kommunikation mit dem VHCI-Kernelmodul bereitgestellter Open-Source-Dienst. Der Dienst fungiert als Gateway zwischen VHCI und dem Citrix USB-Dienst.

USB-Dienst:

Der USB-Dienst ist ein Citrix Modul, das sämtliche Virtualisierungen und Datenübertragungen auf dem USB-Gerät verwaltet.

Funktionsweise der USB-Umleitung

Wenn ein USB-Gerät an den Linux VDA umgeleitet wird, werden normalerweise ein oder mehrere Geräteknoten im Systempfad /dev erstellt. Gelegentlich kann das umgeleitete Gerät jedoch nicht für eine aktive Linux VDA-Sitzung verwendet werden. USB-Geräte funktionieren nur mit Treibern, und manche Geräte erfordern auch Spezialtreiber. Sind diese Treiber nicht vorhanden, kann in der aktiven Linux VDA-Sitzung nicht auf das umgeleitete USB-Gerät zugegriffen werden. Installieren Sie die Treiber und konfigurieren Sie das System, um eine Verbindung mit USB-Geräten zu ermöglichen.

Der Linux VDA unterstützt diverse USB-Geräte, die erfolgreich an den Client und von dem Client umgeleitet werden können. Außerdem werden solche Geräte, insbesondere USB-Datenträger, ordnungsgemäß eingebunden, sodass die Benutzer ohne zusätzliche Konfiguration darauf zugreifen können.

Unterstützte USB-Geräte

Bei den folgenden Geräten wurde die Unterstützung dieser Version des Linux VDA in Tests verifiziert. Andere Geräte können verwendet werden, jedoch können unerwartete Ergebnisse auftreten.

> **Hinweis:**
>
> Der Linux VDA unterstützt nur USB 2.0-Protokolle.

USB-Massenspeichergerät	Hersteller-ID:Produkt-ID	Dateisystem
Netac Technology Co., Ltd	0dd8:173c	FAT32
Kingston Datatraveler 101 II	0951:1625	FAT32
Kingston Datatraveler GT101 G2	1567:8902	FAT32
SanDisk SDCZ80-Flashlaufwerk	0781:5580	FAT32
WD-Festplatte	1058:10B8	FAT32

USB-3D-Maus	Hersteller-ID:Produkt-ID
3DConnexion SpaceMouse Pro	046d:c62b

USB-Scanner	Hersteller-ID:Produkt-ID
Epson Perfection V330 Photo	04B8: 0142

Konfigurieren der USB-Umleitung

Die USB-Geräteumleitung wird über eine Citrix Richtlinie aktiviert bzw. deaktiviert. Außerdem kann der Gerätetyp über eine Delivery Controller-Richtlinie festgelegt werden. Konfigurieren Sie die folgenden Richtlinien und Regeln, um die USB-Umleitung für den Linux VDA zu aktivieren:

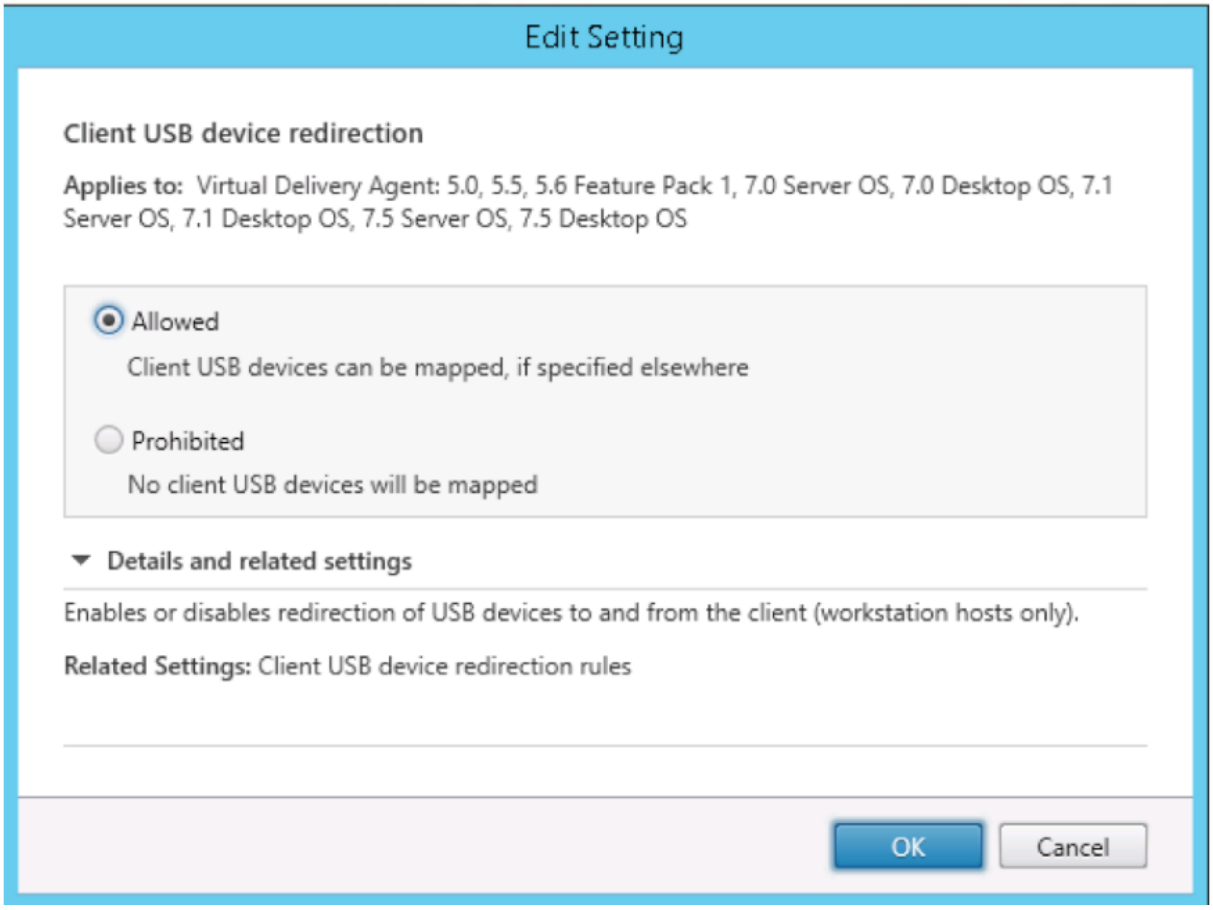
- Richtlinie für die Client-USB-Geräteumleitung
- Regeln für die Client-USB-Geräteumleitung

Aktivieren der Richtlinie für die USB-Umleitung

In Citrix Studio können Sie die Umleitung von USB-Geräten zum und vom Client (nur Arbeitsstationshosts) aktivieren und deaktivieren.

Führen Sie im Dialogfeld **Einstellung bearbeiten** folgende Schritte aus:

1. Wählen Sie **Zugelassen**.
2. Klicken Sie auf **OK**.

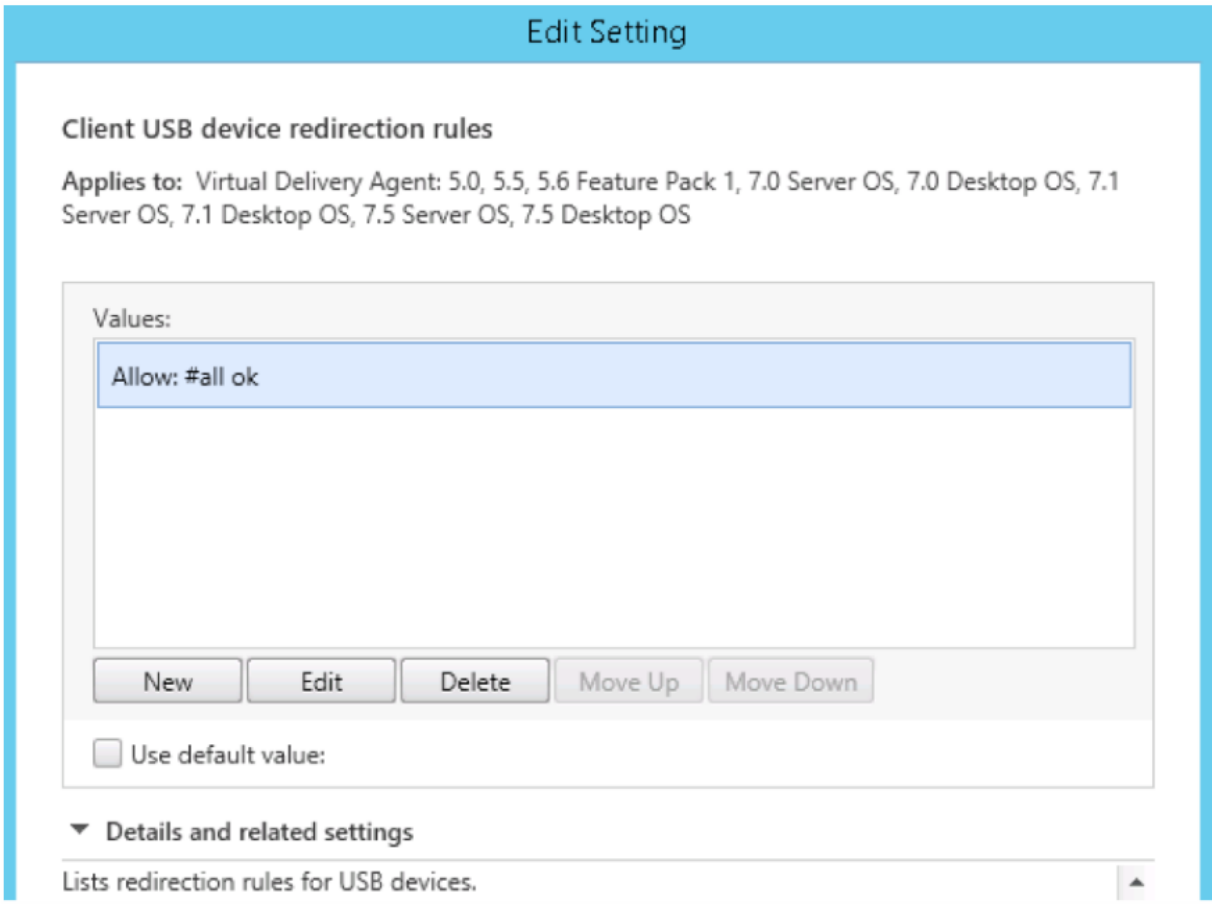


Festlegen von Regeln für die USB-Umleitung

Nach dem Aktivieren der USB-Umleitungsrichtlinie legen Sie mit Citrix Studio die Regeln für die Umleitung fest, d. h. welche Geräte auf dem Linux VDA zulässig sind und welche nicht.

Führen Sie im Dialogfeld “Regeln für die Client-USB-Geräteumleitung”folgende Schritte aus:

1. Klicken Sie auf **Neu**, um eine Umleitungsregel hinzuzufügen oder auf **Bearbeiten**, um eine vorhandene Regel zu prüfen.
2. Nach dem Erstellen bzw. Ändern der Regel klicken Sie auf **OK**.



Weitere Informationen zum Konfigurieren der generischen USB-Umleitung finden Sie im Citrix Generic USB Redirection Configuration Guide.

Erstellen des VHCI-Kernelmoduls

Die USB-Umleitung hängt von den VHCI-Kernelmodulen **usb-vhci-hcd.ko** und **usb-vhci-iocif.ko** ab. Diese Module sind Teil der Linux VDA-Distribution (als Teil des RPM-Pakets). Sie werden auf Basis der Kernel der offiziellen Linux-Distribution kompiliert:

Unterstützte Linux-Distribution	Kernelversion
RHEL 7.3	3.10.0-514.el7.x86_64
RHEL 6.6	2.6.32-504.el6.x86_64
SUSE 12.2	4.4.49-92.11-default
SUSE 11.4	3.0.101-0.47.55-default
Ubuntu 16.04	4.4.0-45-generic

> **Wichtig:**
>
> Wenn der Kernel Ihres Computers nicht mit dem Citrix Treiber für den Linux VDA kompatibel ist, kann der USB-Dienst möglicherweise nicht gestartet werden. In diesem Fall können Sie die USB-Umleitung nur dann verwenden, wenn Sie eigene VHCI-Kernelmodule erstellen.

Prüfen des vorliegenden Kernels auf Konsistenz mit dem Modul von Citrix

Führen Sie an der Befehlszeile den folgenden Befehl aus, um zu überprüfen, ob Ihr Kernel konsistent ist:

```
insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
<!--NeedCopy-->
```

Wird der Befehl ausgeführt, dann wurde das Kernelmodul erfolgreich geladen und die Version ist mit der von Citrix installierten konsistent.

Treten bei der Ausführung des Befehls Fehler auf, bedeutet dies, dass der Kernel nicht mit dem Citrix Modul konsistent ist und neu erstellt werden muss.

Neuerstellen des VHCI-Kernelmoduls

Wenn das Kernelmodul nicht mit der Citrix-Version konsistent ist, führen Sie die folgenden Schritte aus:

1. Laden Sie den LVDA-Quellcode von der Citrix download site herunter. Wählen Sie die im Abschnitt "**Linux Virtual Delivery Agent (sources)**"enthaltene Datei aus.
2. Stellen Sie die Dateien aus der Datei "citrix-linux-vda-sources.zip"wieder her. Sie können die VHCI-Quelldateien in **linux-vda-souces/vhci-hcd-1.15.tar.bz2** finden. Die VHCI-Dateien lassen sich mit **tar xvf vhci-hcd-1.15.tar.bz2** wiederherstellen.
3. Erstellen Sie das Kernelmodul basierend auf den Headerdateien und der Datei **Module.symvers**. Führen Sie die folgenden Schritte aus, um die Kernelheaderdateien zu installieren und **Module.symvers** basierend auf der entsprechenden Linux-Distribution zu erstellen:

   RHEL 7.3/RHEL 6.9/RHEL 6.6:

   ```
   yum install kernel-devel
   <!--NeedCopy-->
   ```

   SUSE 12.2:

   ```
   zypper install kernel-devel

   ```



```
zypper install kernel-source
<!--NeedCopy-->
```

SUSE 11.4:

```
zypper install kernel-source
<!--NeedCopy-->
```

Ubuntu 16.04:

```
apt-get install linux-headers
<!--NeedCopy-->
```

> **Tipp:**
>
> Wird die Installation erfolgreich abgeschlossen, dann gibt es nun einen Kernelordner, der in etwa folgenden Pfad hat:
>
> /usr/src/kernels/3.10.0-327.10.1.el7.x86_64

4. Prüfen Sie, dass in /usr/src/kernels/3.10.0-327.10.1.el7.x86_64 die Datei **Module.symvers** vorhanden ist. Ist dies nicht der Fall, erstellen Sie den Kernel, um sie zu erhalten (z. B. `make oldconfig`; `make prepare`, `make modules`; `make`) oder kopieren Sie sie von **/usr/src/kernels/3.10.0-327.10.1.el7.x86_64-obj/x86_64/defaults/module.***
5. Ändern Sie in der Datei **vhci-hcd-1.15/Makefile** die Makefile von VCHI und legen Sie KDIR auf das Kernelverzeichnis fest:

```
#KDIR = $(BUILD_PREFIX)/lib/modules/$(KVERSION)/build

KDIR = /usr/src/kernels/3.10.0-327.10.1.el7.x86_64
<!--NeedCopy-->
```

6. Führen Sie im Ordner **vhci-hcd-1.15/** den Befehl **make** aus, um den VHCI-Kernel zu erstellen.

> **Hinweis:**
>
> War die Erstellung erfolgreich, werden **usb-vhci-hcd.ko** und **usb-vhci-iocifc.ko** im Ordner **vhci-hcd-1.15/** erstellt.

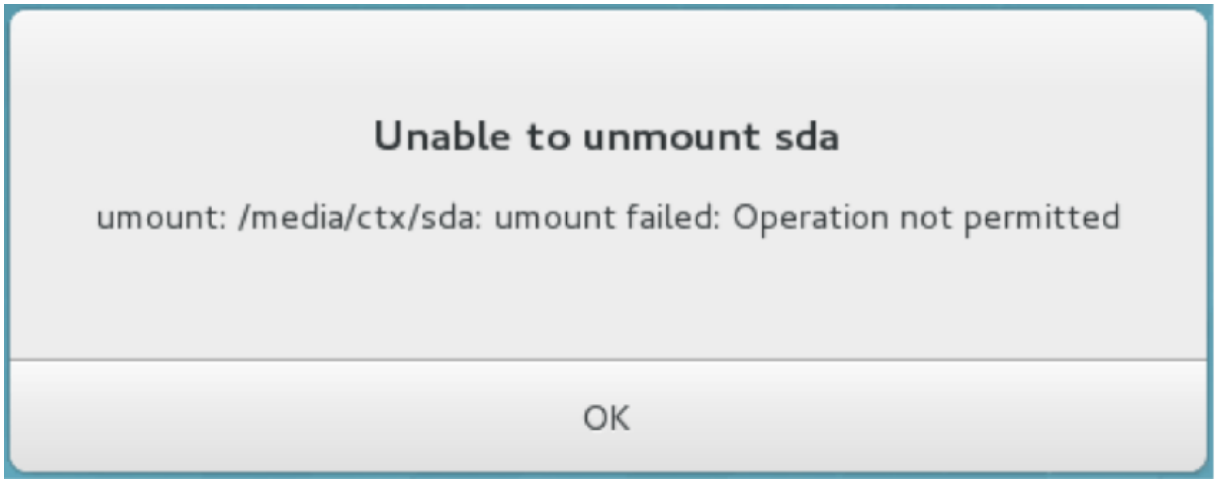
7. Ersetzen Sie das Kernelmodul durch das neu erstellte: **cp -f usb-vhci-*.ko /opt/Citrix/VDA/lib64/**
8. Starten Sie den USB-Dienst neu: **service ctxusbsd restart**
9. Melden Sie sich bei der Sitzung ab und wieder an. Überprüfen Sie, ob die USB-Umleitung funktioniert.

Behandeln von Problemen bei der USB-Umleitung

Anhand der Informationen in diesem Abschnitt können Sie diverse Probleme beheben, die bei der Verwendung des Linux VDA auftreten können.

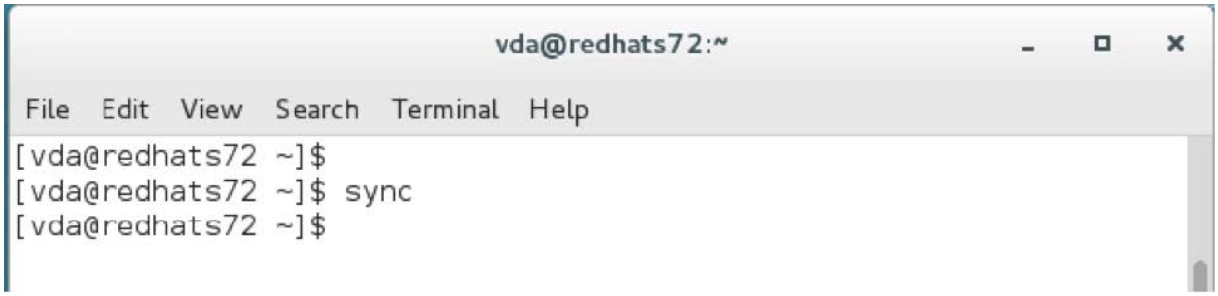
Bereitstellung eines umgeleiteten USB-Datenträgers kann nicht aufgehoben werden

Der Linux VDA verwaltet die Zugriffsteuerung für die USB-Datenträger aller von Citrix Receiver umgeleiteten USB-Geräte unter Verwendung von Administratorrechten, damit nur der Besitzer eines umgeleiteten Geräts darauf zugreifen kann. Daher können Benutzer die Bereitstellung eines Geräts ohne Administratorrechte nicht aufheben.



Bei Beenden der Umleitung eines USB-Datenträgers geht eine Datei verloren

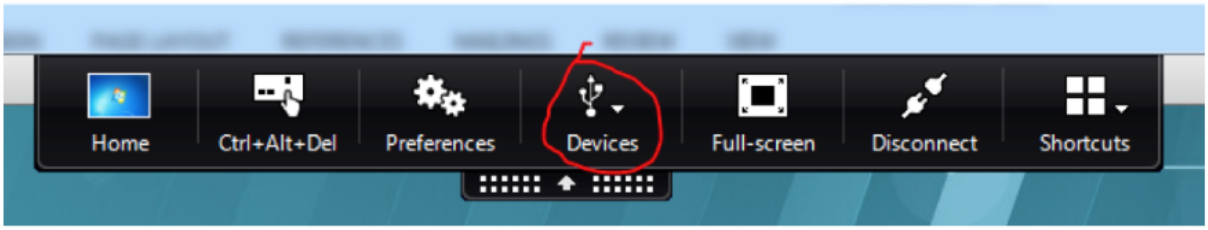
Wenn Sie einen USB-Datenträger in eine Sitzung umleiten, eine Änderung daran vornehmen (z. B. eine Datei auf dem Datenträger erstellen) und die Umleitung dann über die Symbolleiste von Citrix Receiver sofort beenden, kann die geänderte oder erstellte Datei verloren gehen. Dieses Problem tritt auf, weil beim Schreiben von Daten in ein Dateisystem der Speichercache im Dateisystem eingebunden wird. Die Daten werden nicht auf den Datenträger selbst geschrieben. Wenn Sie die Umleitung über die Symbolleiste von Citrix Receiver beenden, bleibt keine Zeit zum Übertragen der Daten auf den Datenträger und die Daten gehen verloren. Zur Problemlösung verwenden Sie den Synchronisierungsbefehl in einem Terminal, um die Daten auf den Datenträger zu übertragen, bevor Sie die USB-Umleitung beenden.



Keine Geräte in der Symbolleiste von Citrix Receiver

Es kann vorkommen, dass in der Citrix Receiver-Symbolleiste keine Geräte aufgeführt werden, d. h. dass keine USB-Umleitung stattfindet. Prüfen Sie in diesem Fall Folgendes:

- Die Richtlinie ist auf Zulassen der USB-Umleitung konfiguriert.
- Das Kernelmodul ist mit Ihrem Kernel kompatibel.



> **Hinweis:**
>
> Die Registerkarte **Geräte** ist in Citrix Receiver für Linux nicht verfügbar.

Die Umleitung schlägt fehl, wenn in der Symbolleiste von Citrix Receiver angezeigte USB-Geräte als *richtlinienbeschränkt* ausgewiesen sind

Dieses Problem wird durch die Richtlinienkonfiguration der Geräte verursacht. Gehen Sie in solchen Fällen folgendermaßen vor:

- Konfigurieren Sie die Linux VDA-Richtlinie zum Aktivieren der Umleitung.
- Prüfen Sie, ob in der Registrierung von Citrix Receiver weitere Richtlinieneinschränkungen konfiguriert sind. Möglicherweise ist ein Gerät in der Registrierung von Citrix Receiver gesperrt. Prüfen Sie **DeviceRules** im Registrierungspfad, um sicherzustellen, dass kein Gerätezugriff durch diese Einstellung verweigert wird:

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

site. Weitere Informationen finden Sie in der Anleitung zum Konfigurieren der automatischen Umleitung von USB-Geräten auf der Citrix Supportsite.

Ein USB-Gerät wird umgeleitet, kann jedoch nicht in einer Sitzung verwendet werden

In der Regel können nur unterstützte USB-Geräte umgeleitet werden. Manchmal werden jedoch auch andere Geräte in eine aktive Linux VDA-Sitzung umgeleitet. Es wird dann für jedes umgeleitete Gerät ein im Besitz des Benutzers stehender Knoten im Systempfad **/dev** erstellt. Allerdings bestimmen Treiber und Konfiguration, ob der Benutzer das Gerät verwenden kann. Wenn Sie ein angeschlossenes Gerät finden, auf das nicht zugegriffen werden kann, fügen Sie es einer uneingeschränkten Richtlinie hinzu.

> **Hinweis:**
>
> Im Fall von USB-Laufwerken erfolgt die Konfiguration und Einbindung durch den Linux VDA. Der Benutzer, der das Laufwerk installiert hat (und kein anderer), kann ohne zusätzliche Konfiguration auf das Laufwerk zugreifen. Dies ist bei Geräten, die nicht auf der Liste der unterstützten Geräte stehen, evtl. nicht möglich.

Client-Eingabemethoden-Editor (IME)

November 21, 2020

Übersicht

Doppelbytezeichen (z. B. Chinesisch, Japanisch und Koreanisch) müssen über einen IME eingegeben werden. Solche Zeichen können mit jedem clientseitig mit der Citrix Workspace-App kompatiblen Eingabemethoden-Editor eingegeben werden (z. B. Windows-eigener CJK IME).

Installation

Dieses Feature wird automatisch installiert, wenn Sie den Linux VDA installieren.

Verwendung

Öffnen Sie wie gewohnt eine XenDesktop- oder XenApp-Sitzung.

Ändern Sie die Eingabemethode nach Bedarf auf der Clientseite, um den Client-IME zu verwenden.

Bekannte Probleme

- Sie müssen auf eine Zelle in einer Google-Kalkulationstabelle doppelklicken, damit Sie mit dem Client-IME-Feature Zeichen in die Zelle eingeben können.
- Der Client-IME wird in Kennwortfeldern nicht automatisch deaktiviert.
- Die IME-Benutzerschnittstelle folgt nicht dem Cursor im Eingabebereich.
- Der Client-IME wird in einer SUSE 11-Distribution nicht unterstützt.

HDX Insight

February 9, 2024

Übersicht

HDX Insight ist Teil von Citrix Application Delivery Management (ADM) und basiert auf dem gebräuchlichen Branchenstandard AppFlow. Es ermöglicht eine ausgezeichnete Benutzererfahrung durch den umfassenden und tiefgehenden Einblick in den Citrix ICA-Datenverkehr, der durch das NetScaler- oder Citrix SD-WAN-Anwendungsnetzwerk fließt.

In diesem Release unterstützt der Linux VDA teilweise das HDX Insight-Feature. Da das Feature für End User Experience Management (EUEM) nicht implementiert ist, stehen die Datenpunkte für Zeitdauer nicht zur Verfügung.

Installation

Keine abhängigen Pakete müssen installiert werden.

Verwendung

HDX Insight analysiert die ICA-Meldungen, die über den NetScaler zwischen der Citrix Workspace-App und dem Linux VDA weitergeleitet werden.

Sie müssen mit dem Linux VDA eine NetScaler Insight Center-Bereitstellung einrichten und das HDX Insight-Feature aktivieren. Sie können Ihre NetScaler Insight Center-Bereitstellung zu Citrix ADM migrieren, ohne die vorhandene Konfiguration, Einstellungen oder Daten zu verlieren. Weitere Informationen finden Sie unter Migrieren von NetScaler Insight Center auf Citrix ADM.

Problembehandlung

Es werden keine Datenpunkte angezeigt

Es gibt zwei mögliche Ursachen:

- HDX Insight ist nicht richtig konfiguriert.

  Möglicherweise ist AppFlow auf NetScaler nicht aktiviert oder eine falsche NetScaler-Instanz ist in Insight Center konfiguriert.

- Der virtuelle ICA-Steuerungskanal wurde auf dem Linux VDA nicht gestartet.

  ```
  ps aux | grep -i ctxctl
  ```

  Wenn `ctxctl` nicht ausgeführt wird, wenden Sie sich an den Administrator, um einen Fehler an Citrix zu melden.

Es werden keine Anwendungsdatenpunkte angezeigt

Stellen Sie sicher, dass der virtuelle Seamlesskanal aktiviert ist und eine Seamlessanwendung gestartet wird.

Bekanntes Problem

Die Datenpunkte für Zeitdauer können nicht angezeigt werden. Weil das EUEM-Feature nicht implementiert ist, sind die Datenpunkte für die Zeitdauer (z. B. ICA-RTT) nicht verfügbar und werden als “–”angezeigt.

Aktive Ablaufverfolgung

November 21, 2020

Übersicht

Das Erfassen von Protokollen und Reproduzieren von Problemen verlangsamen die Diagnose und beeinträchtigen die Benutzerfreundlichkeit. Die Ablaufverfolgung erleichtert solche Aufgaben. Die Ablaufverfolgung ist für den Linux VDA standardmäßig aktiviert.

Konfiguration

Der ctxlogd-Daemon und das setlog-Dienstprogramm sind nun im Linux VDA-Releasepaket enthalten. Standardmäßig wird der ctxlogd-Daemon nach der Installation und Konfiguration des Linux VDA gestartet.

ctxlogd-Daemon

Alle anderen Dienste, deren Ablauf verfolgt wird, hängen vom ctxlogd-Daemon ab. Sie können den ctxlogd-Daemon anhalten, wenn Sie den Ablauf des Linux VDA nicht verfolgen möchten.

setlog-Dienstprogramm

Das Feature für die aktive Ablaufverfolgung wird mit dem setlog-Dienstprogramm konfiguriert. Es befindet sich unter folgendem Pfad: **/opt/Citrix/VDA/bin/**. Nur Root-Benutzer können es ausführen. Verwenden Sie zum Anzeigen und Ändern von Konfigurationen die grafische Benutzeroberfläche oder Befehle. Führen Sie den folgenden Befehl aus, um Hilfe zum setlog-Dienstprogramm aufzurufen:

```
setlog help
<!--NeedCopy-->
```

Werte Standardmäßig ist **Log Output Path** auf **/var/log/xdl/hdx.log** und **Max Log Size** auf 200 MB festgelegt. Sie können zwei alte Protokolldateien unter **Log Output Path** speichern.

Anzeigen der aktuellen setlog-Werte:

```
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-->
```

Anzeigen oder Festlegen eines einzelnen setlog-Werts:

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

Beispiel:

```
setlog value log_size 100
<!--NeedCopy-->
```


Ebenen Standardmäßig ist die Protokollebene auf **Warnings** festgelegt.

Anzeigen der Protokollebenen für verschiedene Komponenten:

```
setlog levels
<!--NeedCopy-->
```

Sie können alle Protokollebenen (einschließlich Disable, Inherited, Verbose, Information, Warnings, Errors und Fatal Errors) mit dem folgenden Befehl festlegen:

```
setlog level <class> [<level>]
<!--NeedCopy-->
```

Mit der Variable **<class>** wird eine Komponente des Linux VDA angegeben. Um alle Komponenten einzubeziehen, legen Sie alle fest:

```
setlog level all error

Setting log class ALL to ERROR.
<!--NeedCopy-->
```

Flags Flags werden wie folgt festgelegt:

```
setlog flags

DATE = true

TIME = true

NAME = true

PID = true

TID = false

SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
<!--NeedCopy-->
```

Anzeigen der aktuellen Flags:


```
setlog flags
<!--NeedCopy-->
```

Anzeigen oder Festlegen eines einzelnen Protokoll-Flags:

```
setlog flag <flag> [<state>]
<!--NeedCopy-->
```

Wiederherstellen der Standardeinstellungen Wiederherstellen der Standardeinstellungen für alle Ebenen, Flags und Werte:

```
setlog default
<!--NeedCopy-->
```

> **Wichtig:**
>
> Der `ctxlogd`-Dienst wird mit der Datei **/var/xdl/.ctxlog** konfiguriert, die nur von Root-Benutzern erstellt werden kann. Andere Benutzer haben keine Schreibrechte für diese Datei. Citrix empfiehlt Root-Benutzern, anderen Benutzern keine Schreibrechte zu geben. Die versehentliche oder mutwillige Fehlkonfiguration von `ctxlogd` kann sich negativ auf die Serverleistung und die Benutzererfahrung auswirken.

Problembehandlung

Wenn die Datei **/var/xdl/.ctxlog** nicht vorhanden ist (z. B. versehentlich gelöscht wurde), schlägt der `ctxlogd`-Daemon fehl und Sie können den `ctxlogd`-Dienst nicht neu starten.

/var/log/messages:

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
   configuration file.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
   =exited, status=1/FAILURE

Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
<!--NeedCopy-->
```

Sie lösen das Problem, indem Sie `setlog` als Root-Benutzer ausführen, um die Datei **/var/xdl/.ctxlog** neu zu erstellen. Starten Sie dann den `ctxlogd`-Dienst neu, da andere Dienste von ihm abhängen.

Konfigurieren nicht authentifizierter Sitzungen

April 18, 2024

Dieser Abschnitt enthält Informationen zum Konfigurieren nicht authentifizierter Sitzungen. Es sind keine besonderen Einstellungen erforderlich, wenn der Linux VDA zur Verwendung dieses Features installiert wird.

> **Hinweis:**
>
> Berücksichtigen Sie beim Konfigurieren nicht authentifizierter Sitzungen, dass der Sitzungsvorabstart nicht unterstützt wird. Der Sitzungsvorabstart wird außerdem nicht von der Citrix Receiver für Android unterstützt.

Erstellen eines Stores ohne Authentifizierung

Sie müssen mit StoreFront einen Store ohne Authentifizierung erstellen, um nicht authentifizierte Sitzungen auf dem Linux VDA zu ermöglichen.

Zulassen nicht authentifizierter Benutzer in einer Bereitstellungsgruppe

Nach dem Erstellen eines Stores ohne Authentifizierung lassen Sie nicht authentifizierte Benutzer in einer Bereitstellungsgruppe zu, um nicht authentifizierte Sitzungen zu ermöglichen. Um nicht authentifizierte Benutzer in einer Bereitstellungsgruppe zu ermöglichen, folgen Sie den Anweisungen in der XenApp und XenDesktop-Dokumentation.

Festlegen der Leerlaufzeit für nicht authentifizierte Sitzungen

Für nicht authentifizierte Sitzungen gilt ein Standardleerlauftimeout von 10 Minuten. Dieser Wert wird über die Registrierungseinstellung **AnonymousUserIdleTime** festgelegt. Verwenden Sie das Tool **ctxreg**, um diesen Wert zu ändern. Wenn Sie beispielsweise fünf Minuten festlegen möchten:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k  "HKLM\System\
     CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime  -d 0
     x00000005
2 <!--NeedCopy-->
```

Festlegen der maximalen Anzahl nicht authentifizierter Benutzer

Zum Festlegen der maximalen Anzahl nicht authentifizierter Benutzer verwenden Sie den Registrierungsschlüssel **MaxAnonymousUserNumber**. Mit dieser Einstellung wird die Anzahl gleichzeit-

iger nicht authentifizierter Sitzungen auf einem Linux VDA beschränkt. Verwenden Sie das Tool **ctxreg**, um diese Registrierungseinstellung zu konfigurieren. Wenn Sie beispielsweise einen Wert von 32 festlegen möchten:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
    CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
    x00000020
<!--NeedCopy-->
```

> **Wichtig:**
>
> Begrenzen Sie die Anzahl nicht authentifizierter Sitzungen. Wenn zu viele Sitzungen gleichzeitig gestartet werden, können Probleme auf dem VDA (z. B. Arbeitsspeichermangel) auftreten.

Problembehandlung

Berücksichtigen Sie beim Konfigurieren authentifizierter Sitzungen Folgendes:

- **Fehler beim Anmelden bei einer nicht authentifizierten Sitzung.**

Prüfen Sie, ob die Registrierung mit folgendem Parameter (Einstellung auf 0) aktualisiert wurde:

```
sudo /opt/Citrix/VDA/bin/ctxreg read –k "HKLM\System\CurrentControlSet
    \Control\Citrix" –v MaxAnonymousUserNumber
<!--NeedCopy-->
```

Prüfen Sie, ob der Dienst **ncsd** ausgeführt wird und die Kennwortzwischenspeicherung **passwd** zulässt:

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
<!--NeedCopy-->
```

Legen Sie die Cachevariable **passwd** auf **no** fest, wenn diese aktiviert ist, und starten Sie den Dienst **ncsd** neu. Nach dem Ändern dieser Konfiguration müssen Sie möglicherweise den Linux VDA neu installieren.

- **Schaltfläche zum Sperren des Bildschirms wird in nicht authentifizierter Sitzung mit KDE angezeigt**.

Die Schaltfläche und das Menü zum Sperren des Bildschirms sind in nicht authentifizierten Sitzungen standardmäßig deaktiviert. Sie werden jedoch ggf. weiterhin in KDE angezeigt. Zum Deaktivieren der Schaltfläche und des Menüs zum Sperren des Bildschirms in KDE für einen bestimmten Benutzer fügen Sie der Konfigurationsdatei **$Home/.kde/share/config/kdeglobals** die nachfolgend aufgeführten Zeilen hinzu. Beispiel:

```
[KDE Action Restrictions]
```



```
action/lock_screen=false
<!--NeedCopy-->
```

Wenn der Parameter **KDE Action Restrictions** jedoch in einer globalen **kdeglobals**-Datei (z. B. **/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals**) als unveränderlich festgelegt ist, hat die Benutzerkonfiguration keine Auswirkung.

Zum Beheben dieses Problems entfernen Sie entweder das Tag **\$i]** aus dem Abschnitt **[KDE Action Restrictions]** der **kdeglobals**-Datei oder deaktivieren Sie die Schaltfläche und das Menü zum Sperren des Bildschirms direkt über die systemweite Konfiguration. Weitere Informationen zur KDE-Konfiguration finden Sie unter [KDE System Administration/Kiosk/Keys page.

Konfigurieren von LDAPS

November 5, 2021

Mit sicherem LDAP (LDAPS) können Sie das Secure Lightweight Directory Access Protocol für die mit Active Directory verwalteten Domänen aktivieren und die Kommunikation über SSL/TLS (Secure Sockets Layer/Transport Layer Security) ermöglichen.

Standardmäßig wird die LDAP-Kommunikation zwischen Client- und Serveranwendungen nicht verschlüsselt. LDAP mit SSL/TLS (LDAPS) ermöglicht den Schutz des Inhalts von LDAP-Abfragen zwischen Linux VDA- und LDAP-Servern.

Die folgenden Linux VDA-Komponenten benötigen LDAPS:

- Brokeragent: Linux VDA-Registrierung beim Delivery Controller
- Richtliniendienst: Richtlinienbewertung

Die Konfiguration von LDAPS umfasst Folgendes:

- Aktivieren von LDAPS auf dem Active Directory (AD)-/LDAP-Server
- Exportieren der Stammzertifizierungsstelle für Clients
- Aktivieren/Deaktivieren von LDAPS auf dem Linux VDA
- Konfigurieren von LDAPS für Drittanbieter-Plattformen
- Konfigurieren von SSSD
- Konfigurieren von Winbind
- Konfigurieren von Centrify
- Konfigurieren von Quest

Aktivieren von LDAPS auf dem AD-/LDAP-Server

Sie können LDAP über SSL (LDAPS) aktivieren, indem Sie ein ordnungsgemäß formatiertes Zertifikat von einer Microsoft Zertifizierungsstelle (ZS) oder einer anderen Zertifizierungsstelle installieren.

> **Tipp:**
>
> LDAP über SSL/TLS (LDAPS) wird automatisch aktiviert, wenn Sie eine unternehmenseigene Stammzertifizierungsstelle auf einem Domänencontroller installieren.

Weitere Informationen zum Installieren des Zertifikats und Verifizieren der LDAPS-Verbindung finden Sie unter How to enable LDAP over SSL with a third-party certification authority auf der Supportwebsite von Microsoft.

Wenn Sie eine Zertifikatauthentifizierungshierachie mit mehreren Ebenen (zwei oder drei Ebenen) haben, verfügen Sie nicht automatisch über das geeignete Zertifikat für die LDAPS-Authentifizierung auf dem Domänencontroller.

Informationen zum Aktivieren von LDAPS für Domänencontroller über eine Zertifikatauthentifizierungshierachie mit mehreren Ebenen finden Sie im Artikel LDAP over SSL (LDAPS) Certificate auf der Microsoft TechNet-Site.

Aktivieren der Stammzertifizierungsstelle für Clients

Der Client muss ein Zertifikat einer Zertifizierungsstelle verwenden, dem der LDAP-Server vertraut. Importieren Sie das Stammzertifizierungsstellenzertifikat in den vertrauenswürdigen Schlüsselspeicher, um die LDAPS-Authentifizierung für den Client zu aktivieren.

Weitere Informationen zum Exportieren der Stammzertifizierungsstelle finden Sie unter How to export Root Certification Authority Certificate auf der Supportwebsite von Microsoft.

Aktivieren oder Deaktivieren von LDAPS auf dem Linux VDA

Zum Aktivieren oder Deaktivieren von LDAPS für den Linux VDA führen Sie das folgende Skript aus (Sie müssen als Administrator angemeldet sein):

Die Syntax für diesen Befehl enthält Folgendes:

- Aktivieren von LDAP über SSL/TLS mit dem bereitgestellten Stammzertifizierungsstellenzertifikat:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```


- Fallback auf LDAP ohne SSL/TLS

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

Der Java-Schlüsselspeicher für LDAPS ist in **/etc/xdl/.keystore**. Unter anderem sind folgende Registrierungsschlüssel betroffen:

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
<!--NeedCopy-->
```

Konfigurieren von LDAPS für Drittanbieter-Plattformen

Neben Linux VDA-Komponenten gibt es verschiedene Softwarekomponenten von Drittanbietern, die mit dem Linux VDA verbunden sind und ebenfalls sicheres LDAP erfordern, z. B. SSSD, Winbind, Centrify und Quest. In den folgenden Abschnitten wird beschrieben, wie Sie sicheres LDAP mit LDAPS, STARTTLS oder SASL Sign and Seal konfigurieren.

> **Tipp:**
>
> Nicht alle diese Softwarekomponenten nutzen den SSL-Port 636 für sicheres LDAP. Außerdem kann LDAPS (LDAP über SSL auf Port 636) meist nicht gemeinsam mit STARTTLS auf Port 389 verwendet werden.

SSSD

Konfigurieren Sie den sicheren LDAP-Datenverkehr mit SSSD auf Port 636 oder 389 entsprechend den Optionen. Weitere Informationen finden Sie hier: SSSD LDAP Linux man page.

Winbind

Die Winbind LDAP-Abfrage verwendet die ADS-Methode. Winbind unterstützt nur die StartTLS-Methode auf Port 389. Die Konfigurationsdateien **ldap.conf** and **smb.conf** sind betroffen. Nehmen Sie an den Dateien die folgenden Änderungen vor:

```
ldap.conf:

TLS_REQCERT never

```



```
smb.conf:

ldap ssl = start tls

ldap ssl ads = yes

client ldap sasl wrapping = plain
<!--NeedCopy-->
```

Alternativ kann sicheres LDAP mit SASL GSSAPI Sign and Seal konfiguriert werden, es kann jedoch nicht neben TLS/SSL existieren. Um SASL-Verschlüsselung zu verwenden, ändern Sie die Konfiguration für **smb.conf**:

```
smb.conf:

ldap ssl = off

ldap ssl ads = no

client ldap sasl wrapping = seal
<!--NeedCopy-->
```

Centrify

Centrify unterstützt LDAPS auf Port 636 nicht. Es bietet jedoch sichere Verschlüsselung auf Port 389. Weitere Informationen finden Sie auf der Website von Centrify.

Quest

Quest Authentication Services unterstützt LDAPS auf Port 636 nicht, bietet jedoch mit einer anderen Methode sichere Verschlüsselung auf Port 389.

Problembehandlung

Folgende Probleme können bei der Verwendung dieses Features auftreten:

- **Verfügbarkeit des LDAPS-Diensts**

  Stellen Sie sicher, dass die LDAPS-Verbindung auf dem AD/LDAP-Server verfügbar ist. Der Port ist standardmäßig 636.

- **Registrierung des Linux VDA schlägt fehl, wenn LDAPS aktiviert ist**

  Überprüfen Sie, ob der LDAP-Server und die Ports richtig konfiguriert sind. Überprüfen Sie zuerst das Stammzertifizierungsstellenzertifikat und stellen Sie sicher, dass es mit dem AD/LDAP-Server übereinstimmt.

- **Versehentlich vorgenommene falsche Registrierungsänderung**

  Wenn die LDAPS-bezogenen Schlüssel versehentlich ohne **enable_ldaps.sh** aktualisiert wurden, wird u. U. die Abhängigkeit der LDAPS-Komponenten unterbrochen.

- **LDAP-Datenverkehr wird nicht durch SSL/TLS von Wireshark oder anderen Netzwerküberwachungs-Tools verschlüsselt.**

  LDAPS ist standardmäßig deaktiviert. Führen Sie **/opt/Citrix/VDA/sbin/enable_ldaps.sh** aus, um die Aktivierung zu erzwingen.

- **Kein LDAPS-Datenverkehr von Wireshark oder einem anderen Netzwerküberwachungstool**

  Bei der Linux VDA-Registrierung und Gruppenrichtlinienbewertung erfolgt LDAP/LDAPS-Datenverkehr.

- **LDAPS-Verfügbarkeit konnte durch Ausführen von "ldp connect"auf dem AD-Server nicht verifiziert werden**

  Verwenden Sie den AD FQDN statt der IP-Adresse.

- **Stammzertifizierungsstellenzertifikat konnte nicht durch Ausführen des Skripts /opt/Citrix/VDA/sbin/enable_ldaps.sh importiert werden**

  Geben Sie den vollständigen Pfad des Zertifizierungsstellenzertifikats an und prüfen Sie den Typ des Stammzertifizierungsstellenzertifikats. Er sollte mit den meisten unterstützten Java Keytool-Typen kompatibel sein. Wenn er nicht in der Liste der unterstützten Typen enthalten ist, können Sie ihn konvertieren. Citrix empfiehlt das mit base64 verschlüsselte PEM-Format, wenn ein Problem mit dem Zertifikatformat auftritt.

- **Stammzertifizierungsstellenzertifikat wird mit Keytool -list nicht angezeigt**

  Wenn Sie LDAPS durch Ausführen von **/opt/Citrix/VDA/sbin/enable_ldaps.sh** aktivieren, wird das Zertifikat nach "/etc/xdl/.keystore"importiert und ein Kennwort wird zum Schutz des Schlüsselspeichers eingerichtet. Wenn Sie das Kennwort vergessen, können Sie das Skript erneut ausführen und einen Schlüsselspeicher erstellen.

Konfigurieren von Xauthority

November 5, 2021

Der Linux VDA unterstützt Umgebungen, in denen X11-Anzeigefunktionalität (einschließlich `xterm` und `gvim`) für interaktives Remoting verwendet wird. Dieses Feature bietet einen Sicherheitsmechanismus für die sichere Kommunikation zwischen XClient und XServer.

Es gibt zwei Methoden zum Sicherstellen der Berechtigung für die sichere Kommunikation:

- **Xhost**. Standardmäßig erlaubt Xhost nur die Kommunikation zwischen dem XClient auf Localhost und XServer. Wenn Sie den Zugriff eines Remote-XClient auf XServer zulassen, muss mit dem Xhost-Befehl die Berechtigung für die spezifische Maschine gewährt werden. Alternativ dazu können Sie auch **xhost +** verwenden, um damit alle XClient-Instanzen eine Verbindung zu XServer herstellen können.
- **Xauthority**. Die `.Xauthority`-Datei ist im Homeverzeichnis von Benutzern. Sie wird zum Speichern von Anmeldeinformationen in Cookies verwendet, die von xauth für die Authentifizierung von XServer verwendet werden. Wenn eine XServer-Instanz (Xorg) gestartet wird, werden Verbindungen mit dem Cookie bei der spezifischen Anzeige authentifiziert.

Funktionsweise

Wenn Xorg gestartet wird, wird eine `.Xauthority`-Datei an Xorg übergeben. Diese `.Xauthority` -Datei enthält folgende Elemente:

- Anzeigenummer
- Remoteanfrageprotokoll
- Cookienummer

Sie können diese Datei mit dem Befehl **xauth** durchsuchen. Beispiel:

```
# xauth -f ~/.Xauthority

# > list

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

Wenn XClient eine Remoteverbindung mit Xorg herstellt, müssen zwei Voraussetzungen erfüllt sein:

- Die Umgebungsvariable **DISPLAY** muss auf den Remote-XServer festgelegt sein.
- Rufen Sie die `.Xauthority`-Datei ab, die eine der Cookienummern in Xorg enthält.

Konfigurieren von Xauthority

Um Xauthority im Linux VDA für X11-Remoteanzeige zu aktivieren, müssen Sie die zwei folgenden Registrierungsschlüssel erstellen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
   XauthEnabled" -d "0x00000001" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
    -d "0x00000001" --force
```



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

Übergeben Sie nach dem Aktivieren von Xauthority die `.Xauthority`-Datei manuell oder über ein freigegebenes Homeverzeichnis an den XClient:

- Manuelle Übergabe der `.Xauthority`-Datei an den XClient

  Nach dem Starten einer ICA-Sitzung generiert der Linux VDA die `.Xauthority`-Datei für den XClient und speichert die Datei im Homeverzeichnis des angemeldeten Benutzers. Sie können die `.Xauthority`-Datei auf die XClient-Remotemaschine kopieren und die Umgebungsvariablen DISPLAY und XAUTHORITY festlegen.DISPLAY ist die in der `.Xauthority`-Datei gespeicherte Anzeigenummer und XAUTHORITY ist der Dateipfad von Xauthority. Ein Beispiel ist der folgende Befehl:

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


  export XAUTHORITY={
  the file path of .Xauthority }

  <!--NeedCopy-->
  ```

  > **Hinweis:**
  >
  > Wenn die Umgebungsvariable `XAUTHORITY` nicht festgelegt ist, wird standardmäßig die Datei `~/.Xauthority` verwendet.

- Übergabe der `.Xauthority`-Datei über ein freigegebenes Homeverzeichnis an den XClient

  Eine bequeme Methode ist das Bereitstellen eines freigegebenen Homeverzeichnisses für den Benutzer, der sich anmeldet. Wenn der Linux VDA eine ICA-Sitzung startet, wird die `.Xauthority`-Datei im Homeverzeichnis des angemeldeten Benutzers erstellt. Wenn dieses Homeverzeichnis für den XClient freigegeben wird, braucht der Benutzer die `.Xauthority` -Datei nicht manuell an den XClient zu übertragen. Wenn die Umgebungsvariablen DISPLAY und XAUTHORITY richtig festgelegt sind, wird die GUI automatisch auf dem XServer-Desktop angezeigt.

Problembehandlung

Wenn Xauthority nicht funktioniert, folgen Sie diesen Anleitungen zur Problembehandlung:

1. Rufen Sie als Administrator mit Root-Privilegien alle Xorg-Cookies ab:

   ```
   ps aux | grep -i xorg
   <!--NeedCopy-->
   ```


Mit diesem Befehl wird der Xorg-Prozess angezeigt sowie die Parameter, die beim Starten an Xorg übergeben wurden. Ein weiterer Parameter zeigt an, welche `.Xauthority`-Datei verwendet wurde. Beispiel:

```
/var/xdl/xauth/.Xauthority110
<!--NeedCopy-->
```

Zeigen Sie Cookies mit dem Befehl **Xauth** an:

```
Xauth -f /var/xdl/xauth/.Xauthority110
<!--NeedCopy-->
```

2. Zeigen Sie mit dem Befehl **Xauth** die in `~/.Xauthority` enthaltenen Cookies an. Für eine bestimmte Anzeigenummer müssen die angezeigten Cookies in den `.Xauthority`-Dateien von Xorg und XClient dieselben sein.
3. Wenn die Cookies dieselben sind, überprüfen Sie den Zugriff auf den Remoteanzeigeport mit der IP-Adresse des Linux VDA (z. B. 10.158.11.11) und der Anzeigenummer des veröffentlichten Desktops (z. B. 160).

   Führen Sie folgenden Befehl auf der XClient-Maschine aus:

   ```
   telnet 10.158.11.11 6160
   <!--NeedCopy-->
   ```

   Die Portnummer ist die Summe von 6000 + <display number>.

   Wenn dieser Telnet-Vorgang fehlschlägt, wird die Anfrage möglicherweise von der Firewall blockiert.