



Linux Virtual Delivery Agent 2207

Contents

Linux Virtual Delivery Agent 2207	5
Was ist neu	5
Behobene Probleme	6
Bekannte Probleme	6
Hinweise zu Drittanbietern	8
Einstellung von Features und Plattformen	8
Systemanforderungen	10
Installationsübersicht	14
Schnelle Installation mit Easy Install (empfohlen)	15
Manuelle Installation von Linux Virtual Delivery Agent für Amazon Linux 2, CentOS und RHEL	36
Manuelle Installation von Linux Virtual Delivery Agent für SUSE	74
Manuelle Installation von Linux Virtual Delivery Agent für Ubuntu	104
Manuelle Installation von Linux Virtual Delivery Agent für Debian	137
Linux VDAs in Citrix DaaS Standard für Azure erstellen	169
Erstellen von Linux-VMs mit Maschinenerstellungsdiensten (MCS)	173
Erstellen von Linux-VMs mit Citrix Provisioning	200
Konfigurieren von Delivery Controllern für XenDesktop 7.6 und frühere Versionen	201
Richtlinien- und LDAP-Servereinstellungen	202
Konfigurieren	203
Verwaltung	204
Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)	204
HDX Insight	209

Integration mit dem Citrix Telemetriedienst	210
Linux VDA-Selbstupdate für Citrix DaaS Standard für Azure	214
Metriken für Linux-VM und Linux-Sitzung	218
Protokollsammlung	226
Sitzungsspiegelung	230
Monitor Service Daemon	237
Tools und Hilfsprogramme	239
Sonstiges	244
Unterstützung für Citrix Workspace-App für HTML5	244
Virtuelle Python3-Umgebung erstellen	245
Integrieren von NIS in Active Directory	248
IPv6	253
LDAPS	255
Xauthority	260
Authentifizierung	263
Authentifizierung mit Azure Active Directory	263
Single-Sign-On-Authentifizierung per Double-Hop	268
Verbundauthentifizierungsdienst	271
Authentifizierung ohne Single Sign-On	280
Smartcards	281
Nicht authentifizierte Sitzungen mit anonymen Benutzern	292
Datei	295
Kopieren und Einfügen von Dateien	295
Dateiübertragung	296

Grafik	301
Automatische DPI-Skalierung	301
Clientakkustatusanzeige	302
Grafikkonfiguration und -feineinstellung	306
HDX-Bildschirmfreigabe	318
Nicht-vGPU-Grafikkarten	328
Sitzungswasserzeichen	331
Progressive Anzeige für Thinwire	336
Tastatur	338
Client-Eingabemethoden-Editor (IME)	339
Synchronisierung der Client-IME-Benutzeroberfläche	340
Dynamische Tastaturlayoutsynchronisierung	344
Bildschirmtastatur	348
Unterstützung der Eingabe in mehreren Sprachen	351
Multimedia	353
Audiofeatures	353
Browserinhaltsumleitung	354
HDX-Webcamvideokomprimierung	360
Nicht in Domänen eingebundene VDAs	366
Liste der unterstützten Richtlinien	368
Drucken	383
Bewährte Methoden beim Drucken	383
PDF-Druck	390
Remote-PC-Zugriff	391

Sitzungsfortbestehen	405
Adaptiver Transport	405
Benutzerdefinierte Hintergründe und Bannermeldungen auf Anmeldebildschirmen	408
Anmeldung mit einem temporären Basisverzeichnis	409
Veröffentlichen von Anwendungen	411
Rendezvous V1	412
Rendezvous V2	416
Sichere Benutzersitzungen mit DTLS	419
Sichere Benutzersitzungen mit TLS	420
Sitzungszuverlässigkeit	424
USB-Umleitung	426
Virtual Channel SDK (experimentell)	434

Linux Virtual Delivery Agent 2207

October 5, 2022

Wichtig:

Informationen zur Produktlebenszyklusstrategie für aktuelle Releases (CR) und Long Term Service Releases (LTSR) finden Sie unter [Lifecycle Milestones](#).

Der Linux Virtual Delivery Agent (VDA) ermöglicht den Zugriff auf virtuelle Linux-Desktops und -Anwendungen auf jedem Gerät, auf dem die Citrix Workspace-App installiert ist.

Sie können virtuelle Apps und Desktops auf der Basis [unterstützter Linux-Distributionen](#) bereitstellen. Installieren Sie die VDA-Software auf den virtuellen Linux-Maschinen, konfigurieren Sie den Delivery Controller und stellen Sie die Apps und Desktops den Benutzern mit Citrix Studio zur Verfügung.

Was ist neu

October 5, 2022

Neue Features in Release 2207

Version 2207 des Linux VDA enthält die folgenden neuen und erweiterten Features:

Unterstützung für zusätzliche Benutzerauthentifizierungsmethoden in Szenarien ohne Single Sign-On

Bisher konnten sich Benutzer bei deaktiviertem Single Sign-On bei der Citrix Workspace-App und bei Sitzungen mit unterschiedlichen Benutzernamen anmelden. Ab diesem Release können sich die Benutzer mit Benutzernamen oder Smartcards anmelden. Weitere Informationen finden Sie unter [Authentifizierung ohne Single Sign-On](#).

Zusätzliche Optionen zum Konfigurieren des Sitzungswasserzeichens

Die Richtlinie **Benutzerdefinierter Wasserzeichentext** bietet neue Optionen, mit denen Sie Sitzungswasserzeichen weiter anpassen können. Beispielsweise können Sie **Benutzerdefinierter Wasserzeichentext** auf **<image=Pfad zu einem PNG-Bild auf dem VDA>** festlegen, um ein PNG-Wasserzeichen zu erstellen. Weitere Informationen finden Sie unter [Sitzungswasserzeichen](#).

Unterstützung für KVM-Hypervisor

Kernel-based Virtual Machine (KVM) ist die führende Open-Source-Virtualisierungstechnologie für Linux. Sie gehört zu Linux und ermöglicht die Umwandlung von Linux-Maschinen in Hypervisoren, sodass sie mehrere isolierte virtuelle Maschinen hosten können. Der Linux VDA funktioniert ordnungsgemäß auf KVM-Hypervisoren. KVM-Hypervisoren werden jedoch nicht für die Verwendung mit MCS zum Erstellen virtueller Maschinen unterstützt.

Kopieren und Einfügen von Dateien für alle unterstützten Linux-Distributionen verfügbar

Bisher war das **Feature zum Kopieren und Einfügen von Dateien** nur für Debian 10, RHEL 7.9 und Ubuntu 18.04 verfügbar. Ab dieser Version ist es für alle Linux-Distributionen verfügbar, die der Linux VDA unterstützt. Weitere Informationen finden Sie unter [Kopieren und Einfügen von Dateien](#).

Neue Features in früheren Releases

Informationen zu neuen Features in den Releases, die nach 1912 LTSR bis zu 2206 CR ausgeliefert wurden, finden Sie unter [Neue Features –Archiv](#).

Behobene Probleme

October 5, 2022

Für Linux Virtual Delivery Agent 2207 gibt über die Fixes von Linux Virtual Delivery Agent 2206 hinaus keine weiteren Fixes.

Bekannte Probleme

July 17, 2023

Die folgenden Probleme wurden in diesem Release identifiziert:

- Die Registrierung von Linux-VDAs wird möglicherweise aufgehoben, wenn Sie den Cloud Connector oder den Delivery Controller neu starten. [CVADHELP-21256]
- Der Linux VDA unterstützt keine SecureICA-Verschlüsselung. Wenn SecureICA auf dem Linux VDA aktiviert ist, führt dies zu einem Sitzungsstartfehler.

- In einer GNOME-Desktopsitzung schlagen Versuche, das Tastaturlayout zu ändern, möglicherweise fehl. [CVADHELP-15639]
- Veröffentlichte Nicht-Seamlessanwendungen können kurz nach dem Start beendet werden. Das Problem tritt nach einem Mutter-Upgrade auf eine Version nach mutter-3.28.3-4 auf. Um das Problem zu umgehen, verwenden Sie mutter-3.28.3-4 oder früher. [LNXVDA-6967]
- Beim Dateidownload wird unerwartet ein Fenster angezeigt. Das Fenster hat keine Auswirkungen auf die Dateidownloadfunktion und wird nach einiger Zeit automatisch ausgeblendet. [LNXVDA-5646]
- Die Standardeinstellungen von PulseAudio bewirken, dass das Soundserverprogramm nach 20 Sekunden Inaktivität beendet wird. Wenn PulseAudio beendet wird, funktioniert das Audio nicht. Als Workaround setzen Sie `exit-idle-time=-1` in der Datei `/etc/pulse/daemon.conf`. [LNXVDA-5464]
- Wenn die SSL-Verschlüsselung aktiviert und die Sitzungszuverlässigkeit deaktiviert ist, können keine Sitzungen in der Citrix Workspace-App für Linux gestartet werden. [RFLNX-1557]
- 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 der Citrix Workspace-App für Android kann beim Sitzungsroaming umgekehrt werden. Der Status der Feststelltaste kann aufgehoben werden, wenn über eine vorhandene Verbindung Roaming zu Citrix Workspace-App 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 der Citrix Workspace-App für Mac eine Verbindung zu einem Linux VDA herstellen. Citrix Workspace-App für Mac sendet standardmäßig für die linke und die rechte Alt-Taste den Befehl "Alt Gr". Sie können dieses Verhalten in den Einstellungen für die Citrix Workspace-App 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:

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

Mit diesem Befehl werden alle Diensttickets im LSA-Cache des Netzwerkdienstprinzips 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.
- Mit der Citrix Workspace-App für Windows können während der Aufzeichnung Audiostörungen auftreten.

Hinweise zu Drittanbietern

December 9, 2022

[Linux Virtual Delivery Agent Version 2207](#) (PDF-Download)

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

Einstellung von Features und Plattformen

October 5, 2022

Die Ankündigungen in diesem Artikel bieten Ihnen frühzeitige Informationen über Plattformen, Citrix Produkte und Features, die ausgemustert werden, sodass Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element.

Informationen zum Produktlebenszyklussupport finden Sie im Artikel [Product Lifecycle Support Policy](#).

Veraltete und entfernte Produkte und Features

Die in der folgenden Tabelle aufgeführten Plattformen, Citrix Produkte und Features sind veraltet oder wurden entfernt:

Veraltete Elemente werden nicht sofort entfernt. Der Support von Citrix wird in dieser Version fortgesetzt. In einer zukünftigen Version werden sie entfernt werden.

Entfernte Elemente wurden entfernt oder werden in Linux VDA nicht mehr unterstützt.

Element	Einstellung der Unterstützung angekündigt in	Entfernt in
Unterstützung für Debian 10.9	2206	2210
Unterstützung für SUSE 15.2	2206	2209
Unterstützung für RHEL 8.2	2206	2209
Unterstützung für RHEL 8.1, RHEL 8.3	2203	2206
Unterstützung für RHEL 7.8, CentOS 7.8	2203	2204
Unterstützung für CentOS 8.x	2110	2201
Unterstützung für SUSE 12.5	2109	2204
Unterstützung für Ubuntu 16.04	2109	2203
Unterstützung für RHEL 7.7, CentOS 7.7	2006	2009
Unterstützung für SUSE 12.3	2006	2006
Unterstützung für RHEL 6.10, CentOS 6.10	2003	2003
Unterstützung für RHEL 6.9, CentOS 6.9	1909	1909
Unterstützung für RHEL 7.5, CentOS 7.5	1903	1903

Element	Einstellung der Unterstützung angekündigt	
	in	Entfernt in
Unterstützung für RHEL 7.4, CentOS 7.4	1811	1811
Unterstützung für RHEL 6.8, CentOS 6.8	1811	1811
Unterstützung für RHEL 7.3, CentOS 7.3	7.18	7.18
Unterstützung für RHEL 6.6, CentOS 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

Systemanforderungen

November 2, 2022

Das aktuelle Release von Linux VDA ist mit Citrix Virtual Apps and Desktops abgestimmt. Es ist auch abwärtskompatibel mit früheren Versionen von Citrix Virtual Apps and Desktops, die das Ende ihres Lebenszyklus noch nicht erreicht haben. Weitere Informationen zum Citrix 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 Windows- und Linux-Desktops vermitteln.

Die Systemanforderungen für Komponenten, die hier nicht behandelt werden (z. B. die Citrix Workspace-App), werden in der jeweiligen Dokumentation beschrieben.

Informationen zur Verwendung einer aktuellen Version (CR) in einer LTSR-Umgebung (Long Term Service Release) und zu anderen häufig gestellten Fragen finden Sie im [Knowledge Center-Artikel](#).

Linux-Distributionen

Folgende Linux-Distributionen werden vom Linux VDA unterstützt:

Wichtig:

Wenn Ihr Betriebssystem vom Hersteller nicht mehr unterstützt wird, kann Citrix Probleme

möglicherweise nur noch eingeschränkt beheben.

Informationen zu veralteten oder entfernten Plattformen finden Sie unter [Einstellung von Features und Plattformen](#).

- Amazon Linux
 - Amazon Linux 2
- CentOS Linux
 - CentOS 7.9
- Debian Linux
 - Debian 11.3
 - Debian 10.9
- Red Hat Enterprise Linux
 - Workstation 8.4
 - Workstation 8.2
 - Workstation 7.9
 - Server 8.4
 - Server 8.2
 - Server 7.9
- SUSE Linux Enterprise:
 - Server 15 Service Pack 3
 - Server 15 Service Pack 2
- Ubuntu Linux
 - Ubuntu Desktop 20.04
 - Ubuntu Server 20.04
 - Ubuntu Desktop 18.04
 - Ubuntu Server 18.04
 - Ubuntu Live Server 18.04

Hinweis:

Das CentOS-Projekt verlagert den Fokus auf CentOS Stream. CentOS Linux 8 endet als Rebuild von RHEL 8 Ende 2021. CentOS Stream wird nach diesem Datum als Upstream- (Entwicklungs-)Zweig von Red Hat Enterprise Linux fortgesetzt. Weitere Informationen finden Sie unter <https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux>.

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	Unterstützter Desktop
Amazon Linux 2	1.20	MATE, GNOME, GNOME Classic
Debian 11.3, Debian 10.9	1.20	MATE, GNOME, GNOME Classic
RHEL 8.4, RHEL 8.2	= 1.20.8	MATE, GNOME, GNOME Classic, KDE
RHEL 7.9, CentOS 7.9		MATE, GNOME, GNOME Classic, KDE
SUSE 15.3, SUSE 15.2	1.20	MATE, GNOME, GNOME Classic
Ubuntu 20.04	1.20	MATE, GNOME, GNOME Classic
Ubuntu 18.04	1.19	MATE, GNOME, GNOME Classic

Tipp:

Verwenden Sie [HWE kernel](#) oder [HWE Xorg](#) nicht unter Ubuntu.

Mindestens ein Desktop muss installiert sein. Sie können mit dem Skript `ctxinstall.sh` oder `ctxsetup.sh` die GNOME- oder MATE-Desktopumgebung angeben, die in Sitzungen verwendet werden soll.

Ihr Benutzernamensformat muss den [systemd](#)-Syntaxregeln für Ihren aktuellen Displaymanager entsprechen. Weitere Hinweise zur [systemd](#)-Benutzernamenssyntax finden Sie unter [User/Group Name Syntax](#).

Unterstützte Hostplattformen und Virtualisierungsumgebungen

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

Hinweis:

In allen Fällen wird die Prozessorarchitektur x86-64 unterstützt.

Von Citrix Virtual Apps and Desktops 7 2003 bis 2112 wurde das Hosten des Linux VDA auf Mi-

icrosoft Azure, AWS und GCP nur für Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) unterstützt. Ab Release 2203 können Sie den Linux VDA auf diesen öffentlichen Clouds sowohl für Citrix DaaS als auch für Citrix Virtual Apps and Desktops hosten. Um diese Verbindungen mit Hosts öffentlicher Clouds zu Ihrer Citrix Virtual Apps and Desktops-Bereitstellung hinzuzufügen, benötigen Sie eine **Hybrid Rights-Lizenz**. Weitere Informationen zu **Hybrid Rights-Lizenzen** finden Sie unter [Übergang und Trade-Up \(TTU\) mit Hybrid Rights](#).

Active Directory-Integrationspakete

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

	Winbind	SSSD	Centrify	PBIS	Quest
Amazon Linux 2	Ja	Ja	Ja	Ja	Nein
Debian 11.3	Ja	Ja	Ja	Ja	Nein
Debian 10.9	Ja	Ja	Ja	Ja	Nein
RHEL 8.4	Ja	Ja	Ja	Ja	Nein
RHEL 8.2	Ja	Ja	Ja	Ja	Nein
RHEL 7.9, CentOS 7.9	Ja	Ja	Ja	Ja	Ja (Quest v4.1 und höher)
SUSE 15.3	Ja	Ja	Ja	Ja	Nein
SUSE 15.2	Ja	Ja	Ja	Ja	Nein
Ubuntu 20.04	Ja	Ja	Ja	Ja	Ja (Quest v4.1 und höher)
Ubuntu 18.04	Ja	Ja	Ja	Ja	Ja (Quest v4.1 und höher)

HDX 3D Pro

Mit HDX 3D Pro von Citrix Virtual Apps and Desktops können Desktops und Anwendungen bereitgestellt werden, die mit einem Grafikprozessor (GPU) für die Hardwarebeschleunigung am besten funktionieren.

Hypervisors

Für den Linux VDA ist HDX 3D Pro mit den folgenden Hypervisoren kompatibel:

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

Hinweis:

Die Hypervisoren sind mit bestimmten Linux-Distributionen kompatibel.

Um HDX 3D Pro für Amazon Linux 2 zu verwenden, empfehlen wir die Installation des NVIDIA-Treibers 470.

GPUs

Um zu erfahren, welche NVIDIA-GPU-Karten von Ihrer Linux-Distribution unterstützt werden, rufen Sie die [NVIDIA-Produktsupportmatrix](#) auf und überprüfen Sie die Spalten **Hypervisor or Bare-Metal OS**, **Software Product Deployment**, **Hardware Supported** und **Guest OS Support**.

Stellen Sie sicher, dass Sie den neuesten vGPU-Treiber für Ihre GPU-Karte installiert haben. Derzeit unterstützt der Linux VDA bis zu vGPU 13. Weitere Informationen finden Sie unter [NVIDIA Virtual GPU Software Supported GPUs](#).

Installationsübersicht

October 5, 2022

Dieser Abschnitt erläutert die folgenden Verfahren:

- Schnelle Installation mit Easy Install (empfohlen bei Neuinstallationen)
- Manuelle Installation auf der Basis verschiedener Linux-Distributionen
- Verwenden von MCS zum Erstellen von Linux-VMs
- Erstellen von in Domänen eingebundenen und nicht eingebundenen Linux VDAs in Citrix DaaS Standard für Azure (früher Citrix Virtual Apps and Desktops Standard für Azure)
- Erstellen von Linux-VMs mit Citrix Provisioning
- Konfigurieren von Delivery Controllern für XenDesktop 7.6 und frühere Versionen

Schnelle Installation mit Easy Install (empfohlen)

October 5, 2022

Wichtig:

- Bei Neuinstallationen wird dieser Artikel für eine schnelle Installation empfohlen. Der Artikel beschreibt die einzelnen Schritte zum Installieren und Konfigurieren des Linux VDA mit Easy Install. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als eine manuelle Installation. Sie können hiermit eine Umgebung zum Ausführen des Linux VDA einrichten, wobei die erforderlichen Pakete automatisch installiert und die Konfigurationsdateien automatisch angepasst werden.
- Um nicht in Domänen eingebundene VDAs zu erstellen, müssen Sie Maschinenerstellungsdienste (MCS) verwenden. Weitere Informationen finden Sie unter [Erstellen von Linux-VMs mit Maschinenerstellungsdiensten \(MCS\)](#).
- Weitere Informationen zu Features, die für nicht in Domänen eingebundene VDAs verfügbar sind, finden Sie unter [Nicht in Domänen eingebundene VDAs](#).

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 NetBIOS-Name der Domäne
- Bereichsname: Der Kerberos-Bereichsname
- Vollqualifizierter Domänenname (FQDN) der Domäne

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.

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 und speichern Sie die Änderung.
- Centrifry unterstützt keine reine IPv6-DNS-Konfiguration. Es ist mindestens ein DNS-Server mit IPv4 in /etc/resolv.conf für **adcli** erforderlich, damit die AD-Dienste ordnungsgemäß gefunden werden.

Protokoll:

```

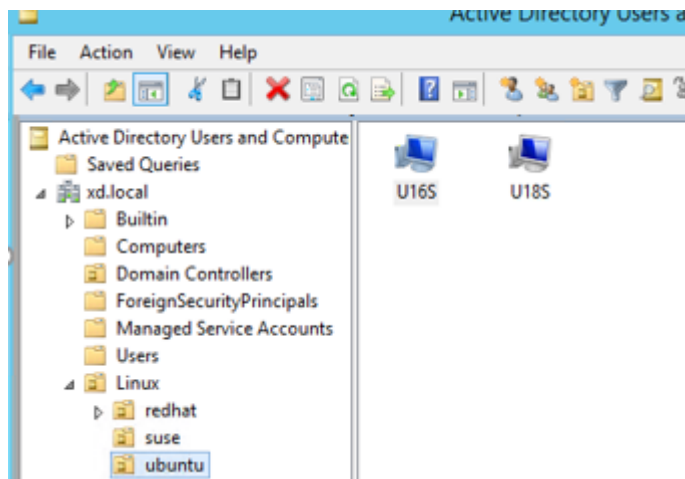
1  ADSITE    : Check that this machine's subnet is in a site known by
      AD      : Failed
2           : This machine's subnet is not known by AD.
3           : We guess you should be in the site Site1.
4  <!--NeedCopy-->

```

Das Problem tritt nur bei Centrifry und dessen Konfiguration auf. Führen Sie folgende Schritte aus, um das Problem zu beheben:

- a. Öffnen Sie **Verwaltungstools** auf dem Domänencontroller.
 - b. Wählen Sie **Active Directory-Standorte und -Dienste** aus.
 - c. Geben Sie in **Subnetze** eine richtige Subnetzadresse ein.
- Gehen Sie folgendermaßen vor, um den VDA einer Organisationseinheit anzufügen:
 1. Stellen Sie sicher, dass die OU auf dem Domänencontroller vorhanden ist.

Ein OU-Beispiel sehen Sie im folgenden Screenshot.



2. Erstellen Sie die Datei /tmp/ctxinstall.conf auf dem VDA.
3. Fügen Sie der Datei /tmp/ctxinstall.conf die Zeile ou=<your ou> hinzu.

OU-Werte variieren je nach AD-Methode. Weitere Informationen bietet die folgende Tabelle.

Betriebssystem	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	<code>ou="Linux/ amazon"</code>	<code>ou="Linux/ amazon"</code>	<code>ou="XD.LOCAL /Linux/ amazon"</code>	<code>ou="Linux/ amazon"</code>
Debian	<code>ou="Linux/ debian"</code>	<code>ou="Linux/ debian"</code>	<code>ou="XD.LOCAL /Linux/ debian"</code>	<code>ou="Linux/ debian"</code>
RHEL 8	<code>ou="OU= redhat,OU= Linux"</code>	<code>ou="OU= redhat,OU= Linux"</code>	<code>ou="XD.LOCAL /Linux/ redhat"</code>	<code>ou="Linux/ redhat"</code>
RHEL 7	<code>ou="Linux/ redhat"</code>	<code>ou="Linux/ redhat"</code>	<code>ou="XD.LOCAL /Linux/ redhat"</code>	<code>ou="Linux/ redhat"</code>
SUSE	<code>ou="Linux/ suse"</code>	<code>ou="Linux/ suse"</code>	<code>ou="XD.LOCAL /Linux/suse"</code>	<code>ou="Linux/ suse"</code>
Ubuntu	<code>ou="Linux/ ubuntu"</code>	<code>ou="Linux/ ubuntu"</code>	<code>ou="XD.LOCAL /Linux/ ubuntu"</code>	<code>ou="Linux/ ubuntu"</code>

- Easy Install unterstützt reines IPv6 ab Linux VDA 7.16. Es gelten folgende Voraussetzungen und Einschränkungen:
 - Ihr Linux-Repository muss so konfiguriert sein, dass die erforderlichen Pakete über reine IPv6-Netzwerke heruntergeladen werden können.
 - Centrify wird in reinen IPv6-Netzwerken nicht unterstützt.

Hinweis:

Wenn Sie ein reines IPv6-Netzwerk haben und alle Eingaben im richtigen IPv6-Format sind, registriert sich der VDA beim Delivery Controller über IPv6. Bei einem Hybridstack mit IPv4 und IPv6 bestimmt der Typ der ersten DNS-IP-Adresse, ob für die Registrierung IPv4 oder IPv6 verwendet wird.

- 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.centrifys.com/products/centrifys-suite/2016-update-1/installers/centrifys-suite-2016.1-rhel4-x86_64.tgz?_ga=1.178323680.558673738.1478847956

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

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

Ubuntu/Debian: wget https://downloads.centrifys.com/products/infrastructure-services/19.9/centrifys-infrastructure-services-19.9-deb8-x86_64.tgz?_ga=2.151462329.1042350071.1592881996-604509155.1572850145

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

```

1 cat /tmp/ctxinstall.conf
2 set "centrifypkgpath=/home/mydir"
3 ls -ls /home/mydir
4 9548 -r-xr-xr-x. 1 root root 9776688 May 13 2016
   adcheck-rhel4-x86_64
5 4140 -r--r--r--. 1 root root 4236714 Apr 21 2016
   centrifysda-3.3.1-rhel4-x86_64.rpm
6 33492 -r--r--r--. 1 root root 34292673 May 13 2016
   centrifysdc-5.3.1-rhel4-x86_64.rpm
7 4 -rw-rw-r--. 1 root root 1168 Dec 1 2015
   centrifysdc-install.cfg
8 756 -r--r--r--. 1 root root 770991 May 13 2016
   centrifysdc-ldaproxy-5.3.1-rhel4-x86_64.rpm
9 268 -r--r--r--. 1 root root 271296 May 13 2016
   centrifysdc-nis-5.3.1-rhel4-x86_64.rpm
10 1888 -r--r--r--. 1 root root 1930084 Apr 12 2016
   centrifysdc-openssh-7.2p2-5.3.1-rhel4-x86_64.rpm
11 124 -rw-rw-r--. 1 root root 124543 Apr 19 2016
   centrifys-suite.cfg
12 0 lrwxrwxrwx. 1 root root 10 Jul 9 2012 install-
   express.sh -> install.sh
13 332 -r-xr-xr--. 1 root root 338292 Apr 10 2016 install
   .sh
14 12 -r--r--r--. 1 root root 11166 Apr 9 2015 release-
   notes-agent-rhel4-x86_64.txt
15 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-->
```

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

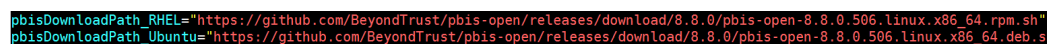
- Mit Easy Install wird das PBIS-Paket automatisch über das Internet heruntergeladen. Dies sind die URLs für die Distributionen:

Amazon Linux 2, CentOS 7, RHEL 8, RHEL 7, SUSE 15.3, SUSE 15.2: `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh`

Debian, Ubuntu: `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh`

- Rufen Sie eine bestimmte Version des PBIS-Pakets im Internet ab. Ändern Sie hierfür die Zeilen “`pbisDownloadRelease`” und “`pbisDownloadExpectedSHA256`” in der Datei `/opt/Citrix/VDA/sbin/ctxinstall.sh`.

Ein Beispiel sehen Sie im folgenden Screenshot:



```
pbisDownloadPath_RHEL="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
pbisDownloadPath_Ubuntu="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
```

Schritt 2: Vorbereiten des Hypervisors

Wenn Sie den Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausführen, sind einige Änderungen erforderlich. Nehmen Sie basierend auf 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 Hypervisor

Wenn das Zeitsynchronisierungsfeature auf Citrix Hypervisor aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme mit NTP und Citrix Hypervisor auf. Beide 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.

Wenn ein paravirtualisierter Linux-Kernel mit installierten Citrix VM Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das Citrix Hypervisor-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/independent_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:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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 Citrix Hypervisor, 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 mit NTP und Hypervisor auf. Beide 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: Installieren von .NET Runtime 6.0 als Voraussetzung

Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Führen Sie nach der Installation von .NET Runtime 6.0 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise `/aa/bb/dotnet` ist, verwenden Sie `/aa/bb` als .NET-Binärpfad.

Schritt 4: Herunterladen des Linux VDA-Pakets

Gehen Sie zur [Citrix Virtual Apps and Desktops-Downloadseite](#). Erweitern Sie die passende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das für Ihre Linux-Distribution geeignete Linux VDA-Paket herunterzuladen.

Schritt 5: Installieren des Linux VDA-Pakets

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

RHEL- und CentOS-Distributionen:

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

Hinweis:

Installieren Sie für RHEL und CentOS das EPEL-Repository, bevor Sie den Linux VDA erfolgreich installieren können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter <https://docs.fedoraproject.org/en-US/epel/>.

Für Ubuntu/Debian-Distributionen:

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

Hinweis:

- Um die notwendigen Abhängigkeiten für eine Distribution mit Debian 11.3 zu installieren, fügen Sie die Zeile `deb http://deb.debian.org/debian/ bullseye main` in der Datei `/etc/apt/sources.list` hinzu.
- Um die notwendigen Abhängigkeiten für eine Distribution mit Debian 10.9 zu installieren, fügen Sie die Zeile `deb http://deb.debian.org/debian/ oldstable main` in der Datei `/etc/apt/sources.list` hinzu.

SUSE-Distributionen:

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

Schritt 6: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro müssen Sie die NVIDIA GRID-Treiber auf Ihrem Hypervisor und auf den VDA-Maschinen installieren.

Informationen zum Installieren und Konfigurieren des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Handbüchern:

- [Citrix Hypervisor](#)
- [VMware ESX](#)
- [Nutanix AHV](#)

Zum Installieren und Konfigurieren der NVIDIA GRID-Gast-VM-Treiber führen Sie die folgenden allgemeinen Schritte aus:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM in der Hypervisor-Systemsteuerung eine GPU zu.
3. Starten Sie die VM.
4. Installieren Sie den Gast-VM-Treiber auf der VM.

Schritt 7: Einrichten der Laufzeitumgebung für die 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.

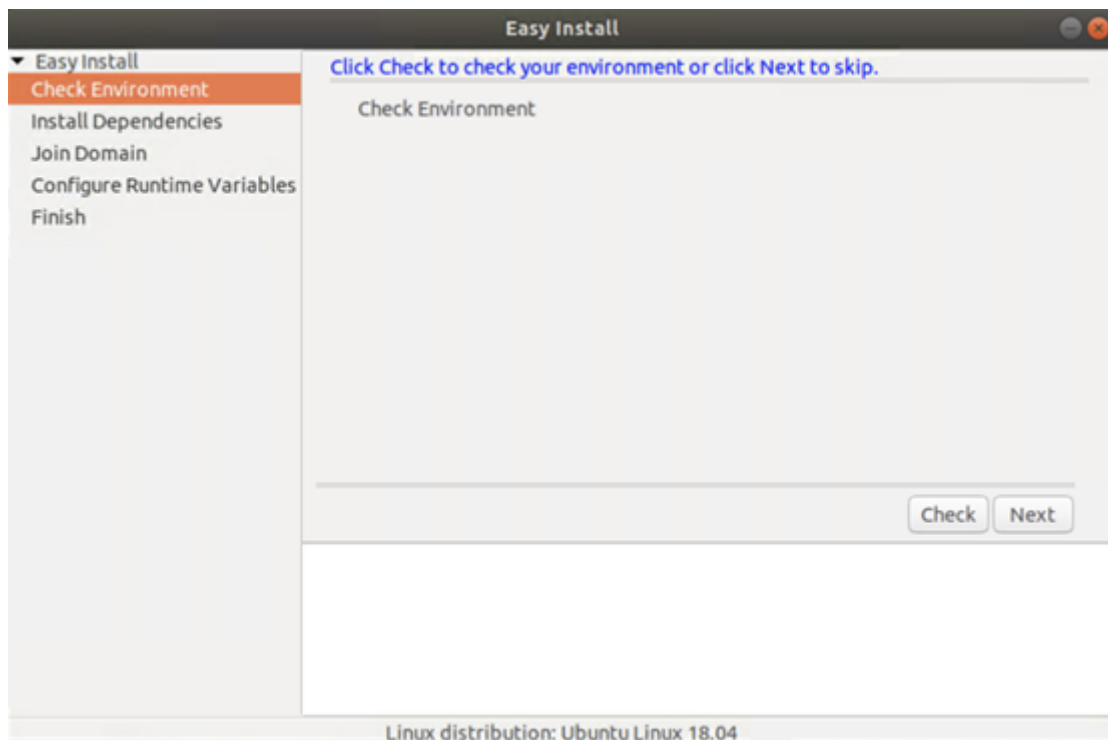
Hinweis:

Stellen Sie vor dem Einrichten der Laufzeitumgebung sicher, dass das Gebietsschema `en_US.UTF-8` in Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema in Ihrem Betriebssystem nicht verfügbar ist, führen Sie den Befehl `sudo locale-gen en_US.UTF-8` aus. Für Debian bearbeiten Sie die Datei `/etc/locale.gen` durch Auskommentierung der Zeile `# en_US.UTF-8 UTF-8`. Führen Sie dann den Befehl `sudo locale-gen` aus.

Interaktiver Modus:

Zum Verwenden von Easy Install im interaktiven Modus gibt es zwei Möglichkeiten:

- Führen Sie den Befehl `sudo /opt/Citrix/VDA/sbin/ctxinstall.sh` aus und geben Sie den entsprechenden Parameter an jeder Eingabeaufforderung in der Befehlszeile ein.
- Führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktopumgebung Ihres VDA aus und folgen Sie dann den Anweisungen in der GUI für Easy Install.



Die GUI für Easy Install führt Sie durch die folgenden Vorgänge:

- Überprüfen der Systemumgebung
- Installieren von Abhängigkeiten
- Mit dem VDA einer bestimmten Domäne beitreten
- Konfigurieren der Laufzeitumgebung

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 | pbis** –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.

ctxsetup.sh verwendet die folgenden Variablen:

- **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 Domännennamen (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 VDA-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, legen Sie **<none>** fest.
- **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 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Wenn Sie die LDAP-Portnummer als 389 angeben, fragt der Linux VDA jeden LDAP-Server in der angegebenen Domäne im Abfragemodus ab. Wenn es x Richtlinien und y Anzahl von LDAP-Servern gibt, führt der Linux VDA die Summe von X multipliziert mit Y-Abfragen aus. Wenn die Abfragezeit den Schwellenwert überschreitet, schlagen Sitzungsanmeldungen möglicherweise fehl. Für schnellere LDAP-Abfragen aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben die entsprechende LDAP-Portnummer als 3268 an. 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). Wenn dies unnötig ist, legen Sie **<none>** fest.
- **CTX_XDL_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. `ctx_xdl_fas_fas_list='FAS_Server_1_URL:Port_Number;fas_server_2_url:port_number;fas_server_3_url:port_number'`.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (**ctxvda**). Der Standardpfad ist `/usr/bin`.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate:** Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

Sie können die Desktopumgebung für Sitzungsbenutzer auch über die folgenden Schritte ändern:

1. Erstellen Sie die Datei `.xsession` oder `.Xclients` auf dem VDA im Verzeichnis **\$HOME/<username>**. Wenn Sie Amazon Linux 2 verwenden, erstellen Sie die Datei `.Xclients`. Wenn Sie andere Distributionen verwenden, erstellen Sie die Datei `.xsession`.
2. Geben Sie in der Datei `.xsession` oder `.Xclients` eine auf Distributionen basierende Desktopumgebung an.

– **MATE-Desktop unter Amazon Linux 2, Debian, RHEL 8, SUSE 15 und Ubuntu**

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

– **Für GNOME Classic-Desktop unter Amazon Linux 2, CentOS, Debian, RHEL, SUSE 15 und Ubuntu**

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

– **Für GNOME-Desktop unter Amazon Linux 2, CentOS, Debian, RHEL, SUSE 15 und Ubuntu**

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

3. Teilen Sie die 700-Dateiberechtigung mit dem Zielsitzungsbenutzer.

- **CTX_XDL_START_SERVICE=Y | N** –Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Konfiguration abgeschlossen ist.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

Wenn ein Parameter nicht festgelegt ist, wird die Installation in den interaktiven Modus versetzt und eine Benutzereingabe ist erforderlich. Selbst wenn alle Parameter bereits über die Umgebungsvariablen festgelegt sind, fordert das Skript `ctxinstall.sh` zur Eingabe des Pfads zur Installation von .NET Runtime 6.0 auf.

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

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



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

Sie müssen die Option -E mit dem Befehl “sudo” angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, 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:

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

```
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \  
12 \  
13 CTX_XDL_HDX_3D_PRO=Y|N \  
14 \  
15 CTX_XDL_VDI_MODE=Y|N \  
16 \  
17 CTX_XDL_SITE_NAME=dns-name \  
18 \  
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \  
20 \  
21 CTX_XDL_SEARCH_BASE=search-base-set \  
22 \  
23 CTX_XDL_FAS_LIST='list-fas-servers' \  
24 \  
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \  
26 \  
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \  
28 \  
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \  
30 \  
31 CTX_XDL_TELEMETRY_PORT=port-number \  
32 \  
33 CTX_XDL_START_SERVICE=Y|N \  
34 \  
35 /opt/Citrix/VDA/sbin/ctxsetup.sh  
36 <!--NeedCopy-->
```

Schritt 8: Ausführen von XDPing

Mit `sudo /opt/Citrix/VDA/bin/xdping` können Sie Linux VDA-Umgebungen auf häufige Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter [XDPing](#).

Schritt 9: Ausführen des Linux VDA

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxhdx start  
2  
3 sudo /sbin/service ctxvda start  
4 <!--NeedCopy-->
```

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda stop  
2
```

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

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl `service ctxmonitorservice stop`, bevor Sie die Dienste `ctxvda` und `ctxhdx` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
6 <!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
4 <!--NeedCopy-->
```

Schritt 10: Erstellen des Maschinenkatalogs in Citrix Virtual Apps oder Citrix Virtual Desktops

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:
 - Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
 - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.

- 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 11: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- 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.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter [Citrix Virtual Apps and Desktops 7 2206](#).

Problembehandlung

Verwenden Sie die Informationen in diesem Abschnitt, um Probleme zu beheben, die sich aus der Verwendung des Features Easy Install 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 Maschine 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 folgende Zeile zu hinzu `/etc/lightdm/lightdm.conf`:
`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-->

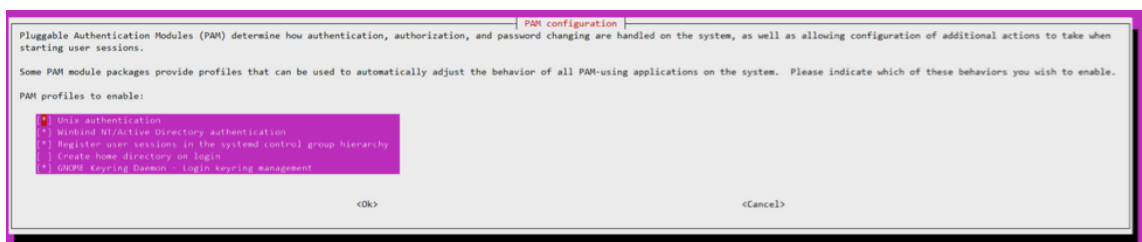
```

Tipp:

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 Dialogfeld, ob **Create home directory login** ausgewählt ist.

**Sitzung wird nicht gestartet 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, empfehlen wir, 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`:

```
1 Jan 25 23:30:31 yz-rhel72-1 setroubleshoot[3945]: SELinux is preventing
  /usr/sbin/sshd from setattr access on the directory /root. For
  complete SELinux messages. run sealert -l 32f52c1f-8ff9-4566-a698
  -963a79f16b81
2
3 Jan 25 23:30:31 yz-rhel72-1 python[3945]: SELinux is preventing /usr/
  sbin/sshd from setattr access on the directory /root.
4
```



```
5 ***** Plugin catchall_boolean (89.3 confidence) suggests
   *****
6
7 If you want to allow polyinstantiation to enabled
8
9 Then you must tell SELinux about this by enabling the '
  polyinstantiation_enabled' boolean.
10
11 You can read 'None' man page for more details.
12
13 Do
14
15     setsebool -P polyinstantiation_enabled 1
16
17 ***** Plugin catchall (11.6 confidence) suggests
   *****
18
19 If you believe that sshd should be allowed setattr access on the root
  directory by default.
20
21 Then you should report this as a bug.
22
23 You can generate a local policy module to allow this access.
24
25 Do
26
27     allow this access for now by executing:
28
29     # grep sshd /var/log/audit/audit.log | audit2allow -M mypol
30
31 # semodule -i mypol.pp
32 <!--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.

Manuelle Installation von Linux Virtual Delivery Agent für Amazon Linux 2, CentOS und RHEL

September 25, 2023

Wichtig:

Für Neuinstallationen empfehlen wir die Verwendung von [Easy Install](#) für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

Schritt 1: Vorbereiten Ihrer Linux-Distribution für die VDA-Installation

Schritt 1a: Überprüfen der Netzwerkkonfiguration

Stellen Sie sicher, dass das Netzwerk verbunden und richtig konfiguriert ist. Beispielsweise müssen Sie den DNS-Server auf dem Linux VDA konfigurieren.

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 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.

Hinweis:

Der Linux VDA unterstützt derzeit nicht das Abschneiden von NetBIOS-Namen. Der Hostname darf 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-->
```

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-->
```

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:

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--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 Uhrensynchronisierung

Es ist wichtig, dass die Uhrensynchronisierung 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.

In RHEL 8- oder RHEL 7-Standardumgebungen wird der Chrony-Daemon ([chronyd](#)) für die Uhrensynchronisierung verwendet.

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

```
1 server peer1-fqdn-or-ip-address iburst
2
3 server peer2-fqdn-or-ip-address iburst
4 <!--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:

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

Schritt 1g: Installieren von OpenJDK 11

Der Linux VDA erfordert das Vorhandensein von OpenJDK 11.

- Wenn Sie CentOS oder RHEL verwenden, wird beim Installieren des Linux VDA automatisch OpenJDK 11 als Abhängigkeit installiert.
- Wenn Sie Amazon Linux 2 verwenden, führen Sie den folgenden Befehl aus, um OpenJDK 11 zu aktivieren und zu installieren:

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

Bestätigen Sie die richtige Version:

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

Das OpenJDK-Paket ist möglicherweise eine frühere Version. Update auf OpenJDK 11:

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

Schritt 1h: Installieren von PostgreSQL

Der Linux VDA erfordert PostgreSQL. Mit den folgenden Befehlen installieren Sie PostgreSQL aus dem Linux VDA-Paket (PostgreSQL 9 für Amazon Linux 2, RHEL 7 und CentOS 7 sowie PostgreSQL 10 für RHEL 8).

```
1 sudo yum -y install postgresql-server
2
3 sudo yum -y install postgresql-jdbc
4 <!--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.

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

Schritt 1i: Starten von PostgreSQL

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

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl start postgresql
4 <!--NeedCopy-->
```

Überprüfen Sie die Version von PostgreSQL mit folgendem Befehl:

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

(Nur RHEL 7) Stellen Sie mit dem **psql**-Befehlszeilenprogramm sicher, dass das Datenverzeichnis festgelegt ist:

```
1 sudo -u postgres psql -c 'show data_directory'
2 <!--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 basierend auf 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 Hypervisor

Wenn das Zeitsynchronisierungsfeature auf Citrix Hypervisor aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme mit NTP und Citrix Hypervisor auf. Beide 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.

Wenn ein paravirtualisierter Linux-Kernel mit installierten Citrix VM Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das Citrix Hypervisor-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/independent_wallclock` nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

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

```
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:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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 Citrix Hypervisor, 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 mit NTP und Hypervisor auf. Beide 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 Services](#)
- [Centrify DirectControl](#)

- [SSSD](#)
- [PBIS](#)

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:

RHEL 8:

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

Amazon Linux 2, CentOS 7 und RHEL 7:

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

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

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

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

1. Führen Sie den folgenden Befehl aus:

RHEL 8:

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

Amazon Linux 2, CentOS 7 und RHEL 7:

```
1 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  
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
```

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.

2. 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  
winbind offline logon = no
```

3. (nur RHEL 8) Öffnen Sie `/etc/krb5.conf` fügen Sie den Abschnitten `[libdefaults]`, `[realms]` und `[domain_realm]` Einträge hinzu:

Unter dem Abschnitt `[libdefaults]`:

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

Unter dem Abschnitt `[realms]`:

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

Unter dem Abschnitt `[domain_realm]`:

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

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 beitrifft.

Windows-Domäne beitreten 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:

RHEL 8:

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

Amazon Linux 2 und RHEL 7:

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

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

PAM für Winbind konfigurieren 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:

```
1 sudo /sbin/service winbind restart
2 <!--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 }
```

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:

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

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

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

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

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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:

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

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

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

```
2 <!--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 bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

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

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache 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 6: Installieren des Linux VDA](#) fort.

Quest Authentication Services

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

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:

```
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.

VAS-Daemon konfigurieren 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.

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:

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
4 <!--NeedCopy-->
```

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

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
2 <!--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:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--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 bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\username
2 id -u
3 <!--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 gültig und nicht abgelaufen sind:

```
1 /opt/quest/bin/vastool 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 6: 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:

```
1 su -
2 adjoin -w -V -u user domain-name
3 <!--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 beitrifft.

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:

```
1 su -
2 adinfo
3 <!--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:

```
1 adinfo --sysinfo all
2 adinfo -diag
3 <!--NeedCopy-->
```

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

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

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
2. SSSD einrichten
3. Aktivieren von SSSD
4. Überprüfen der Kerberos-Konfiguration
5. Benutzerauthentifizierung überprüfen

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

In diesem Abschnitt wird die **Samba**-Methode für Amazon Linux 2 und RHEL 7 und die **adcli**-Methode für RHEL 8 beschrieben. Informationen über **realmd** finden Sie in der Dokumentation zu RHEL oder CentOS. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

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

Installieren oder aktualisieren Sie die erforderlichen Pakete:

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

Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

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

Konfigurieren Sie die Maschine für die **Samba**- und Kerberos-Authentifizierung:


```
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.

Hinweis:

Die Einstellungen in diesem Artikel sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen. Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur.

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  
winbind offline logon = no
```

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:

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

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

• Adcli (RHEL 8):

Installieren oder aktualisieren Sie die erforderlichen Pakete:

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

Konfigurieren Sie die Maschine für die **Samba**- und Kerberos-Authentifizierung:

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

Öffnen Sie **/etc/krb5.conf** fügen Sie den Abschnitten **[realms]** und **[domain_realm]** die nachfolgend aufgeführten Einträge hinzu:

Im Abschnitt [realms]:

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

Im Abschnitt [domain_realm]:

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

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:

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

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

SSSD einrichten Die Einrichtung von SSSD umfasst die folgenden Schritte:

- Installieren Sie das Paket **sssd-ad** auf dem Linux VDA, indem Sie den Befehl `sudo yum -y install sssd` ausführen.
- Ändern Sie die Konfiguration verschiedener Dateien (z. B. von `sssd.conf`).
- Starten des Diensts **sssd**.

Muster einer **sssd.conf**-Konfiguration für RHEL 7 (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
```

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](#).

(nur RHEL 8)

Öffnen Sie **/etc/sss/sssd.conf** und fügen Sie dem Abschnitt `[domain/ad.example.com]` folgende Einträge hinzu:

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

Legen Sie Dateieigentümer und Berechtigungen für `sssd.conf` fest:

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

Aktivieren von SSSD RHEL 8:

Um SSSD zu aktivieren, führen Sie den folgenden Befehl aus:

```
1 sudo systemctl restart sssd
2 sudo systemctl enable sssd.service
3 sudo chkconfig sssd on
4 <!--NeedCopy-->
```

Amazon Linux 2, CentOS 7 und RHEL 7:

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

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo service sssd start
4
5 sudo chkconfig sssd on
6 <!--NeedCopy-->
```

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

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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:

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

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

```
1 sudo getent passwd DOMAIN\username
2 <!--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 bislang noch nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 sudo 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 folgenden Befehl zurückgegebene **UID** erstellt wurde:

```
1 ls /tmp/krb5cc_{
2   uid }
3
4 <!--NeedCopy-->
```

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

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

PBIS

Download des erforderlichen PBIS-Pakets

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

Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei

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

Ausführen des PBIS-Installationsskripts

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

Windows-Domäne beitreten 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:

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

user ist ein Domänenbenutzer mit der Berechtigung, Computer zur Active Directory-Domäne hinzuzufügen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Hinweis: Führen Sie den Befehl **/opt/pbis/bin/config LoginShellTemplate/bin/bash** aus, um Bash als Standardshell festzulegen.

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 PBIS angemeldete Linux-Maschine zur Domäne gehört:

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

Wenn die Maschine einer Domäne beigetreten ist, werden mit diesem Befehl Informationen zur aktuell beigetretenen AD-Domäne und Organisationseinheit abgefragt. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen Um sicherzustellen, dass PBIS Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\user
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-->
```

Beenden Sie die Sitzung.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

Schritt 4: Installieren von .NET Runtime 6.0 als Voraussetzung

Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Führen Sie nach der Installation von .NET Runtime 6.0 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

Gehen Sie zur [Citrix Virtual Apps and Desktops-Downloadseite](#). Erweitern Sie die passende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das für Ihre Linux-Distribution geeignete Linux VDA-Paket herunterzuladen.

Schritt 6: Installieren des Linux VDA

Sie können eine Neuinstallation oder ein Upgrade für eine vorhandene Installation der vorherigen beiden Versionen und von einer LTSR-Version durchführen.

Durchführen einer Neuinstallation

1. (Optional) Deinstallieren Sie die alte 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.

- a) Halten Sie die Linux VDA-Dienste an:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl **service ctxmonitorservice stop**, bevor Sie die Dienste `ctxvda` und `ctxhdx` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

b) Deinstallieren Sie das Paket:

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

Hinweis:

Zum Ausführen eines Befehls ist der vollständige Pfad erforderlich. Alternativ können Sie dem Systempfad `/opt/Citrix/VDA/sbin` und `/opt/Citrix/VDA/bin` hinzufügen.

2. Laden Sie das Linux VDA -Paket herunter

Gehen Sie zur [Citrix Virtual Apps and Desktops-Downloadseite](#). Erweitern Sie die passende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das für Ihre Linux-Distribution geeignete Linux VDA-Paket herunterzuladen.

3. Installieren des Linux VDA

Hinweis:

Installieren Sie für RHEL und CentOS das EPEL-Repository, bevor Sie den Linux VDA erfolgreich installieren können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter <https://docs.fedoraproject.org/en-US/epel/>.

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

Amazon Linux 2:

```
1 sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
2 <!--NeedCopy-->
```

RHEL 8:

```
1 sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
2 <!--NeedCopy-->
```

Für CentOS 7 und RHEL 7:

```
1 sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
2 <!--NeedCopy-->
```

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

Amazon Linux 2:


```
1 sudo rpm -i XenDesktopVDA-<version>.amzn2.x86_64.rpm
2 <!--NeedCopy-->
```

RHEL 8:

```
1 sudo rpm -i XenDesktopVDA-<version>.el8.x.x86_64.rpm
2 <!--NeedCopy-->
```

Für CentOS 7 und RHEL 7:

```
1 sudo rpm -i XenDesktopVDA-<version>.el7.x.x86_64.rpm
2 <!--NeedCopy-->
```

RPM-Abhängigkeitsliste für RHEL 8:

```
1 qt5-qtbase >= 5.5~
2
3 ibus >= 1.5
4
5 nss-tools >= 3.44.0
6
7 gperftools-libs >= 2.4
8
9 cyrus-sasl-gssapi >= 2.1
10
11 python2 >= 2.7~
12
13 postgresql-jdbc >= 42.2.3
14
15 postgresql-server >= 10.6
16
17 java-11-openjdk >= 11
18
19 icoutils >= 0.32
20
21 firewalld >= 0.8.0
22
23 policycoreutils-python-utils >= 2.9
24
25 python3-policycoreutils >= 2.9
26
27 dbus >= 1.12.8
28
29 dbus-common >= 1.12.8
30
31 dbus-daemon >= 1.12.8
32
33 dbus-tools >= 1.12.8
34
35 dbus-x11 >= 1.12.8
36
37 xorg-x11-server-utils >= 7.7
38
```

```
39  xorg-x11-xinit >= 1.3.4
40
41  libXpm >= 3.5.12
42
43  libXrandr >= 1.5.1
44
45  libXtst >= 1.2.3
46
47  motif >= 2.3.4
48
49  pam >= 1.3.1
50
51  util-linux >= 2.32.1
52
53  util-linux-user >= 2.32.1
54
55  xorg-x11-utils >= 7.5
56
57  bash >= 4.4
58
59  findutils >= 4.6
60
61  gawk >= 4.2
62
63  sed >= 4.5
64
65  cups >= 2.2
66
67  foomatic-filters >= 4.0.9
68
69  cups-filters >= 1.20.0
70
71  ghostscript >= 9.25
72
73  libxml2 >= 2.9
74
75  libmspack >= 0.7
76  <!--NeedCopy-->
```

RPM-Abhängigkeitsliste für Amazon Linux 2, CentOS 7 und RHEL 7:

```
1  qt5-qtbase >= 5.5~
2
3  libmspack >= 0.5
4
5  ibus >= 1.5
6
7  cyrus-sasl-gssapi >= 2.1
8
9  gperftools-libs >= 2.4
10
11 nss-tools >= 3.44.0
12
```

```
13 postgresql-server >= 9.2
14
15 postgresql-jdbc >= 9.2
16
17 java-11-openjdk >= 11
18
19 ImageMagick >= 6.7.8.9
20
21 firewalld >= 0.3.9
22
23 polycoreutils-python >= 2.0.83
24
25 dbus >= 1.6.12
26
27 dbus-x11 >= 1.6.12
28
29 xorg-x11-server-utils >= 7.7
30
31 xorg-x11-xinit >= 1.3.2
32
33 xorg-x11-server-Xorg >= 1.20.4
34
35 libXpm >= 3.5.10
36
37 libXrandr >= 1.4.1
38
39 libXtst >= 1.2.2
40
41 motif >= 2.3.4
42
43 pam >= 1.1.8
44
45 util-linux >= 2.23.2
46
47 bash >= 4.2
48
49 findutils >= 4.5
50
51 gawk >= 4.0
52
53 sed >= 4.2
54
55 cups >= 1.6.0
56
57 foomatic-filters >= 4.0.9
58
59 openldap >= 2.4
60
61 cyrus-sasl >= 2.1
62
63 cyrus-sasl-gssapi >= 2.1
64
65 libxml2 >= 2.9
```

```
66
67  python-requests >= 2.6.0
68
69  gperftools-libs >= 2.4
70
71  rpmlib(FileDigests) <= 4.6.0-1
72
73  rpmlib(PayloadFilesHavePrefix) <= 4.0-1
74
75  pmlib(CompressedFileNames) <= 3.0.4-1
76
77  rpmlib(PayloadIsXz) <= 5.2-1
78  <!--NeedCopy-->
```

Hinweis:

Eine Übersicht der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden, finden Sie in der Tabelle [Systemanforderungen](#).

Führen Sie nach der Installation des Linux VDA unter RHEL 7.x den Befehl `sudo yum install -y python-websockify x11vnc` aus. Damit werden `python-websockify` und `x11vnc` manuell für die Verwendung der Sitzungsspiegelung installiert. Weitere Informationen finden Sie unter [Sitzungen spiegeln](#).

So aktualisieren Sie eine vorhandene Installation

Sie können ein Upgrade für eine vorhandene Installation der vorherigen beiden Versionen und von einer LTSR-Version durchführen.

Hinweis:

Durch das Upgrade einer Installation werden die Konfigurationsdateien unter `/etc/xdl` überschrieben. Sichern Sie die Dateien vor jedem Upgrade.

- So aktualisieren Sie Ihre Software mit Yum:

Amazon Linux 2:

```
1  sudo yum install -y XenDesktopVDA-<version>.amzn2.x86_64.rpm
2  <!--NeedCopy-->
```

RHEL 8:

```
1  sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
2  <!--NeedCopy-->
```

Für CentOS 7 und RHEL 7:

```
1  sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
2  <!--NeedCopy-->
```

- So aktualisieren Sie Ihre Software mit RPM-Paketmanager:

Amazon Linux 2:

```
1 sudo rpm -U XenDesktopVDA-<version>.amzn2.x86_64.rpm
2 <!--NeedCopy-->
```

RHEL 8:

```
1 sudo rpm -U XenDesktopVDA-<version>.el8.x.x86_64.rpm
2 <!--NeedCopy-->
```

Für CentOS 7 und RHEL 7:

```
1 sudo rpm -U XenDesktopVDA-<version>.el7.x.x86_64.rpm
2 <!--NeedCopy-->
```

Hinweis:

Bei Verwendung von RHEL 7 sind nach dem Ausführen der vorherigen Upgrade-Befehle folgende Schritte erforderlich:

1. Führen Sie `/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_SZ"-v "DotNetRuntimePath"-d "/opt/rh/rh-dotnet31/root/usr/bin/"--force` aus, um den richtigen .NET-Laufzeitpfad festzulegen.
2. Starten Sie den Dienst `ctxvda` neu.

Wichtig:

Starten Sie die Linux VDA-Maschine nach der Softwareaktualisierung neu.

Schritt 7: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro müssen Sie die NVIDIA GRID-Treiber auf Ihrem Hypervisor und auf den VDA-Maschinen installieren.

Hinweis:

Um HDX 3D Pro für Amazon Linux 2 zu verwenden, empfehlen wir die Installation des NVIDIA-Treibers 470. Weitere Informationen finden Sie unter [Systemanforderungen](#).

Informationen zum Installieren und Konfigurieren des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Handbüchern:

- [Citrix Hypervisor](#)
- [VMware ESX](#)

`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 8: 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:

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

Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--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 Domännennamen (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 VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-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 | 5** –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 Authentication Services
 - 3 –Centrify DirectControl
 - 4 –SSSD
 - 5 –PBIS
- **CTX_XDL_HDX_3D_PRO=Y | N** –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung grafikintensiver Anwendungen. 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 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Wenn Sie die LDAP-Portnummer als 389 angeben, fragt der Linux VDA jeden LDAP-Server in der angegebenen Domäne im Abfragemodus ab. Wenn es x Richtlinien und y Anzahl von LDAP-Servern gibt, führt der Linux VDA die Summe von X multipliziert mit Y-Abfragen aus. Wenn die Abfragezeit den Schwellenwert überschreitet, schlagen Sitzungsanmeldungen möglicherweise fehl. Für schnellere LDAP-Abfragen aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben die entsprechende LDAP-Portnummer als 3268 an. 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_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. `ctx_xdl_fas_fas_list='FAS_Server_1_URL:Port_Number; fas_server_2_url: port_number; fas_server_3_url: port_number'`.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (**ctxvda**). Der Standardpfad ist `/usr/bin`.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate:** Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

Sie können die Desktopumgebung für Sitzungsbenutzer auch über die folgenden Schritte ändern:

1. Erstellen Sie die Datei `.xsession` oder `.Xclients` auf dem VDA im Verzeichnis **\$HOME/<username>**. Wenn Sie Amazon Linux 2 verwenden, erstellen Sie die Datei `.Xclients`. Wenn Sie andere Distributionen verwenden, erstellen Sie die Datei `.xsession`.
2. Geben Sie in der Datei `.xsession` oder `.Xclients` eine auf Distributionen basierende Desktopumgebung an.

– **MATE-Desktop unter Amazon Linux 2 und RHEL 8**

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

– **Für GNOME Classic-Desktop unter Amazon Linux 2, CentOS und RHEL**

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

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

– **Für GNOME-Desktop unter Amazon Linux 2, CentOS und RHEL**

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

3. Teilen Sie die 700-Dateiberechtigung mit dem Zielsitzungsbenutzer.

- **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.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

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

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<none>'
```

```
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

Sie müssen die Option **-E** mit dem Befehl “sudo” angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, 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:

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

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:

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

Entfernen von Konfigurationsänderungen:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--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 9: Ausführen von XDPing

Mit `sudo /opt/Citrix/VDA/bin/xdping` können Sie Linux VDA-Umgebungen auf häufige Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter [XDPing](#).

Schritt 10: 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:

```
1 sudo /sbin/service ctxhdx start
2
3 sudo /sbin/service ctxvda start
4 <!--NeedCopy-->
```

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl `service ctxmonitorservice stop`, bevor Sie die Dienste `ctxvda` und `ctxhdx` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
6 <!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
4 <!--NeedCopy-->
```

Schritt 11: Erstellen des Maschinenkatalogs in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
 - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- 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 12: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- 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.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter [Citrix Virtual Apps and Desktops 7 2206](#).

Manuelle Installation von Linux Virtual Delivery Agent für SUSE

February 9, 2024

Wichtig:

Für Neuinstallationen empfehlen wir die Verwendung von [Easy Install](#) für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

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:

```
1 su -
2
3 yast
4 <!--NeedCopy-->
```

Starten des UI-basierten YaST-Tools:

```
1 su -
2
3 yast2 &
4 <!--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 Domain Name System (DNS)

1. Starten Sie das UI-basierte YaST-Tool.
2. Wählen Sie **System** und dann **Network Settings** aus.

3. Öffnen Sie die Registerkarte **Hostname/DNS**.
4. Wählen Sie die Option **no** für **Set Hostname via DHCP**.
5. Wählen Sie für **Modify DNS Configuration** die Option **Use Custom Policy**.
6. Geben Sie die folgenden Informationen entsprechend Ihrer Netzwerkeinstellungen an:
 - **Static Hostname** –Geben Sie den DNS-Hostnamen 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-Domännennamen an.
7. Ändern Sie die folgende Zeile der Datei `/etc/hosts`, sodass sie den FQDN und den Hostnamen als die ersten beiden Einträge enthält:

```
127.0.0.1 <FQDN of the VDA> <hostname of the VDA> localhost
```

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.

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 zurückgegeben, nicht der vollqualifizierte Domänenname (FQDN).

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
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--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 LinuxVDAs 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.

SUSE 15.3 und SUSE 15.2:

1. Starten Sie das UI-basierte YaST-Tool.
2. Wählen Sie **Network Services** und dann **NTP Configuration**.
3. Wählen Sie im Abschnitt **Start NTP Daemon** die Option **Now and on Boot**.
4. Wählen Sie für **Configuration Source** die Option **Dynamic**.
5. Fügen Sie nach Bedarf NTP-Server hinzu. Der NTP-Dienst wird normalerweise auf dem Active Directory-Domänencontroller gehostet.
6. Falls vorhanden, löschen Sie die folgende Zeile in `/etc/chrony.conf` oder kommentieren Sie sie aus.

```
include /etc/chrony.d/*.conf
```

Nachdem Sie `chrony.conf` bearbeitet haben, starten Sie den Dienst `chronyd` neu.

```
1 sudo systemctl restart chronyd.service
2 <!--NeedCopy-->
```

Schritt 1d: Installieren von Linux VDA-abhängigen Paketen

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

- `Postgresql13-server` 13 oder höher

- OpenJDK 11
- Open Motif Runtime Environment 2.3.1 oder höher
- Cups 1.6.0 oder höher
- ImageMagick 6.8 oder höher

Hinzufügen von Repositories Sie können die meisten benötigten Pakete außer ImageMagick aus offiziellen Repositories beziehen. Um die ImageMagick-Pakete abzurufen, aktivieren Sie das Repository `sle-module-desktop-applications` mit YaST oder dem folgenden Befehl:

```
SUSEConnect -p sle-module-desktop-applications/<version number>/x86_64
```

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

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

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

Installieren von OpenJDK 11 Der Linux VDA erfordert das Vorhandensein von OpenJDK 11.

Führen Sie den folgenden Befehl aus, um OpenJDK 11 zu installieren:

```
1 sudo zypper install java-11-openjdk
2 <!--NeedCopy-->
```

Installieren von PostgreSQL Führen Sie zur Installation von `Postgresql` die folgenden Befehle aus:

```
1 sudo zypper install postgresql-server
2
3 sudo zypper install postgresql-jdbc
4 <!--NeedCopy-->
```

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

```
1 sudo systemctl enable postgresql
2
3 sudo systemctl restart postgresql
4 <!--NeedCopy-->
```

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

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 basierend auf 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 Hypervisor

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

Wenn ein paravirtualisierter Linux-Kernel mit installierten Citrix VM Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das Citrix Hypervisor-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/independent_wallclock** nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

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

```
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:

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

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

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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 Citrix Hypervisor, 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 mit NTP und Hypervisor auf. Beide versuchen, die Systemuhr zu synchronisieren. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, synchronisieren Sie die Systemuhr aller Linux-Gäste mit dem NTP. 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](#)
- [PBIS](#)

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

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. Starten Sie YaST, wählen Sie **Network Services** und dann **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 **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 die Berechtigung hat, Maschinen der Domäne hinzuzufügen, und klicken Sie auf **OK**.

6. Starten Sie Ihre Dienste manuell neu oder starten Sie die Maschine neu. Wir empfehlen Ihnen, den Computer neu zu starten:

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

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:

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

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

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

Kerberos-Konfiguration überprüfen Stellen Sie sicher, dass die keytab-Systemdatei erstellt wurde und gültige Schlüssel enthält:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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:

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

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

```
1 wbinfo --krb5auth=domain\username%password
2 <!--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.

Stellen Sie sicher, dass das Winbind PAM-Modul korrekt konfiguriert ist. Melden Sie sich dazu mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\username
2 id -u
3 <!--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 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 6: Installieren des Linux VDA](#) fort.

Quest Authentication Service

Quest auf dem Domänencontroller konfigurieren Es wird vorausgesetzt, dass Sie die Quest-Software auf den Domänencontrollern installiert und konfiguriert haben und über Administrator-

rechte 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 Verwaltungskonsolle 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.

```
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.

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

```
1 sudo /opt/quest/bin/vastool configure pam  
2  
3 sudo /opt/quest/bin/vastool configure nss  
4 <!--NeedCopy-->
```


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

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

user ist ein beliebiger Domänenbenutzer mit der Berechtigung, Maschinen 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:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--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 Stellen Sie sicher, dass Quest Domänenbenutzer über PAM authentifizieren kann. Melden Sie sich dazu mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\username
2 id -u
3 <!--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 gültig und nicht abgelaufen sind:

```
1 /opt/quest/bin/vastool 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 6: 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:

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

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

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:

```
1 sudo adinfo
2 <!--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:

```
1 adinfo --sysinfo all
2
3 adinfo -diag
4 <!--NeedCopy-->
```

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

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

SSSD

Beim Einsatz von SSSD auf SUSE 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.

Um SSSD für SUSE einzurichten, führen Sie die folgenden Schritte aus:

1. Domänenbeitritt und Erstellen von Hostschlüsseltabellen
2. Konfigurieren von PAM für SSSD
3. SSSD einrichten
4. Aktivieren von SSSD
5. Domäneneigentümerschaft überprüfen
6. Überprüfen der Kerberos-Konfiguration
7. Benutzerauthentifizierung überprüfen

Domänenbeitritt und Erstellen einer Hostschlüsseltabelle SSSD bietet keine Active Directory-Clientfunktionen für den Domänenbeitritt und die Verwaltung der Systemschlüsseltabelle. Sie können stattdessen den **Samba**-Ansatz verwenden. Führen Sie die folgenden Schritte aus, bevor Sie SSSD konfigurieren.

1. Stoppen und deaktivieren Sie den Name Service Cache Daemon (NSCD).

```
1 sudo systemctl stop nscd
2 sudo systemctl disable nscd
3 <!--NeedCopy-->
```

2. Überprüfen Sie den Hostnamen und die Chrony-Zeitsynchronisierung.

```
1 hostname
2 hostname -f
3 chronyc traking
4 <!--NeedCopy-->
```

3. Installieren oder aktualisieren Sie die erforderlichen Pakete:

```
1 sudo zypper install samba-client sssd-ad
2 <!--NeedCopy-->
```

4. Bearbeiten Sie die Datei `/etc/krb5.conf` als Root-Benutzer, damit das **kinit**-Hilfsprogramm mit der Zieldomäne kommunizieren kann. Fügen Sie die folgenden Einträge in den Abschnitten **[libdefaults]**, **[realms]** und **[domain_realm]** hinzu:

Hinweis:

Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellun-

gen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
1 [libdefaults]
2
3     dns_canonicalize_hostname = false
4
5     rdns = false
6
7     default_realm = REALM
8
9     forwardable = true
10
11 [realms]
12
13     REALM = {
14
15
16         kdc = fqdn-of-domain-controller
17
18         default_domain = realm
19
20         admin_server = fqdn-of-domain-controller
21     }
22
23 [domain_realm]
24
25     .realm = REALM
26 <!--NeedCopy-->
```

realm ist der Kerberos-Bereichsname, z. B. example.com. **REALM** ist der Kerberos-Bereichsname in Großbuchstaben, z. B. EXAMPLE.COM.

5. Bearbeiten Sie die Datei `/etc/samba/smb.conf` als Root-Benutzer, damit das **net-**Hilfsprogramm mit der Zieldomäne kommunizieren kann. Fügen Sie die folgenden Einträge im Abschnitt **[global]** hinzu:

```
1 [global]
2     workgroup = domain
3
4     client signing = yes
5
6     client use spnego = yes
7
8     kerberos method = secrets and keytab
9
10    realm = REALM
11
12    security = ADS
13 <!--NeedCopy-->
```

domain ist der kurze NetBIOS-Name einer Active Directory-Domäne, z. B. EXAMPLE.

6. Ändern Sie die Einträge **passwd** und **group** in der Datei `/etc/nsswitch.conf`, sodass sie beim Auflösen von Benutzern und Gruppen auf SSSD verweisen.

```
1 passwd: compat sss
2
3 group: compat sss
4 <!--NeedCopy-->
```

7. Verwenden Sie den konfigurierten Kerberos-Client, um sich bei der Zieldomäne als Administrator zu authentifizieren.

```
1 kinit administrator
2 <!--NeedCopy-->
```

8. Verwenden Sie das Hilfsprogramm **net**, um das System mit der Domäne zu verbinden und eine Keytab-Datei für das System zu generieren.

```
1 net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
  administrator
2 <!--NeedCopy-->
```

Konfigurieren von PAM für SSSD Bevor Sie PAM für SSSD konfigurieren, installieren oder aktualisieren Sie die erforderlichen Pakete:

```
1 sudo zypper install sssd sssd-ad
2 <!--NeedCopy-->
```

Konfigurieren Sie das PAM-Modul für die Benutzerauthentifizierung über SSSD und erstellen Sie Homeverzeichnisse für Benutzeranmeldungen.

```
1 sudo pam-config --add --sss
2 sudo pam-config --add --mkhomedir
3 <!--NeedCopy-->
```

SSSD einrichten

1. Bearbeiten Sie `/etc/sss/sss.conf` als Root-Benutzer, damit der SSSD-Daemon mit der Zieldomäne kommunizieren kann. Muster einer `sss.conf`-Konfiguration (zusätzliche Optionen können bei Bedarf hinzugefügt werden):

```
1 [sss]
2     config_file_version = 2
3     services = nss,pam
4     domains = domain-dns-name
5
6 [domain/domain-dns-name]
7     id_provider = ad
8     auth_provider = ad
```

```
9     access_provider = ad
10     ad_domain = domain-dns-name
11     ad_server = fqdn-of-domain-controller
12     ldap_id_mapping = true
13     ldap_schema = ad
14
15     # Kerberos settings
16     krb5_ccachedir = /tmp
17     krb5_ccname_template = FILE:%d/krb5cc_%U
18
19     # Comment out if the users have the shell and home dir set on the
20     # AD side
21     fallback_homedir = /home/%d/%u
22     default_shell = /bin/bash
23
24     # Uncomment and adjust if the default principal SHORTNAME$@REALM
25     # is not available
26     # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
27
28     ad_gpo_access_control = permissive
29
30     <!--NeedCopy-->
```

domain-dns-name ist der DNS-Domänenname, z. B. example.com.

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. **ad_gpo_access_control** ist auf **permissive** festgelegt, um einen ungültigen Anmeldefehler für Linux-Sitzungen zu verhindern. Weitere Informationen finden Sie in den Manpages für `sssd.conf` und `sssd-ad`.

2. Legen Sie Dateieigentümer und Berechtigungen für `sssd.conf` fest:

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

Aktivieren von SSSD Führen Sie die folgenden Befehle aus, um den SSSD-Daemon beim Systemstart zu aktivieren und zu starten:

```
1 sudo systemctl enable sssd
2 sudo systemctl start sssd
3 <!--NeedCopy-->
```

Domäneneigentümerschaft überprüfen

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

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

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

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

Kerberos-Konfiguration überprüfen Stellen Sie sicher, dass die keytab-Systemdatei erstellt wurde und gültige Schlüssel enthält:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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:

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

Benutzerauthentifizierung überprüfen 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 bislang noch nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

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

```
2
3 id -u
4
5 klist
6
7 exit
8 <!--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:

```
1 ls /tmp/krb5cc_uid
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 6: Installieren des Linux VDA](#) fort.

PBIS

Download des erforderlichen PBIS-Pakets Beispiel:

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

Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei Beispiel:

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

Ausführen des PBIS-Installationsskripts Beispiel:

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

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 Maschinen zur Domäne verfügen:

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


user ist ein beliebiger Domänenbenutzer mit der Berechtigung, Maschinen der Active Directory-Domäne hinzuzufügen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Hinweis: Führen Sie den Befehl `/opt/pbis/bin/config LoginShellTemplate/bin/bash` aus, um Bash als Standardshell festzulegen.

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 PBIS angemeldete Linux-Maschine zur Domäne gehört:

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

Wenn die Maschine einer Domäne beigetreten ist, werden mit diesem Befehl Informationen zur aktuell beigetretenen AD-Domäne und Organisationseinheit abgefragt. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen Stellen Sie sicher, dass PBIS Domänenbenutzer über PAM authentifizieren kann. Melden Sie sich dazu mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\user
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-->
```

Beenden Sie die Sitzung.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

Schritt 4: Installieren von .NET Runtime 6.0 als Voraussetzung

Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Führen Sie nach der Installation von .NET Runtime 6.0 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite. Erweitern Sie die passende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das für Ihre Linux-Distribution geeignete Linux VDA-Paket herunterzuladen.

Schritt 6: Installieren des Linux VDA

Schritt 6a: 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:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl `service ctxmonitorservice stop`, bevor Sie die Dienste `ctxvda` und `ctxhdx` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

2. Deinstallieren Sie das Paket:

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

Wichtig:

Upgrades von den letzten zwei Versionen werden unterstützt.

Hinweis:

Installierte Komponenten finden Sie unter `/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 6b: Installieren des Linux VDA

Installieren der Linux VDA-Software mit Zypper:

```
1 sudo zypper install XenDesktopVDA-<version>.sle15_x.x86_64.rpm
2 <!--NeedCopy-->
```

Installieren der Linux VDA-Software mit dem RPM-Paketmanager:

```
1 sudo rpm -i XenDesktopVDA-<version>.sle15_x.x86_64.rpm
2 <!--NeedCopy-->
```

Schritt 6c: Upgrade des Linux VDA (optional)

Sie können ein Upgrade für eine vorhandene Installation der vorherigen beiden Versionen und von einer LTSR-Version durchführen.

Hinweis:

Durch das Upgrade einer Installation werden die Konfigurationsdateien unter **/etc/xdl** überschrieben. Sichern Sie die Dateien vor jedem Upgrade.

```
1 sudo rpm -U XenDesktopVDA-<version>.sle15_x.x86_64.rpm
2 <!--NeedCopy-->
```

RPM-Abhängigkeitsliste für SUSE 15:

```
1 postgresql >= 13
2
3 postgresql-server >= 13
4
5 postgresql-jdbc >= 9.4
6
7 java-11-openjdk >= 11
8
9 ImageMagick >= 7.0
10
11 dbus-1 >= 1.12.2
12
13 dbus-1-x11 >= 1.12.2
14
15 xorg-x11 >= 7.6_1
16
17 libXpm4 >= 3.5.12
18
```

```
19 libXrandr2 >= 1.5.1
20
21 libXtst6 >= 1.2.3
22
23 motif >= 2.3.4
24
25 pam >= 1.3.0
26
27 bash >= 4.4
28
29 findutils >= 4.6
30
31 gawk >= 4.2
32
33 sed >= 4.4
34
35 cups >= 2.2
36
37 cups-filters >= 1.25
38
39 libxml2-2 >= 2.9
40
41 libmspack0 >= 0.6
42
43 ibus >= 1.5
44
45 libtcmalloc4 >= 2.5
46
47 libcap-progs >= 2.26
48
49 mozilla-nss-tools >= 3.53.1
50
51 libpython2_7-1_0 >= 2.7
52 <!--NeedCopy-->
```

Wichtig:

Starten Sie die Linux VDA-Maschine nach dem Upgrade neu.

Schritt 7: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro müssen Sie die NVIDIA GRID-Treiber auf Ihrem Hypervisor und auf den VDA-Maschinen installieren.

Informationen zum Installieren und Konfigurieren des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Handbüchern:

- [Citrix Hypervisor](#)
- [VMware ESX](#)
- [Nutanix AHV](#)

Zum Installieren und Konfigurieren der NVIDIA GRID-Gast-VM-Treiber führen Sie die folgenden allgemeinen Schritte aus:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM in der Hypervisor-Systemsteuerung eine GPU zu.
3. Starten Sie die VM.
4. Installieren Sie den Gast-VM-Treiber auf der VM.

Schritt 8: Konfigurieren des Linux VDA

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript `ctxsetup.sh` ausführen. Bevor das Skript Änderungen macht, überprüft es die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. 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:

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

Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--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 Domännennamen (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 VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für den Linux VDA 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. 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 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Wenn Sie die LDAP-Portnummer als 389 angeben, fragt der Linux VDA jeden LDAP-Server in der angegebenen Domäne im Abfragemodus ab. Wenn es x Richtlinien und y Anzahl von LDAP-Servern gibt, führt der Linux VDA die Summe von X multipliziert mit Y-Abfragen aus. Wenn die Abfragezeit den Schwellenwert überschreitet, schlagen Sitzungsanmeldungen möglicherweise fehl. Für schnellere LDAP-Abfragen aktivieren Sie **Global Catalog** auf einem Domänencon-

troller und geben die entsprechende LDAP-Portnummer als 3268 an. 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_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. `ctx_xdl_fas_fas_list='FAS_Server_1_URL:Port_Number; fas_server_2_url: port_number; fas_server_3_url: port_number'`.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts ([ctxvda](#)). Der Standardpfad ist `/usr/bin`.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate:** Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

Sie können die Desktopumgebung für Sitzungsbenutzer auch über die folgenden Schritte ändern:

1. Erstellen Sie die Datei `.xsession` auf dem VDA im Verzeichnis **\$HOME/<username>**.
2. Geben Sie in der Datei `.xsession` eine auf Distributionen basierende Desktopumgebung an.

– Für MATE-Desktop unter SUSE 15

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

– Für GNOME Classic Desktop auf SUSE 15

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

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

– Für GNOME Desktop auf SUSE 15

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

3. Teilen Sie die 700-Dateiberechtigung mit dem Zielsitzungsbenutzer.

- **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.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

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

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
2
3 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<none>'
```



```
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

Sie müssen die Option **-E** mit dem Befehl “sudo” angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, 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:

```
1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4 \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

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:

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

Entfernen von Konfigurationsänderungen:

```
1 sudo /usr/local/sbin/ctxcleanup.sh
2 <!--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 9: Ausführen von XDPing

Mit `sudo /opt/Citrix/VDA/bin/xdping` können Sie Linux VDA-Umgebungen auf häufige Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter [XDPing](#).

Schritt 10: 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:

```
1 sudo /sbin/service ctxhdx start
2
3 sudo /sbin/service ctxvda start
4 <!--NeedCopy-->
```

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx stop
4 <!--NeedCopy-->
```

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl `service ctxmonitorservice stop`, bevor Sie die Dienste `ctxvda` und `ctxhdx` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda stop
2
3 sudo /sbin/service ctxhdx restart
4
5 sudo /sbin/service ctxvda start
6 <!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
1 sudo /sbin/service ctxvda status
2
3 sudo /sbin/service ctxhdx status
4 <!--NeedCopy-->
```

Schritt 11: Erstellen des Maschinenkatalogs in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
 - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- 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 12: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- 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.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter [Citrix Virtual Apps and Desktops 7 2206](#).

Manuelle Installation von Linux Virtual Delivery Agent für Ubuntu

October 5, 2022

Wichtig:

Für Neuinstallationen empfehlen wir die Verwendung von [Easy Install](#) für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

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. Beispielsweise müssen Sie den DNS-Server auf dem Linux VDA konfigurieren.

Nehmen Sie bei Verwendung von Ubuntu 18.04 Live Server folgende Änderung in der Konfigurationsdatei **/etc/cloud/cloud.cfg** vor, bevor Sie den Hostnamen festlegen:

```
preserve_hostname: true
```

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

Vergewissern Sie sich, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine korrekt gemeldet werden. Sie können hierfür die folgende Zeile der Datei **/etc/hosts** durch den FQDN und den Hostnamen als erste beiden Einträge erweitern:

```
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 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.

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 Sie folgende 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:

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
6
7 ping delivery-controller-fqdn
8 <!--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:

```
1 apt-get install chrony
2 <!--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:

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

Schritt 1h: Installieren von OpenJDK 11

Der Linux VDA erfordert das Vorhandensein von OpenJDK 11.

Installieren Sie unter Ubuntu 20.04 und Ubuntu 18.04 OpenJDK 11:

```
1 sudo apt-get install -y openjdk-11-jdk
2 <!--NeedCopy-->
```

Schritt 1i: Installieren von PostgreSQL

Der Linux VDA erfordert PostgreSQL 9.x unter Ubuntu:

```
1 sudo apt-get install -y postgresql
2
3 sudo apt-get install -y libpostgresql-jdbc-java
4 <!--NeedCopy-->
```

Schritt 1j: Installieren von Motif

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

Schritt 1k: Installieren weiterer Pakete

```
1 sudo apt-get install -y libsasl2-2
2
3 sudo apt-get install -y libsasl2-modules-gssapi-mit
4
5 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 libgtk2.0-0
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 basierend auf 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 Hypervisor

Wenn das Zeitsynchronisierungsfeature auf Citrix Hypervisor aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme mit NTP und Citrix Hypervisor auf. Beide 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.

Wenn ein paravirtualisierter Linux-Kernel mit installierten Citrix VM Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das Citrix Hypervisor-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/independent_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:

```
1 su -
2
3 cat /proc/sys/xen/independent_wallclock
4 <!--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 Citrix Hypervisor, 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 mit NTP und Hypervisor auf. Beide 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](#)
- [PBIS](#)

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

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

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

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

Hinweis:

Stellen Sie sicher, dass das `winbind`-Skript unter `/etc/init.d` ist.

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

Hinweis:

Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
[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
```

Der Parameter **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:

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

WORKGROUP 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:

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

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

Neustart von winbind

```
1 sudo systemctl restart winbind
2 <!--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:

```
1 sudo pam-auth-update
2 <!--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:

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

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

```
1 sudo net ads info
2 <!--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 **Schlüsselstabelle** erstellt wurde und gültige Schlüssel enthält:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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:

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

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

```
1 wbinfo --krb5auth=domain\username%password
2 <!--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 bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

Hinweis:

Um einen SSH-Befehl erfolgreich auszuführen, stellen Sie sicher, dass SSH aktiviert ist und ordnungsgemäß funktioniert.

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 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 6: 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:

```
1 sudo /opt/quest/bin/vastool configure pam
2
3 sudo /opt/quest/bin/vastool configure nss
4 <!--NeedCopy-->
```

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

```
1 sudo /opt/quest/bin/vastool -u user join domain-name
2 <!--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:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--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 bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 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 gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: 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:

```
1 su -
2 adjoin -w -V -u user domain-name
3 <!--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 beitrifft.

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:

```
1 su -
2
3 adinfo
4 <!--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:

```
1 adinfo --sysinfo all
2
3 adinfo --diag
4 <!--NeedCopy-->
```

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

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

SSSD

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

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

Zum Konfigurieren von Kerberos öffnen Sie als Root-Benutzer **/etc/krb5.conf** und legen Sie folgende Parameter fest:

Hinweis:

Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
[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
```

Der Parameter `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 für **adcli** und **Samba**.

- **Wenn Sie der Domäne mit adcli beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie **adcli**.

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

2. Treten Sie mit **adcli** der Domäne bei.

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

```
1 su -
2
3 rm -rf /etc/krb5.keytab
4
5 adcli join domain-dns-name -U user -H hostname-fqdn
6 <!--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.

3. Überprüfen Sie die Domänenmitgliedschaft.

Führen Sie bei einem Ubuntu 20.04-Computer den Befehl `adcli testjoin` aus.

Führen Sie bei einem Ubuntu 18.04-Computer den Befehl `sudo klist -ket` aus. Die Leistungsfähigkeit des **adcli**-Tools ist begrenzt. Das Tool bietet keine Möglichkeit zu testen, ob eine Maschine mit der Domäne verbunden ist. Die beste Alternative ist, sicherzustellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde. Prüfen Sie, ob die Zeitstempel der einzelnen Schlüssel mit der Zeit übereinstimmen, zu der der Domänenbeitritt der Maschine erfolgte.

- **Wenn Sie der Domäne mit Samba beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.

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

2. 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
```

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

3. Treten Sie der Domäne mit **Samba** bei.

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

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

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

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

```
1 sudo apt-get install --only-upgrade sssd
2 <!--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/sss/sss.conf** nicht standardmäßig installiert und muss manuell erstellt werden. Öffnen oder erstellen Sie als Root-Benutzer **/etc/sss/sss.conf** und nehmen Sie folgende Einstellungen vor:

```
[sss]
```

```
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
```

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.

Der Parameter **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-Domännennamens ist nicht erforderlich.

Weitere Informationen zu den Konfigurationseinstellungen finden Sie auf den Manpages über `sssd.conf` und `sssd-ad`.

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

```
1 sudo chmod 0600 /etc/sssd/sssd.conf
2 <!--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:

```
1 sudo systemctl start sssd
2
3 sudo systemctl enable sssd
4 <!--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:

```
1 sudo pam-auth-update
2 <!--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.

- Wenn Sie die Domänenmitgliedschaft mit **adcli** überprüfen, führen Sie den Befehl `sudo adcli info domain-dns-name` aus, um die Domäneninformationen anzuzeigen.
- Wenn Sie die Domänenmitgliedschaft mit **Samba** überprüfen, führen Sie den Befehl `sudo net ads testjoin` aus, um zu überprüfen, ob die Maschine Mitglied einer Domäne ist, und den Befehl `sudo net ads info` zum Überprüfen zusätzlicher Domänen- und Computerobjektinformationen.

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:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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 für das Maschinenkonto zwischengespeichert wurde:

```
1 sudo klist
2 <!--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 bislang noch nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\username
2
3 id -u
4
5 klist
6
7 exit
8 <!--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:

```
1 ls /tmp/krb5cc_uid
2 <!--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 6: Installieren des Linux VDA](#) fort.

PBIS

Download des erforderlichen PBIS-Pakets

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


Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei

```
1 sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

Ausführen des PBIS-Installationsskripts

```
1 sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

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:

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

user ist ein Domänenbenutzer mit der Berechtigung, Computer zur Active Directory-Domäne hinzuzufügen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Hinweis: Führen Sie den Befehl **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** aus, um Bash als Standardshell festzulegen.

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 PBIS angemeldete Linux-Maschine zur Domäne gehört:

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

Wenn die Maschine einer Domäne beigetreten ist, werden mit diesem Befehl Informationen zur aktuell beigetretenen AD-Domäne und Organisationseinheit abgefragt. Andernfalls wird nur der Hostname angezeigt.

Überprüfen der Benutzerauthentifizierung Um sicherzustellen, dass PBIS Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 sudo ssh localhost -l domain\user
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-->
```

Beenden Sie die Sitzung.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

Schritt 4: Installieren von .NET Runtime 6.0 als Voraussetzung

Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Führen Sie nach der Installation von .NET Runtime 6.0 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite. Erweitern Sie die passende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das für Ihre Linux-Distribution geeignete Linux VDA-Paket herunterzuladen.

Schritt 6: Installieren des Linux VDA

Schritt 6a: Installieren des Linux VDA

Installieren Sie die Linux VDA-Software mit dem Debian-Paketmanager:

Ubuntu 20.04:

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

Ubuntu 18.04:

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

Debian-Abhängigkeitsliste for Ubuntu 20.04:

```
1  libqt5widgets5 >= 5.7~
2
3  ibus >= 1.5
4
5  libsasl2-modules-gssapi-mit >= 2.1.~
6
7  postgresql >= 12
8
9  libpostgresql-jdbc-java >= 42.2
10
11 openjdk-11-jdk >= 11
12
13 imagemagick >= 8:6.9.10
14
15 ufw >= 0.36
16
17 ubuntu-desktop >= 1.450
18
19 libxrandr2 >= 2:1.5.2
20
21 libxtst6 >= 2:1.2.3
22
23 libxm4 >= 2.3.8
24
25 util-linux >= 2.34
26
27 gtk3-nocsd >= 3
28
29 bash >= 5.0
30
31 findutils >= 4.7.0
32
33 sed >= 4.7
34
35 cups >= 2.3
36
37 libmspack0 >= 0.10
38
39 libgoogle-perftools4 >= 2.7~
40
41 libpython2.7 >= 2.7~
42 <!--NeedCopy-->
```

Debian-Abhängigkeitsliste for Ubuntu 18.04:

```
1  libqt5widgets5 >= 5.7~
2
3  libmspack0 >= 0.6
4
5  ibus >= 1.5
6
7  libnss3-tools >= 2:3.35
```

```
8
9 postgresql >= 9.5
10
11 libpostgresql-jdbc-java >= 9.2
12
13 openjdk-11-jdk >= 11
14
15 gtk3-nocsd >=3
16
17 imagemagick >= 8:6.8.9.9
18
19 ufw >= 0.35
20
21 ubuntu-desktop >= 1.361
22
23 libxrandr2 >= 2:1.5.0
24
25 libxtst6 >= 2:1.2.2
26
27 libxm4 >= 2.3.4
28
29 util-linux >= 2.27.1
30
31 bash >= 4.3
32
33 findutils >= 4.6.0
34
35 sed >= 4.2.2
36
37 cups >= 2.1
38
39 libldap-2.4-2 >= 2.4.42
40
41 libsasl2-modules-gssapi-mit >= 2.1.~
42
43 python-requests >= 2.9.1
44
45 libgoogle-perftools4 >= 2.4~
46
47 xserver-xorg-core >= 2:1.18
48
49 xserver-xorg-core << 2:1.19
50
51 x11vnc>=0.9.13
52
53 python-websocketify >= 0.6.1
54 <!--NeedCopy-->
```

Hinweis:

Eine Übersicht der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden, finden Sie in der Tabelle [Systemanforderungen](#).

Schritt 6b: Upgrade des Linux VDA (optional)

Sie können ein Upgrade für eine vorhandene Installation der vorherigen beiden Versionen und von einer LTSR-Version durchführen.

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
2 <!--NeedCopy-->
```

Hinweis:

Durch das Upgrade einer Installation werden die Konfigurationsdateien unter `/etc/xdl` überschrieben. Sichern Sie die Dateien vor jedem Upgrade.

Schritt 7: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro müssen Sie die NVIDIA GRID-Treiber auf Ihrem Hypervisor und auf den VDA-Maschinen installieren.

Informationen zum Installieren und Konfigurieren des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Handbüchern:

- [Citrix Hypervisor](#)
- [VMware ESX](#)
- [Nutanix AHV](#)

Zum Installieren und Konfigurieren der NVIDIA GRID-Gast-VM-Treiber führen Sie die folgenden allgemeinen Schritte aus:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM in der Hypervisor-Systemsteuerung eine GPU zu.
3. Starten Sie die VM.
4. Installieren Sie den Gast-VM-Treiber auf der VM.

Schritt 8: 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:

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

Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--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 Domännennamen (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 VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für den Linux VDA öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION=1 | 2 | 3 | 4 | 5** –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
 - 5 –PBIS

- **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 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Wenn Sie die LDAP-Portnummer als 389 angeben, fragt der Linux VDA jeden LDAP-Server in der angegebenen Domäne im Abfragemodus ab. Wenn es x Richtlinien und y Anzahl von LDAP-Servern gibt, führt der Linux VDA die Summe von X multipliziert mit Y-Abfragen aus. Wenn die Abfragezeit den Schwellenwert überschreitet, schlagen Sitzungsanmeldungen möglicherweise fehl. Für schnellere LDAP-Abfragen aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben die entsprechende LDAP-Portnummer als 3268 an. 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_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. ctx_xdl_fas_fas_list='FAS_Server_1_URL:Port_Number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts ([ctxvda](#)).

Der Standardpfad ist /usr/bin.

- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate:** Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

Sie können die Desktopumgebung für Sitzungsbenutzer auch über die folgenden Schritte ändern:

1. Erstellen Sie die Datei `.xsession` auf dem VDA im Verzeichnis **\$HOME/<username>**.
2. Geben Sie in der Datei `.xsession` eine auf Distributionen basierende Desktopumgebung an.

– **Für MATE-Desktop**

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

– **Für GNOME Classic-Desktop**

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

– **Für GNOME-Desktop**

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

3. Teilen Sie die 700-Dateiberechtigung mit dem Zielsitzungsbenutzer.

- **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.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

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

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N
```



```
2
3 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
  none>'
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

Sie müssen die Option **-E** mit dem Befehl “sudo” angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, 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:

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

```
11 CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \  
12 \  
13 CTX_XDL_HDX_3D_PRO=Y|N \  
14 \  
15 CTX_XDL_VDI_MODE=Y|N \  
16 \  
17 CTX_XDL_SITE_NAME=dns-name \  
18 \  
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \  
20 \  
21 CTX_XDL_SEARCH_BASE=search-base-set \  
22 \  
23 CTX_XDL_FAS_LIST='list-fas-servers' \  
24 \  
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \  
26 \  
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \  
28 \  
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \  
30 \  
31 CTX_XDL_TELEMETRY_PORT=port-number \  
32 \  
33 CTX_XDL_START_SERVICE=Y|N \  
34 \  
35 /opt/Citrix/VDA/sbin/ctxsetup.sh  
36 <!--NeedCopy-->
```

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:

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

Entfernen von Konfigurationsänderungen:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh  
2 <!--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.

Deinstallieren der Linux VDA-Software

Überprüfen, ob der Linux VDA installiert ist, und Anzeigen der Version des installierten Pakets:

```
1 dpkg -l xendesktopvda
2 <!--NeedCopy-->
```

Anzeigen weiterer Details:

```
1 apt-cache show xendesktopvda
2 <!--NeedCopy-->
```

Deinstallieren der Linux VDA-Software:

```
1 dpkg -r xendesktopvda
2 <!--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 9: Ausführen von XDPing

Mit `sudo /opt/Citrix/VDA/bin/xdping` können Sie Linux VDA-Umgebungen auf häufige Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter [XDPing](#).

Schritt 10: 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:

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
4 <!--NeedCopy-->
```

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
4 <!--NeedCopy-->
```

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl `service ctxmonitorservice stop`, bevor Sie die Dienste `ctxvda` und `ctxhdx` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl restart ctxvda
6 <!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
4 <!--NeedCopy-->
```

Schritt 11: Erstellen des Maschinenkatalogs in Citrix Virtual Apps oder Citrix Virtual Desktops

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:
 - Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
 - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- 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 12: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- 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.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter [Citrix Virtual Apps and Desktops 7 2206](#).

Manuelle Installation von Linux Virtual Delivery Agent für Debian

October 5, 2022

Wichtig:

Für Neuinstallationen empfehlen wir die Verwendung von [Easy Install](#) für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

Schritt 1: Vorbereiten von Debian für die VDA-Installation

Schritt 1a: Überprüfen der Netzwerkkonfiguration

Stellen Sie sicher, dass das Netzwerk verbunden und richtig konfiguriert ist. Beispielsweise müssen Sie den DNS-Server auf dem Linux VDA konfigurieren.

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

Vergewissern Sie sich, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine korrekt gemeldet werden. Sie können hierfür die folgende Zeile der Datei **/etc/hosts** durch den FQDN und den Hostnamen als erste beiden Einträge erweitern:

```
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 Hostname darf 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:

```
1 nslookup domain-controller-fqdn
2
3 ping domain-controller-fqdn
4
5 nslookup delivery-controller-fqdn
```

```
6
7 ping delivery-controller-fqdn
8 <!--NeedCopy-->
```

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

Schritt 1g: Konfigurieren der Uhrensynchronisierung (Chrony)

Es ist wichtig, dass die Uhrensynchronisierung 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:

```
1 apt-get install chrony
2 <!--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:

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

Schritt 1h: Installieren von Paketen

```
1 sudo apt-get install -y libssl2-2
2
3 sudo apt-get install -y libgtk2.0-0
4 <!--NeedCopy-->
```


Schritt 1i: Hinzufügen von Repositorys zur Installation notwendiger Abhängigkeiten

Für Debian 11.3 fügen Sie die Zeile `deb http://deb.debian.org/debian/ bullseye main` zur Datei `/etc/apt/sources.list` hinzu.

Für Debian 10.9 fügen Sie die Zeile `deb http://deb.debian.org/debian/ oldstable main` zur Datei `/etc/apt/sources.list` hinzu.

Schritt 1j: Installieren von PostgreSQL

Der Linux VDA erfordert PostgreSQL unter Debian:

```
1 sudo apt-get install -y postgresql
2
3 sudo apt-get install -y libpostgresql-jdbc-java
4 <!--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 basierend auf 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 Hypervisor

Wenn das Zeitsynchronisierungsfeature auf Citrix Hypervisor aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme mit NTP und Citrix Hypervisor auf. Beide 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.

Wenn ein paravirtualisierter Linux-Kernel mit installierten Citrix VM Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das Citrix Hypervisor-Zeitsynchronisierungsfeature vorhanden und aktiviert ist:

```
1 su -
2 cat /proc/sys/xen/independent_wallclock
3 <!--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/independent_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:

```
1 su -
2 cat /proc/sys/xen/independent_wallclock
3 <!--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 Citrix Hypervisor, 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 mit NTP und Hypervisor auf. Beide 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](#)
- [PBIS](#)

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

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

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

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

Hinweis:

Stellen Sie sicher, dass das `winbind`-Skript unter `/etc/init.d` ist.

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

Hinweis:

Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
[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
```

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

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
```

```
winbind trusted domains only = no
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

WORKGROUP 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: systemd winbind
group: systemd 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:

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

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

Neustarten von Winbind

```
1 sudo systemctl restart winbind
2 <!--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:

```
1 sudo pam-auth-update
2 <!--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:

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

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

```
1 sudo net ads info
2 <!--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:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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:

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

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

```
1 wbinfo --krb5auth=domain\username%password
2 <!--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 bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\username
2
3 id -u
4 <!--NeedCopy-->
```

Hinweis:

Um einen SSH-Befehl erfolgreich auszuführen, stellen Sie sicher, dass SSH aktiviert ist und ordnungsgemäß funktioniert.

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 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 6: 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:

```
1 sudo /opt/quest/bin/vastool configure pam  
2 sudo /opt/quest/bin/vastool configure nss  
3 <!--NeedCopy-->
```

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

```
1 sudo /opt/quest/bin/vastool -u user join domain-name  
2 <!--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:

```
1 sudo /opt/quest/bin/vastool info domain
2 <!--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 bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 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 gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: 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:

```
1 su -
2 adjoin -w -V -u user domain-name
3 <!--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 beitrifft.

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:

```
1 su -
2
3 adinfo
4 <!--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:

```
1 adinfo --sysinfo all
2
3 adinfo --diag
4 <!--NeedCopy-->
```

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

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

SSSD

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

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

Zum Konfigurieren von Kerberos öffnen Sie als Root-Benutzer **/etc/krb5.conf** und legen Sie folgende Parameter fest:

Hinweis:

Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
[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
```

Der Parameter `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 für **adcli** und **Samba**.

- **Wenn Sie der Domäne mit adcli beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie **adcli**.

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

2. Treten Sie mit **adcli** der Domäne bei.

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

```
1 su -
2
3 rm -rf /etc/krb5.keytab
4
5 adcli join domain-dns-name -U user -H hostname-fqdn
6 <!--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.

3. Überprüfen Sie die Systemschlüsseltabelle.

Führen Sie den Befehl `sudo klist -ket` aus, um sicherzustellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde.

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

• **Wenn Sie der Domäne mit Samba beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.

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

2. 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
```

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

3. Treten Sie der Domäne mit **Samba** bei.

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

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

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

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

```
1 sudo apt-get install --only-upgrade sssd
2 <!--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/sss/sss.conf** nicht standardmäßig installiert und muss manuell erstellt werden. Öffnen oder erstellen Sie als Root-Benutzer **/etc/sss/sss.conf** und nehmen Sie folgende Einstellungen vor:

```
[sss]
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
```

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.

Der Parameter **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-Domännennamens ist nicht erforderlich.

Weitere Informationen zu den Konfigurationseinstellungen finden Sie auf den Manpages über [sssd.conf](#) und [sssd-ad](#).

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

```
1 sudo chmod 0600 /etc/sssd/sssd.conf
2 <!--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:

```
1 sudo systemctl start sssd
2
3 sudo systemctl enable sssd
4 <!--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:

```
1 sudo pam-auth-update
2 <!--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.

- Wenn Sie die Domänenmitgliedschaft mit **adcli** überprüfen, führen Sie den Befehl `sudo adcli info domain-dns-name` aus, um die Domäneninformationen anzuzeigen.
- Wenn Sie die Domänenmitgliedschaft mit **Samba** überprüfen, führen Sie den Befehl `sudo net ads testjoin` aus, um zu überprüfen, ob die Maschine Mitglied einer Domäne ist, und den Befehl `sudo net ads info` zum Überprüfen zusätzlicher Domänen- und Computerobjektinformationen.

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:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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 für das Maschinenkonto zwischengespeichert wurde:

```
1 sudo klist
2 <!--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 bislang noch nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 ssh localhost -l domain\username
2
3 id -u
4
5 klist
6
7 exit
8 <!--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:

```
1 ls /tmp/krb5cc_uid
2 <!--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 6: Installieren des Linux VDA](#) fort.

PBIS

Download des erforderlichen PBIS-Pakets

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

Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei

```
1 sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

Ausführen des PBIS-Installationsskripts

```
1 sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
2 <!--NeedCopy-->
```

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:

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

user ist ein Domänenbenutzer mit der Berechtigung, Computer zur Active Directory-Domäne hinzuzufügen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Hinweis: Führen Sie den Befehl **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** aus, um Bash als Standardshell festzulegen.

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 PBIS angemeldete Linux-Maschine zur Domäne gehört:

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

Wenn die Maschine einer Domäne beigetreten ist, werden mit diesem Befehl Informationen zur aktuell beigetretenen AD-Domäne und Organisationseinheit abgefragt. Andernfalls wird nur der Hostname angezeigt.

Überprüfen der Benutzerauthentifizierung Um sicherzustellen, dass PBIS Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
1 sudo ssh localhost -l domain\user
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-->
```

Beenden Sie die Sitzung.

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

Fahren Sie nach der Überprüfung des Domänenbeitritts mit [Schritt 6: Installieren des Linux VDA](#) fort.

Schritt 4: Installieren von .NET Runtime 6.0 als Voraussetzung

Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.

Führen Sie nach der Installation von .NET Runtime 6.0 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite. Erweitern Sie die passende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das für Ihre Linux-Distribution geeignete Linux VDA-Paket herunterzuladen.

Schritt 6: Installieren des Linux VDA

Schritt 6a: Installieren des Linux VDA

Installieren Sie die Linux VDA-Software mit dem Debian-Paketmanager:

```
1 sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
2 <!--NeedCopy-->
```

Abhängigkeitsliste für Debian 11.3:

```
1 postgresql >= 13
2 libpostgresql-jdbc-java >= 42.2
3 openjdk-11-jdk >= 11
4 imagemagick >= 8:6.9.10
5 ufw >= 0.36
6 desktop-base >= 10.0.2
7 libxrandr2 >= 2:1.5.1
8 libxtst6 >= 2:1.2.3
9 libxm4 >= 2.3.8
10 util-linux >= 2.33
11 gtk3-nocsd >= 3
12 bash >= 5.0
13 findutils >= 4.6.0
14 sed >= 4.7
15 cups >= 2.2
16 ghostscript >= 9.53~
17 libmspack0 >= 0.10
18 ibus >= 1.5
```

```
19 libgoogle-perftools4      >= 2.7~
20 libpython3.9               >= 3.9~
21 libsasl2-modules-gssapi-mit >= 2.1.~
22 libqt5widgets5            >= 5.5~
23 mutter                     >= 3.38.6~
24 libqrencode4               >= 4.0.0
25 libimlib2                  >= 1.5.1
26 <!--NeedCopy-->
```

Abhängigkeitsliste für Debian 10.9:

```
1  libqt5widgets5            >= 5.5~
2  ibus                      >= 1.5
3  postgresql                >= 11
4  libpostgresql-jdbc-java   >= 42.2
5  openjdk-11-jdk            >= 11
6  imagemagick               >= 8:6.9.10
7  ufw                       >= 0.36
8  desktop-base              >= 10.0.2
9  libxrandr2                >= 2:1.5.1
10 libxtst6                  >= 2:1.2.3
11 libxm4                    >= 2.3.8
12 util-linux                >= 2.33
13 gtk3-nocsd                >= 3
14 bash                      >= 5.0
15 findutils                 >= 4.6.0
16 sed                       >= 4.7
17 cups                      >= 2.2
18 ghostscript               >= 9.27~
19 libmspack0                >= 0.10
20 libgoogle-perftools4      >= 2.7~
21 libpython2.7               >= 2.7~
22 libsasl2-modules-gssapi-mit >= 2.1.~
23 <!--NeedCopy-->
```

Hinweis:

Eine Übersicht der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden, finden Sie in der Tabelle [Systemanforderungen](#).

Schritt 6b: Upgrade des Linux VDA (optional)

Sie können ein Upgrade für eine vorhandene Installation der vorherigen beiden Versionen und von einer LTSR-Version durchführen.

```
1 sudo dpkg -i <PATH>/<Linux VDA deb>
2 <!--NeedCopy-->
```

Hinweis:

Durch das Upgrade einer Installation werden die Konfigurationsdateien unter `/etc/xdl` überschrieben. Sichern Sie die Dateien vor jedem Upgrade.

Schritt 7: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro müssen Sie die NVIDIA GRID-Treiber auf Ihrem Hypervisor und auf den VDA-Maschinen installieren.

Informationen zum Installieren und Konfigurieren des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Handbüchern:

- [Citrix Hypervisor](#)
- [VMware ESX](#)
- [Nutanix AHV](#)

Zum Installieren und Konfigurieren der NVIDIA GRID-Gast-VM-Treiber führen Sie die folgenden allgemeinen Schritte aus:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM in der Hypervisor-Systemsteuerung eine GPU zu.
3. Starten Sie die VM.
4. Installieren Sie den Gast-VM-Treiber auf der VM.

Schritt 8: 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:

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

Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
1 sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
2 <!--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 Domännennamen (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 VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für den Linux VDA öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION=1 | 2 | 3 | 4 | 5** –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
 - 5 –PBIS
- **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 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 ad2.mycompany.com:3268 ad3.mycompany.com:3268. Wenn Sie die LDAP-Portnummer als 389 angeben, fragt der Linux VDA jeden LDAP-Server in der angegebenen Domäne im Abfragemodus ab. Wenn es x Richtlinien und y Anzahl von LDAP-Servern gibt, führt der Linux VDA die Summe von x multipliziert mit y-Abfragen aus. Wenn die Abfragezeit den Schwellenwert überschreitet, schlagen Sitzungsanmeldungen möglicherweise fehl. Für schnellere LDAP-Abfragen aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben die entsprechende LDAP-Portnummer als 3268 an. 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_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. ctx_xdl_fas_fas_list='FAS_Server_1_URL:Port_Number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (**ctxvda**). Der Standardpfad ist /usr/bin.

- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate:** Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

Sie können die Desktopumgebung für Sitzungsbenutzer auch über die folgenden Schritte ändern:

1. Erstellen Sie die Datei `.xsession` auf dem VDA im Verzeichnis **\$HOME/<username>**.
2. Geben Sie in der Datei `.xsession` eine auf Distributionen basierende Desktopumgebung an.

– **Für MATE-Desktop**

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

– **Für GNOME Classic-Desktop**

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

– **Für GNOME-Desktop**

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

3. Teilen Sie die 700-Dateiberechtigung mit dem Zielsitzungsbenutzer.

- **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.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

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

```
1 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
2
3 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
```



```

4
5 export CTX_XDL_VDA_PORT=port-number
6
7 export CTX_XDL_REGISTER_SERVICE=Y|N
8
9 export CTX_XDL_ADD_FIREWALL_RULES=Y|N
10
11 export CTX_XDL_AD_INTEGRATION=1|2|3|4|5
12
13 export CTX_XDL_HDX_3D_PRO=Y|N
14
15 export CTX_XDL_VDI_MODE=Y|N
16
17 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
18
19 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
20
21 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
22
23 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
24
25 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
26
27 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
  none>'
28
29 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
30
31 export CTX_XDL_TELEMETRY_PORT=port-number
32
33 export CTX_XDL_START_SERVICE=Y|N
34
35 sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->

```

Sie müssen die Option **-E** mit dem Befehl “sudo” angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, 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:

```

1 sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \
2
3 CTX_XDL_DDC_LIST='list-ddc-fqdns' \
4
5 CTX_XDL_VDA_PORT=port-number \
6
7 CTX_XDL_REGISTER_SERVICE=Y|N \
8
9 CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \
12

```

```
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh
36 <!--NeedCopy-->
```

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:

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

Entfernen von Konfigurationsänderungen:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--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.

Deinstallieren der Linux VDA-Software

Überprüfen, ob der Linux VDA installiert ist, und Anzeigen der Version des installierten Pakets:

```
1 dpkg -l xendesktopvda
2 <!--NeedCopy-->
```

Anzeigen weiterer Details:

```
1 apt-cache show xendesktopvda
2 <!--NeedCopy-->
```

Deinstallieren der Linux VDA-Software:

```
1 dpkg -r xendesktopvda
2 <!--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 9: Ausführen von XDPing

Mit `sudo /opt/Citrix/VDA/bin/xdping` können Sie Linux VDA-Umgebungen auf häufige Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter [XDPing](#).

Schritt 10: 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:

```
1 sudo systemctl start ctxhdx
2
3 sudo systemctl start ctxvda
```

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

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl stop ctxhdx
4 <!--NeedCopy-->
```

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl `service ctxmonitorservice stop`, bevor Sie die Dienste `ctxvda` und `ctxhdx` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
1 sudo systemctl stop ctxvda
2
3 sudo systemctl restart ctxhdx
4
5 sudo systemctl restart ctxvda
6 <!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
1 sudo systemctl status ctxvda
2
3 sudo systemctl status ctxhdx
4 <!--NeedCopy-->
```

Schritt 11: Erstellen des Maschinenkatalogs in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
 - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- 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 12: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps oder Citrix Virtual Desktops

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:

- 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.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter [Citrix Virtual Apps and Desktops 7 2206](#).

Linux VDAs in Citrix DaaS Standard für Azure erstellen

June 19, 2023

Sie können Linux VDAs in Domänen, sowie solche die es nicht sind, in Citrix DaaS Standard für Azure (früher Citrix Virtual Apps and Desktops Standard für Azure) erstellen, um virtuelle Apps und Desktops über Microsoft Azure auf beliebigen Geräten bereitzustellen. Weitere Informationen finden Sie unter [Citrix DaaS Standard for Azure](#).

Unterstützte Linux-Distributionen

Die folgenden Linux-Distributionen unterstützen dieses Feature:

- RHEL 8.2
- Ubuntu 20.04
- Ubuntu 18.04

Schritte

Führen Sie die folgenden Schritte aus, um Linux VDAs in Citrix DaaS Standard für Azure zu erstellen:

1. Bereiten Sie ein Masterimage in Azure vor:

Hinweis:

Mit dem Feature [Linux VDA-Selbstupdate](#) können Sie auch automatische Softwareupdates planen. Fügen Sie hierzu der Datei `etc/xdm/mcs/mcs_local_setting.reg` im Masterimage Befehlszeilen hinzu.

Beispiel:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" -
   force
2
3 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately"
   - force
4
5 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-
   Url>" - force
6
7 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
   SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-
   Certificate-Path-of-PortalAzureCom>" --force
```

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

- a) Erstellen Sie in Azure eine Linux-VM einer unterstützten Distribution.
- b) Installieren Sie bei Bedarf eine Desktopumgebung auf der Linux-VM.
- c) Installieren Sie .NET Runtime 6.0 auf der VM gemäß den Anweisungen unter <https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers>.
- d) (Nur für Ubuntu) Fügen Sie die Zeile `source /etc/network/interfaces.d/*` in der Datei `/etc/network/interfaces` hinzu.
- e) (Nur für Ubuntu) Sorgen Sie dafür, dass `/etc/resolv.conf` auf `/run/systemd/resolve/resolv.conf` verweist anstatt auf `/run/systemd/resolve/stub-resolv.conf`:

```
1 unlink /etc/resolv.conf
2
3 ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
4 <!--NeedCopy-->
```

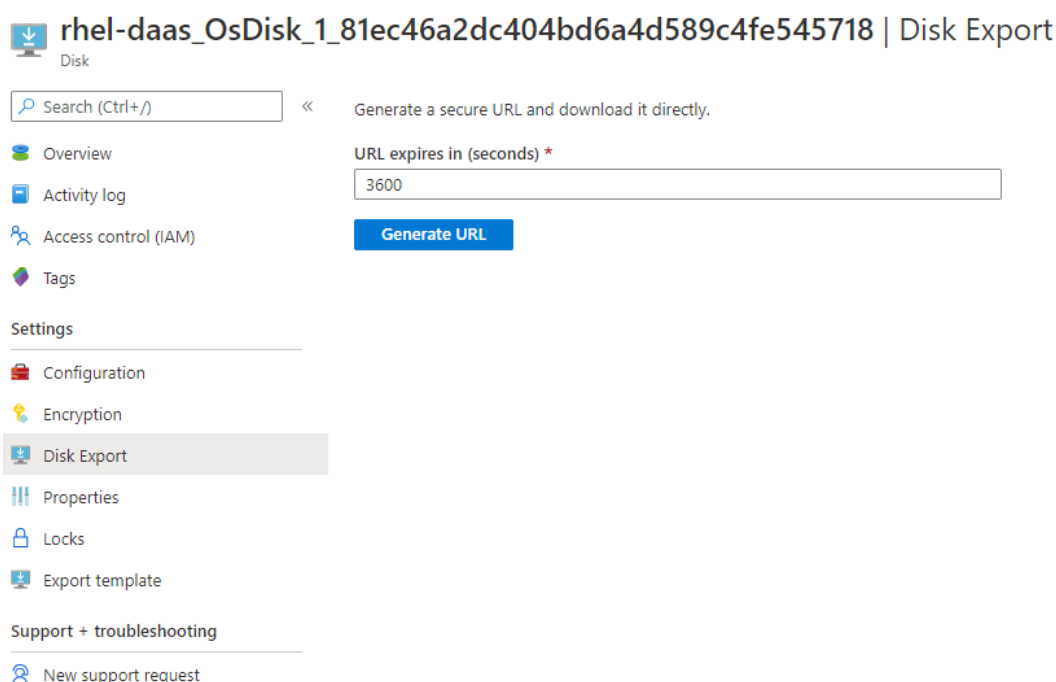
- f) Installieren Sie das Linux VDA-Paket.
- g) Ändern Sie die Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Einrichten von MCS und Linux VDA.

Hinweis:

Geben Sie die DNS-Variable nicht an.

Wenn Sie beim Erstellen eines Maschinenkatalogs den Typ **Statisch** oder **Zufällig** auswählen, legen Sie `VDI_MODE=Y` fest.

- h) Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
- i) Beenden Sie die VM in Azure (oder heben Sie die Zuordnung auf). Klicken Sie auf **Datenträgerexport**, um eine SAS-URL für die VHD-Datei zu generieren, die Sie als Masterimage zum Erstellen anderer VMs verwenden können.



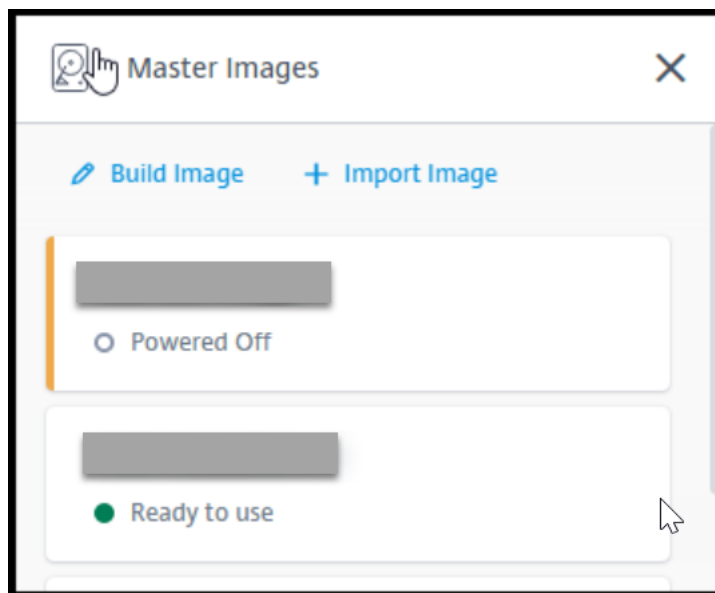
- j) (Optional) Nehmen Sie Gruppenrichtlinieneinstellungen auf dem Masterimage vor. Sie können das Tool `ctxreg` verwenden, um Gruppenrichtlinieneinstellungen vorzunehmen. Mit dem folgenden Befehl wird beispielsweise die Richtlinie **Universellen PDF-Drucker automatisch erstellen** für den PDF-Druck aktiviert.

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

2. Importieren Sie das Masterimage aus Azure.

- a) Erweitern Sie im Dashboard **Verwalten** rechts **Masterimages**. In der Anzeige werden die von Citrix bereitgestellte Masterimages sowie die von Ihnen erstellten und importierten Images aufgeführt.

Tipp: Die meisten Administratoraktivitäten für diesen Dienst werden über die Dashboards **Verwalten** und **Überwachen** verwaltet. Nach dem Erstellen Ihres ersten Katalogs wird das Dashboard **Verwalten** automatisch gestartet, wenn Sie sich bei Citrix Cloud angemeldet und den Dienst **Managed Desktops** ausgewählt haben.



- b) Klicken Sie auf **Image importieren**.
- c) Geben Sie die SAS-URL für die in Azure generierte VHD-Datei ein. Wählen Sie **Linux** als Masterimagetyp aus.

Import Image from Azure

Enter the Azure-generated URL for the Virtual Hard Disk ?

[How do I find my Url?](#)

Master image type

- ☐ Windows
- ☒ Linux

Name The New Master Image

- d) Folgen Sie den Anweisungen im Assistenten, um den Import des Masterimages abzuschließen.
3. Erstellen Sie einen Maschinenkatalog.

Öffnen Sie das Dashboard [Verwalten](#) und klicken Sie auf **Katalog erstellen**. Wählen Sie beim Erstellen des Maschinenkatalogs das Masterimage aus, das Sie zuvor erstellt haben.

Hinweis:

Sie können nicht über SSH oder RDP auf die VM zugreifen, die als Masterimage verwendet wird. Um auf die VM zuzugreifen, verwenden Sie die serielle Konsole im Azure-Portal.

Erstellen von Linux-VMs mit Maschinenerstellungsdiensten (MCS)

January 8, 2024

Unterstützte Distributionen

	Winbind	SSSD	Centrify	PBIS
Debian 11.3, Debian 10.9	Ja	Ja	Nein	Ja
RHEL 8.4, RHEL 8.2	Ja	Nein	Ja	Ja
RHEL 7.9, CentOS 7.9	Ja	Ja	Ja	Ja
SUSE 15.3, SUSE 15.2	Ja	Ja	Nein	Ja
Ubuntu 20.04, Ubuntu 18.04	Ja	Ja	Nein	Ja

Unterstützte Hypervisors

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

Das Vorbereiten des Masterimages auf einem anderen Hypervisor als den unterstützten kann zu unerwarteten Ergebnissen führen.

MCS zum Erstellen von Linux-VMs verwenden

Hinweis:

Von Citrix Virtual Apps and Desktops 7 2003 bis Citrix Virtual Apps and Desktops 7 2112 wurde das Hosten des Linux VDA auf Microsoft Azure, AWS und GCP nur für Citrix DaaS (früher Citrix Virtual Apps and Desktops Service) unterstützt. Ab Release 2203 können Sie den Linux VDA auf diesen öffentlichen Clouds sowohl für Citrix DaaS als auch für Citrix Virtual Apps and Desktops hosten. Um diese Verbindungen mit Hosts öffentlicher Clouds zu Ihrer Citrix Virtual Apps and Desktops-Bereitstellung hinzuzufügen, benötigen Sie eine Hybrid Rights-Lizenz. Informationen zur Hybrid Rights-Lizenz finden Sie unter [Transition und Trade-Up \(TTU\) mit Hybrid Rights](#).

Bare-Metal-Server werden nicht unterstützt, wenn MCS zum Erstellen virtueller Maschinen verwendet wird.

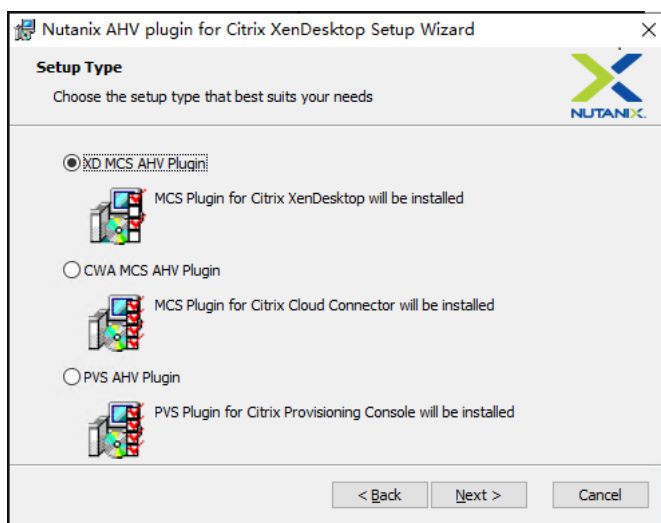
Wenn Sie PBIS oder Centrify zum Hinzufügen von mit MCS erstellten Maschinen zu Windows-Domänen verwenden, führen Sie die folgenden Aufgaben aus:

- Konfigurieren Sie auf der Vorlagenmaschine den Downloadpfad des PBIS- bzw. Centrify-Pakets in der Datei `/etc/xdl/mcs/mcs.conf` oder installieren Sie das Paket direkt.
- Erstellen Sie vor dem Ausführen von `/opt/Citrix/VDA/sbin/deploymcs.sh` eine Organisationseinheit mit Schreib- und Kennworrücksetzberechtigung für alle untergeordneten, mit MCS erstellten Maschinen.
- Bevor Sie mit MCS erstellte Maschinen nach Abschluss der Ausführung von `/opt/Citrix/VDA/sbin/deploymcs.sh` neu starten, führen Sie je nach Bereitstellung `klist -li 0x3e4 purge` auf Ihrem Delivery Controller oder Citrix Cloud Connector aus.

Schritt 1 (nur für Nutanix): Installieren und Registrieren des Nutanix-AHV-Plug-Ins

Beschaffen Sie das Nutanix AHV Plug-In-Paket von Nutanix. Installieren und registrieren Sie das Plug-In in der Citrix Virtual Apps and Desktops-Umgebung. Weitere Informationen finden Sie in der Installationsdokumentation zum Nutanix Acropolis MCS-Plug-In, verfügbar im [Nutanix Support Portal](#).

Schritt 1a: Installieren und Registrieren des Nutanix AHV-Plug-Ins für On-Premises-Delivery Controller Nach Installation von Citrix Virtual Apps and Desktops wählen und installieren Sie **XD MCS AHV Plugin** auf den Delivery Controllern.



Schritt 1b: Installieren und Registrieren des Nutanix AHV-Plug-Ins für Cloud-Delivery Controller Wählen und installieren Sie **CWA MCS AHV Plugin** für Citrix Cloud Connectors. Installieren Sie das Plug-In auf allen Citrix Cloud Connectors, die beim Citrix Cloud-Mandanten registriert sind. Sie müssen Citrix Cloud Connectors auch dann registrieren, wenn sie einen Ressourcenstandort ohne AHV bereitstellen.

Schritt 1c: Ausführen der nachfolgend aufgeführten Schritte nach der Plug-In-Installation

- Vergewissern Sie sich, dass in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0` ein Nutanix Acropolis-Ordner erstellt wurde.
- Führen Sie den Befehl "`C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe`"-PluginsRoot "`C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0`" aus.
- Starten Sie den Citrix Host, Citrix Broker und Citrix Maschinenerstellungsdienste auf den On-Premises-Delivery Controllern neu bzw. starten Sie auf Citrix Cloud Connectors Citrix Remote-HCLServer neu.

Tipp:

Wir empfehlen, den Citrix Host, den Citrix Broker und Maschinenerstellungsdienste zu beenden und neu zu starten, wenn Sie das Nutanix-AHV-Plug-In installieren oder aktualisieren.

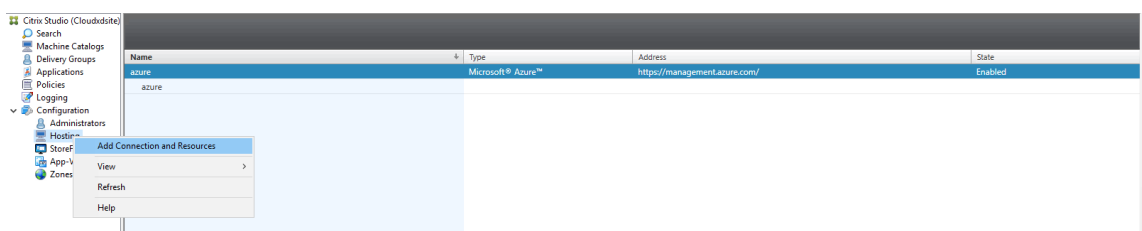
Schritt 2: Erstellen einer Hostingverbindung

Dieser Abschnitt führt Sie durch das Erstellen einer Hostingverbindung zu Azure, AWS, GCP, Nutanix AHV und VMware vSphere:

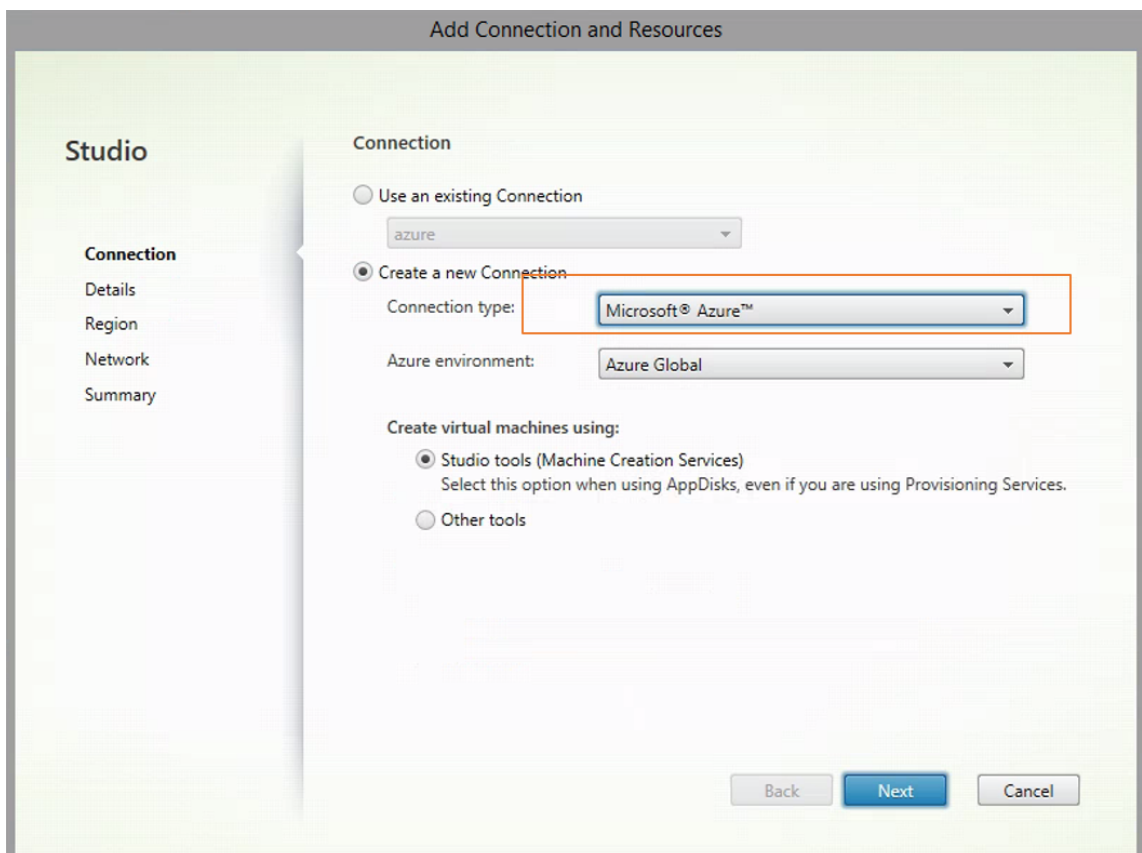
- [Hostverbindung zu Azure in Citrix Studio erstellen](#)
- [Hostverbindung zu AWS in Citrix Studio erstellen](#)
- [Hostverbindung zu GCP in Citrix Studio erstellen](#)
- [Hostverbindung zu Nutanix in Citrix Studio erstellen](#)
- [Hostverbindung zu VMware in Citrix Studio erstellen](#)

Hostverbindung zu Azure in Citrix Studio erstellen

1. Wählen Sie in Citrix Studio in Citrix Cloud **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu Azure herzustellen.



2. Wählen Sie als Verbindungstyp “Microsoft Azure”.



3. Geben Sie die Abonnement-ID Ihres Azure-Kontos und Ihren Verbindungsnamen ein.

Add Connection and Resources

Studio

- ✓ Connection
 - Details**
 - Region
 - Network
 - Summary

Connection Details

A service principal in the subscription's Azure Active Directory is required. Create a new service principal or provide details of an existing service principal.

The Azure service principal is assigned the Contributor role at the subscription scope. The service principal has permission to create and manage all types of Azure resources in the subscription, and may have access to resources that are unrelated to the deployment of resources in the catalog. (Permissions at the subscription scope are required to create resource groups.)

Learn more:

- [Setting up an Azure Active Directory account](#)
- [Creating a host connection](#)
- [Azure role based access control](#)

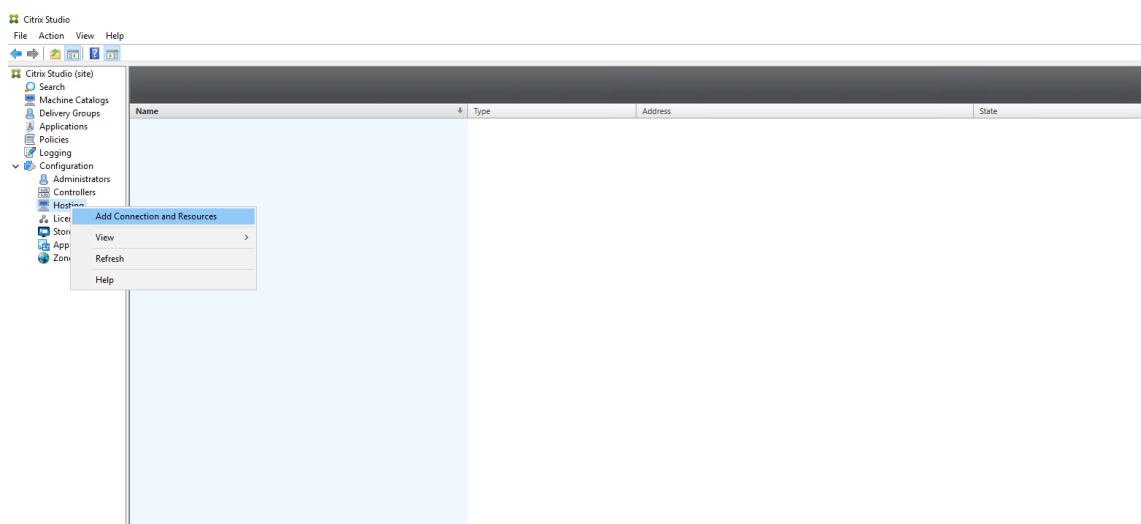
Subscription ID:

Connection name:

Create new... Use existing...

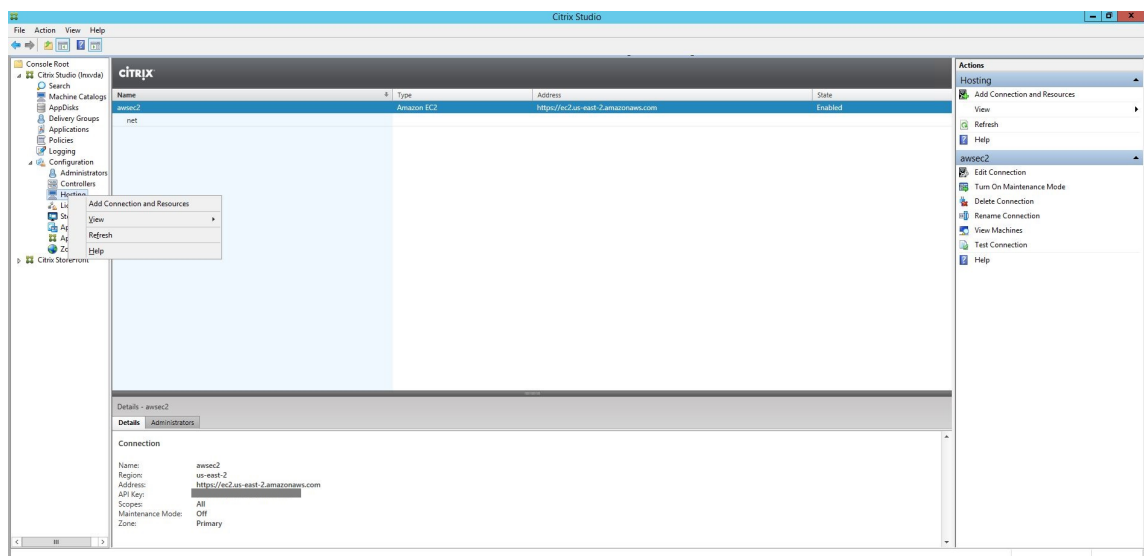
Back Next Cancel

Eine neue Verbindung wird im Hostingbereich angezeigt.

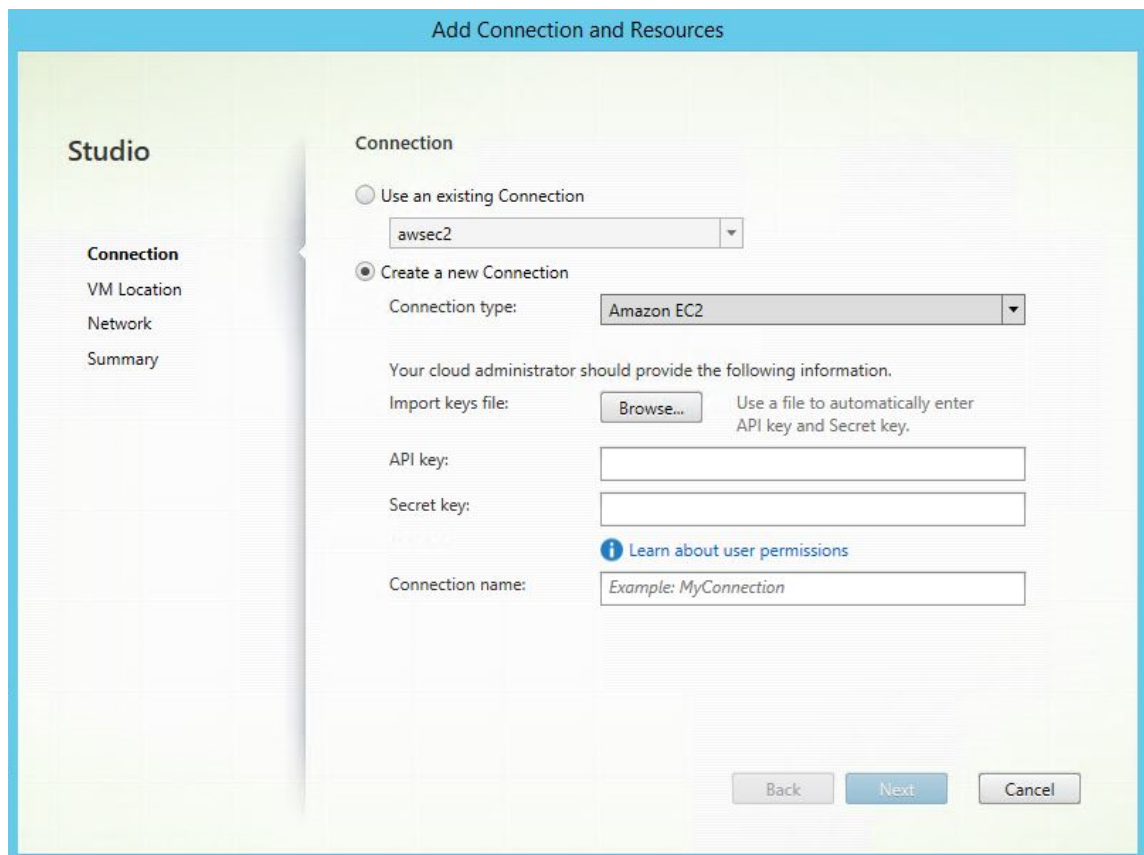


Hostverbindung zu AWS in Citrix Studio erstellen

1. Wählen Sie in Citrix Studio in Citrix Cloud **Konfiguration** > **Hosting** > **Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu AWS herzustellen.



2. Wählen Sie als Verbindungstyp **Amazon EC2** aus.



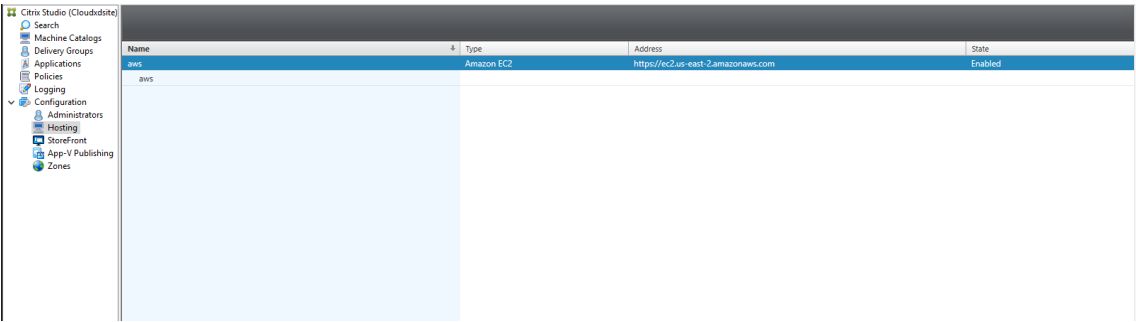
3. Geben Sie den API-Schlüssel und den geheimen Schlüssel Ihres AWS-Kontos und Ihren Verbindungsnamen ein.

The screenshot shows the 'Add Connection and Resources' window in the Studio application. The 'Connection' tab is selected in the left sidebar. The main area is divided into two sections: 'Use an existing Connection' (which is not selected) and 'Create a new Connection' (which is selected). Under 'Create a new Connection', the 'Connection type' is set to 'Amazon EC2'. Below this, there is a note: 'Your cloud administrator should provide the following information.' The 'Import keys file' section has a 'Browse...' button and a description: 'Use a file to automatically enter API key and Secret key.' Below this are two input fields for 'API key' and 'Secret key'. A link 'Learn about user permissions' is provided. The 'Connection name' field has a placeholder 'Example: MyConnection'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Der **API-Schlüssel** ist Ihre Zugriffsschlüssel-ID und der **geheime Schlüssel** ist Ihr geheimer Zugriffsschlüssel. Beide zusammen sind das Zugriffsschlüsselpaar. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, können Sie den Zugriffsschlüssel löschen und einen anderen erstellen. Gehen Sie folgendermaßen vor, um einen Zugriffsschlüssel zu erstellen:

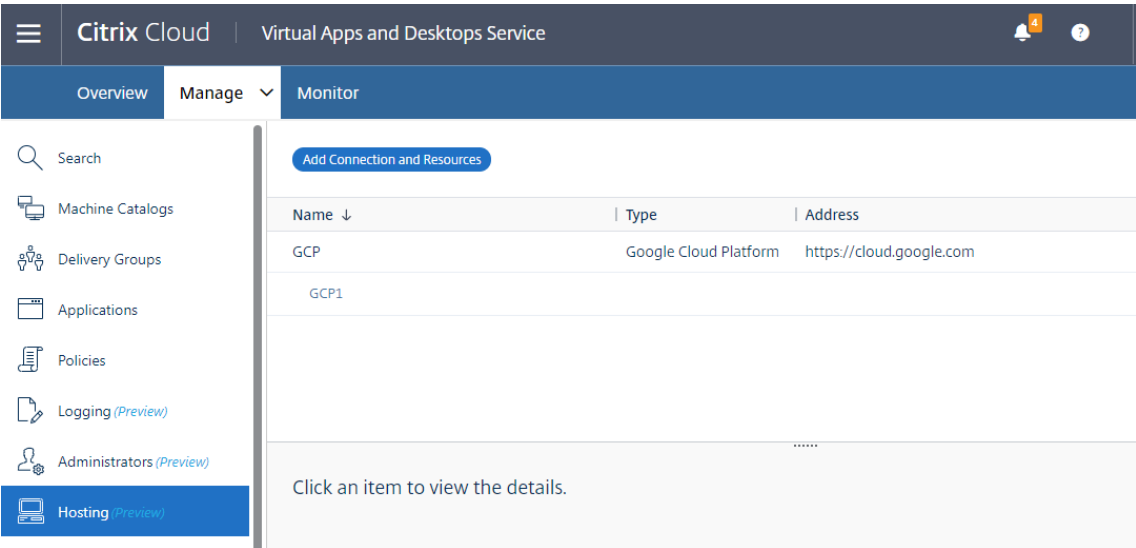
- Melden Sie sich bei AWS an.
- Navigieren Sie zur IAM-Konsole (Identity and Access Management).
- Wählen Sie im linken Navigationsbereich **Users** aus.
- Wählen Sie den Zielbenutzer aus und scrollen Sie nach unten, um die Registerkarte **Security credentials** auszuwählen.
- Scrollen Sie nach unten und klicken Sie auf **Create access key**. Ein neues Fenster wird angezeigt.
- Klicken Sie auf **Download .csv file** und speichern Sie den Zugriffsschlüssel an einem sicheren Speicherort.

Eine neue Verbindung wird im Hostingbereich angezeigt.



Hostverbindung zu GCP in Citrix Studio erstellen Richten Sie Ihre GCP-Umgebung gemäß [Google Cloud Platform-Virtualisierungsumgebungen](#) ein und führen Sie dann die folgenden Schritte aus, um eine Hostingverbindung zu GCP herzustellen.

1. Wählen Sie in Citrix Studio in Citrix Cloud **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu GCP herzustellen.



2. Wählen Sie als Verbindungstyp die Option **Google Cloud Platform**.

Add Connection and Resources

1 Connection

2 Region

3 Network

4 Summary

☒ Create a new Connection

Connection type:

Google Cloud Platform

Service account key:

Import key...

Service account ID:

Zone name:

GCP

Connection name:

Create virtual machines using:
☒ Studio tools (Machine Creation Services)
☐ Other tools

Next

Cancel

3. Importieren Sie den Dienstkontoschlüssel Ihres GCP-Kontos und geben Sie Ihren Verbindungsnamen ein.

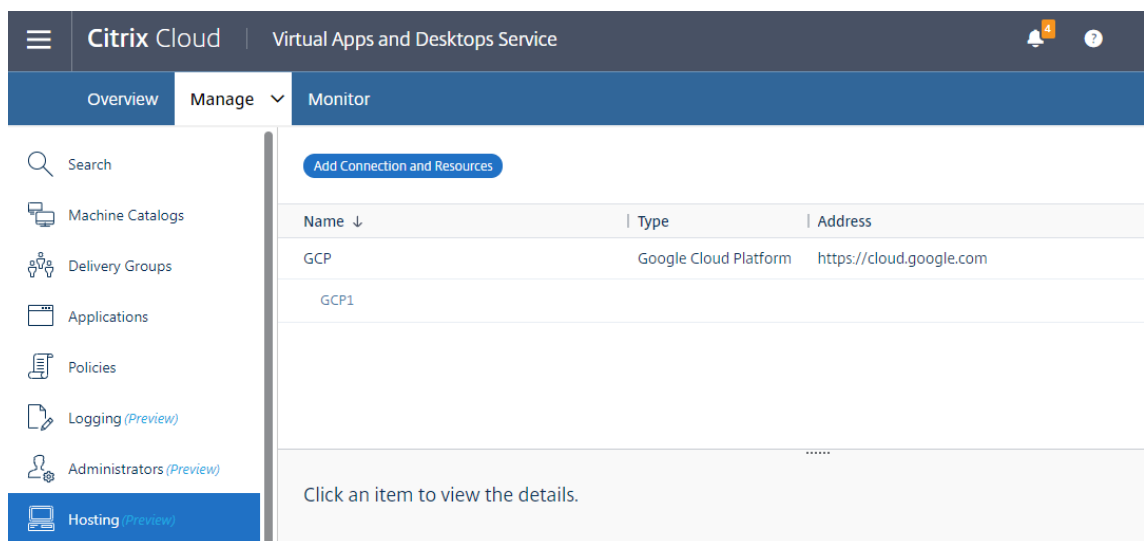
Google Cloud Platform Service Account Credentials

Paste the key contained in your Google service account credential file (.json).

Save

Cancel

Eine neue Verbindung wird im Hostingbereich angezeigt.



Hostverbindung zu Nutanix in Citrix Studio erstellen

1. Wählen Sie für On-Premises-Delivery Controller im On-Premises-Citrix Studio **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**. Wählen Sie für Cloud-Delivery Controller **Verwalten > Hosting > Verbindung und Ressourcen hinzufügen** in der webbasierten Studio-Konsole in Citrix Cloud, um eine Verbindung zum Nutanix-Hypervisor herzustellen.
2. Wählen Sie im Assistenten zum Hinzufügen einer Verbindung und Ressourcen auf der Seite **Verbindung** den Verbindungstyp **Nutanix AHV**. Geben Sie dann die Hypervisoradresse und Anmeldeinformationen sowie Ihren Verbindungsnamen ein. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit aus.

Beispiel für On-Premises-Citrix Studio:

The screenshot shows the 'Add Connection and Resources' wizard in Citrix Studio, specifically the 'Network' step. On the left, a sidebar shows the progression: 'Connection' (checked), 'Network' (active), and 'Summary'. The main area is titled 'Network' and contains a text input field for 'Name for these resources:'. Below this, a note states: 'The name helps identify the storage and network combination associated with the connection.' Further down, it says 'Select one or more networks for the virtual machines to use:'. A list box shows two options: 'INTERNAL_1' and 'VM', both with checkboxes. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

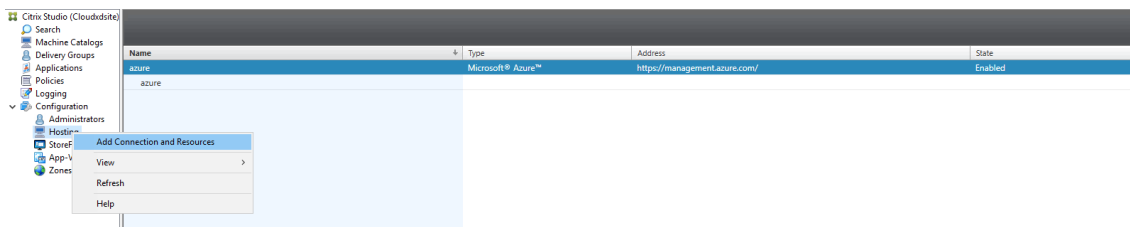
Beispiel für die webbasierte Studio-Konsole in Citrix Cloud:

The screenshot shows the 'Add Connection and Resources' wizard in Citrix Cloud Studio, specifically the 'Connection' step. On the left, a sidebar shows the progression: '1 Connection' (active), '2 Network', and '3 Summary'. The main area is titled 'Add Connection and Resources' and contains a radio button for 'Create a new Connection'. Below this, there are several input fields: 'Connection type:' (dropdown menu with 'Nutanix AHV' selected), 'Connection address:' (text input with placeholder 'Example: acropolis.example.com'), 'User name:', 'Password:', 'Zone name:' (dropdown menu with 'My Resource Location' selected), and 'Connection name:'. At the bottom, there is a label 'Create virtual machines using:' followed by a text input field. At the bottom right, there are 'Next' and 'Cancel' buttons.

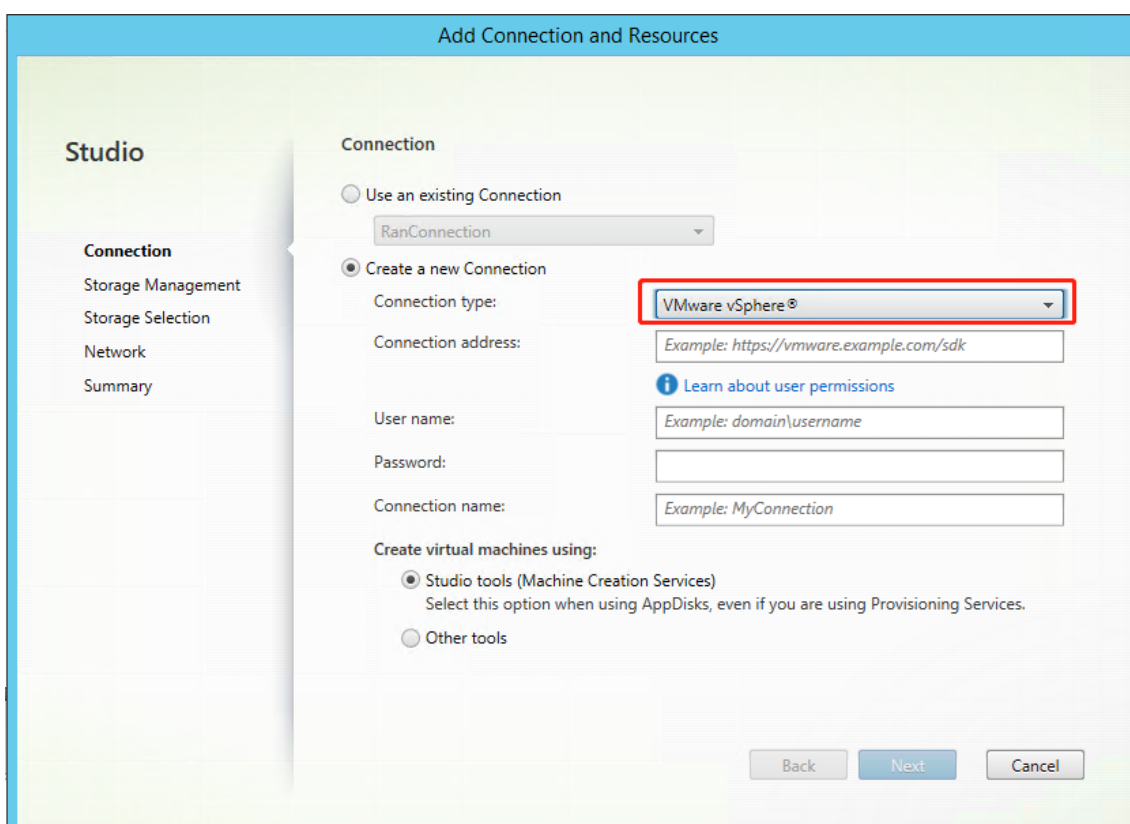
3. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit aus.

Hostverbindung zu VMware in Citrix Studio erstellen

1. Installieren Sie vCenter Server in der vSphere-Umgebung. Weitere Informationen finden Sie unter [VMware vSphere](#).
2. Wählen Sie in Citrix Studio **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu VMware vSphere herzustellen.



3. Wählen Sie als Verbindungstyp "VMware vSphere" aus.



4. Geben Sie die Verbindungsadresse (die vCenter Server-URL) Ihres VMware-Kontos, Ihren Benutzernamen und Ihr Kennwort sowie Ihren Verbindungsnamen ein.

Add Connection and Resources

Studio

- Connection
- Storage Management
- Storage Selection
- Network
- Summary

Connection

☐ Use an existing Connection

☐ Create a new Connection

Connection type: VMware vSphere®

Connection address: Example: <https://vmware.example.com/sdk>

User name: Example: domain\username

Password:

Connection name: Example: MyConnection

Learn about user permissions

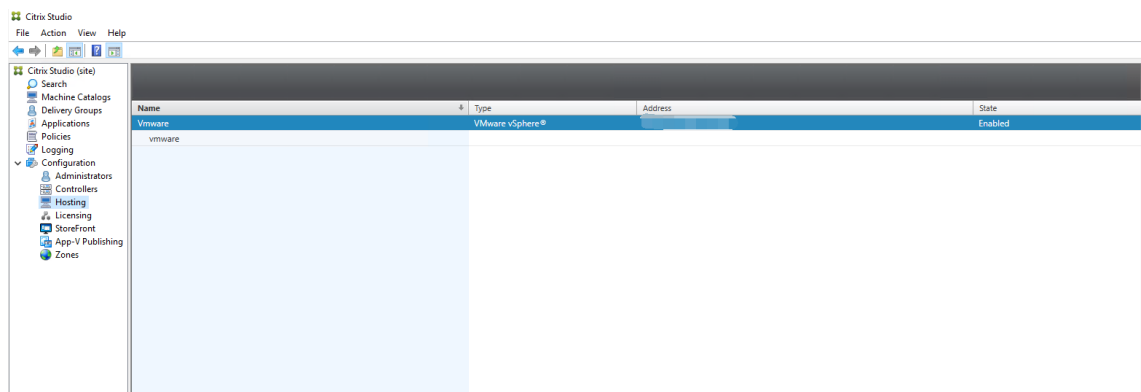
Create virtual machines using:

☒ Studio tools (Machine Creation Services)
Select this option when using AppDisks, even if you are using Provisioning Services.

☐ Other tools

Back Next Cancel

Eine neue Verbindung wird im Hostingbereich angezeigt.



Schritt 3: Masterimage vorbereiten

(Nur für Citrix Hypervisor) Schritt 3a: Citrix VM Tools installieren Installieren Sie Citrix VM Tools auf der Vorlagen-VM für jede VM, die die xe-Befehlszeilenschnittstelle oder XenCenter verwenden soll. Die VM kann langsam sein, wenn Sie die Tools nicht installieren. Folgende Schritte sind ohne diese Tools nicht möglich:

- Herunterfahren, Neustarten oder Anhalten einer VM.
- Anzeige der VM-Leistungsdaten in XenCenter.

- Migrieren einer ausgeführten VM (über [XenMotion](#)).
 - Erstellen von Prüfpunkten (Snapshots mit oder ohne Arbeitsspeicher) und Wiederherstellen der Snapshots
 - Anpassen der Anzahl der vCPUs auf einer laufenden Linux-VM.
1. Führen Sie folgenden Befehl aus, um Citrix VM Tools bereitzustellen (Dateiname: guest-tools.iso).

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

2. Führen Sie je nach Linux-Distribution folgenden Befehl aus, um das Paket `xe-guest-utilities` zu installieren.

RHEL/CentOS:

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

Ubuntu/Debian:

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

SUSE:

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

3. Überprüfen Sie den Virtualisierungsstatus der Vorlagen-VM auf der Registerkarte **Allgemein** in XenCenter. Wenn Citrix VM Tools ordnungsgemäß installiert ist, wird der Virtualisierungsstatus als **Optimiert** angezeigt.

(Für Azure, AWS und GCP) Schritt 3b: Konfigurieren von cloud-init für Ubuntu 18.04

1. Um sicherzustellen, dass ein VDA-Hostname beim Neustart oder Beenden einer VM beibehalten wird, führen Sie den folgenden Befehl aus:

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

Überprüfen Sie, ob die folgenden Zeilen im Abschnitt **system_info** in der Datei `/etc/cloud/cloud.cfg` vorhanden sind:

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

2. Um SSH für den Remotezugriff auf durch MCS erstellte VMs in AWS zu verwenden, aktivieren Sie die Kennwortauthentifizierung, da diesen VMs kein Schlüsselname angehängt ist. Führen Sie die folgenden Schritte nach Bedarf aus.

- Bearbeiten Sie die `cloud-init`-Konfigurationsdatei `/etc/cloud/cloud.cfg`. Stellen Sie sicher, dass die Zeile **ssh_pwauth: true** vorhanden ist. Entfernen Sie die Zeile **set-password** und eventuell vorhandene nachfolgende Zeilen oder kommentieren Sie sie aus.

```
1 users:
2   - default
3   <!--NeedCopy-->
```

- Wenn Sie den Standardbenutzer `ec2-user` oder den von `cloud-init` erstellten Benutzer `ubuntu` verwenden möchten, können Sie das Benutzerkennwort mit dem Befehl `passwd` ändern. Merken Sie sich das neue Kennwort zur späteren Verwendung bei der Anmeldung an von MCS erstellten VMs.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um sicherzustellen, dass die folgende Zeile vorhanden ist:

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

Speichern Sie die Datei und führen Sie den Befehl `sudo service sshd restart` aus.

Schritt 3c: Linux VDA-Paket auf der Vorlagen-VM installieren

Hinweis:

Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden möchten, lassen Sie diesen Schritt aus.

Installieren Sie .NET Runtime 6.0, bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren.

Führen Sie gemäß Ihrer Linux-Distribution folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

RHEL/CentOS:


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

Hinweis:

Installieren Sie für RHEL und CentOS das EPEL-Repository, bevor Sie den Linux VDA installieren und `deploymcs.sh` erfolgreich ausführen können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter <https://docs.fedoraproject.org/en-US/epel/>.

Ubuntu/Debian:

```
1 sudo dpkg -i <PATH>/<Linux VDA DEB>
2
3 apt-get install -f
4 <!--NeedCopy-->
```

SUSE:

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

Schritt 3d: Aktivieren der Repositorys zum Installieren des tdb-tools-Pakets RHEL 7-Server:

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

RHEL 7-Arbeitsstation:

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

Schritt 3e (SUSE): Manuelle Installation von ntfs-3g Unter SUSE gibt es kein Repository, das ntfs-3g bereitstellt. Laden Sie den Quellcode herunter, führen Sie die Kompilation aus und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC) Compiler-System und das make-Paket:

```
1 sudo zypper install gcc
2 sudo zypper install make
3 <!--NeedCopy-->
```

2. Laden Sie das ntfs-3g-Paket herunter.

3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

```
1 ./configure
2 make
3 make install
4 <!--NeedCopy-->
```

Schritt 3f: Bearbeiten der MCS-Konfigurationsdateien

1. Ändern Sie Variablen in `/etc/xdl/mcs/mcs.conf`.

- **Szenarien ohne Domäneneinbindung**

Bei Szenarien ohne Domänenbindung können Sie Variablen in `/etc/xdl/mcs/mcs.conf` unspezifiziert lassen oder die folgenden Variablen nach Bedarf ändern:

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

Tipp:

Die Variable `AD_INTEGRATION` in `/etc/xdl/mcs/mcs.conf` ist standardmäßig auf `Winbind` festgelegt. Der Standardwert hat keine Auswirkungen auf Szenarien ohne Domäneneinbindung.

- **Szenarien mit Domäneneinbindung**

Ändern Sie Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` bietet Variablen zum Einrichten von MCS und Linux VDA. Folgende Variablen können Sie festlegen:

- **Use_Existing_Configurations_Of_Current_VDA:** Legt fest, ob die AD-bezogenen Konfigurationsdateien (/etc/krb5.conf, /etc/sss.conf und /etc/samba/smb.conf) des aktuell ausgeführten VDAs verwendet werden sollen. Bei Einstellung auf Y entsprechen die Konfigurationsdateien von durch MCS erstellten Maschinen den äquivalenten Dateien auf dem aktuell ausgeführten VDA. Die Variablen **dns** und **AD_INTEGRATION** müssen Sie dennoch konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsdateien von durch MCS erstellten Maschinen durch die Konfigurationsvorlagen auf dem Masterimage festgelegt werden.
- **dns:** Festlegen der IP-Adresse für jeden DNS-Server. Sie können bis zu vier DNS-Server einrichten.
- **NTP_SERVER:** Festlegen der IP-Adresse für Ihren NTP-Server. Sofern nicht anders angegeben, ist dies die IP-Adresse Ihres Domänencontrollers.
- **WORKGROUP:** Legt den Arbeitsgruppennamen mit dem NetBIOS-Namen (Groß-/Kleinschreibung wird beachtet) fest, den Sie in AD konfiguriert haben. Andernfalls verwendet MCS den Teil des Domännennamens, der unmittelbar auf den Maschinenhostnamen folgt, als Arbeitsgruppennamen. Lautet das Maschinenkonto beispielsweise **user1.lvda.citrix.com**, verwendet MCS **lvda** als Arbeitsgruppennamen, wohingegen **Citrix** die richtige Wahl ist. Achten Sie darauf, den Arbeitsgruppennamen richtig festzulegen.
- **AD_INTEGRATION:** Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der Linux-Distributionen und Methoden zum Domänenbeitritt, die MSC unterstützt, finden Sie unter Unterstützte Distributionen in diesem Artikel.
- **CENTRIFY_DOWNLOAD_PATH:** Legt den Pfad zum Herunterladen von Server Suite Free (zuvor “Centrify Express”) fest. Der Wert wird nur wirksam, wenn Sie die Variable **AD_INTEGRATION** auf “Centrify” festlegen.
- **CENTRIFY_SAMBA_DOWNLOAD_PATH:** Legt den Pfad zum Herunterladen des Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable **AD_INTEGRATION** auf “Centrify” festlegen.
- **PBIS_DOWNLOAD_PATH:** Legt den Pfad zum Herunterladen des PBIS-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable **AD_INTEGRATION** auf “PBIS” festlegen.
- **UPDATE_MACHINE_PW:** Aktiviert oder deaktiviert die Automatisierung der Kennwortaktualisierung von Maschinenkonten. Weitere Informationen finden Sie unter [Kennwortaktualisierung für Maschinenkonten automatisieren](#).
- Die folgenden Linux VDA-Konfigurationsvariablen:

DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime ****

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

Ein Beispiel für `mcs.conf` sehen Sie im folgenden Screenshot:

```
#!/bin/bash

#####
#
# Citrix Virtual Apps & Desktops For Linux Script: Machine Creation Service
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#
# This is the configuration file for mcs scripts.

#####Template machine check#####
# If unspecified, the value is N by default, meaning that mcs configuration templates will overwrite configuration items
# If you choose Y, MCS created VMs will use the existing configurations of the current VDA that must running correctly
Use_Existing_Configurations_Of_Current_VDA=N

#####DNS Configuration#####
# Provide DNS information
# You can provide 4 DNS servers at most.
# Leave empty if you do not have 4 servers. You may also leave all of them empty
# and configure dns manually.
# Format:
# dns1="xx.xx.xx.xx"
# dns2="xx.xx.xx.xx"
# dns3=
# dns4=
dns1="192.1681.5"
dns2="192.168.3.4"
dns3=
dns4=

#####NTP Configuration#####
# Provide NTP server information.
# If not set here, the default value will be the address of domain controller.
# Format:
# NTP_SERVER="xx.xx.xx.xx"
NTP_SERVER="192.168.4.5"

#####WORKGROUP Configuration#####
# Provide Workgroup information.
# Usually workgroup is the same with domain name and you do not need to configure it here.
# If that is not the case, please config it according to the correct format:
# WORKGROUP="workgroup_name"
WORKGROUP="example"

#####Domain Join Configuration#####
# Provide Domain Join method.
# Winbind: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# SSSD: support RHEL7/CentOS7, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, SUSE12, SUSE15
# Centrif: support RHEL7/CentOS7
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12, SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04, Debian 10
# AD_INTEGRATION="winbind" or AD_INTEGRATION="sssd" or AD_INTEGRATION="centrify" or AD_INTEGRATION="pbis"
AD_INTEGRATION="winbind"

#####Centrify download path Configuration#####
# When choose Centrify as AD_INTEGRATION, provide Centrify download path with related distribution if Centrify is not installed.
# To find out the correct download url for your os, you may go here:
# https://www.centrify.com/express/linux/download-files/#accordion-download-express-02
CENTRIFY_DOWNLOAD_PATH=

#####Centrify Samba download path Configuration#####
# When choose Centrify as AD_INTEGRATION, provide Centrify Samba download path with related distribution if Centrify is not installed.
# CENTRIFY_SAMBA_DOWNLOAD_PATH="http://edge.centrify.com/products/opensource/samba-4.5.9/centrify-samba-4.5.9-rhel3-x86_64.tgz"
CENTRIFY_SAMBA_DOWNLOAD_PATH=

#####PBIS download path Configuration#####
# When choose PBIS as AD_INTEGRATION, provide PBIS download path if PBIS is not installed.
# PBIS: support RHEL7/CentOS7, RHEL8/CentOS8, SUSE12/SUSE15, Ubuntu16.04, Ubuntu18.04, Ubuntu20.04
# RHEL7 and SUSE12: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
# RHEL8: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# Ubuntu: "https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh"
# SUSE15: "https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh"
# PBIS_DOWNLOAD_PATH="https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh"
PBIS_DOWNLOAD_PATH=

#####Machine Password Automate Update#####
# Machine password will expire after 30 days(default), so we have a mechanism to update
# this password regularly.
# You can set this value to enabled to enable this feature.
UPDATE_MACHINE_PW="disabled"

#####Linux VDA Configuration#####
# Provide Linux VDA configuration information.
# Please refer to Linux VDA Documentation for these settings.
DOTNET_RUNTIME_PATH=/opt/dotnet
DESKTOP_ENVIRONMENT=gnome
SUPPORT_DDC_AS_CNAME=N
VDA_PORT=80
REGISTER_SERVICE=Y
ADD_FIREWALL_RULES=Y
HDX_3D_PRO=N
VDI_MODE=Y
SITE_NAME='<none>'
LDAP_LIST="dc1.example.com"
SEARCH_BASE="DC=example,DC=com"
FAS_LIST='<none>'
START_SERVICE=Y
TELEMETRY_SOCKET_PORT=7503
TELEMETRY_PORT=7502
```

2. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
3. Fügen Sie auf der Vorlagenmaschine der Datei `/etc/xdl/mcs/mcs_local_setting.reg` Befehlszeilen hinzu, um Registrierungswerte nach Bedarf zu schreiben oder zu aktualisieren. Diese Aktion verhindert den Verlust von Daten und Einstellungen bei jedem Neustart einer von MCS-Provisioningmaschine.

Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

Beispielsweise können Sie der Datei `/etc/xdl/mcs/mcs_local_setting.reg` die folgenden Befehlszeilen hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 3g: Erstellen eines Masterimages

1. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
2. (Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden, lassen Sie diesen Schritt aus.) Aktualisieren Sie auf der Vorlagen-VM die Konfigurationsvorlagen, um die relevanten Dateien `/etc/krb5.conf`, `/etc/samba/smb.conf` und `/etc/sss/sss.conf` auf allen erstellten VMs anzupassen.

Aktualisieren Sie für Winbind-Benutzer die Vorlagen `/etc/xdl/mcs/winbind_krb5.conf.tpl` und `/etc/xdl/mcs/winbind_smb.conf.tpl`.

Aktualisieren Sie für SSSD-Benutzer die Vorlagen `/etc/xdl/mcs/sss.conf.tpl`, `/etc/xdl/mcs/sss_krb5.conf.tpl` und `/etc/xdl/mcs/sss_smb.conf.tpl`.

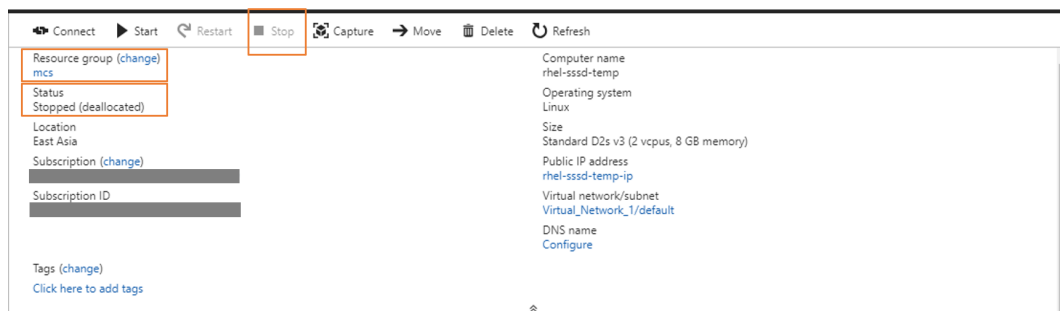
Aktualisieren Sie für Centrify-Benutzer die Vorlagen `/etc/xdl/mcs/centrify_krb5.conf.tpl` und `/etc/xdl/mcs/centrify_smb.conf.tpl`.

Hinweis:

Behalten Sie das vorhandene Format bei, das in den Vorlagendateien verwendet wird, und verwenden Sie Variablen wie `$WORKGROUP`, `$REALM`, `$realm`, `${new_hostname}` und `$AD_FQDN`.

3. Erstellen und benennen Sie einen Snapshot Ihres Masterimages basierend auf der von Ihnen verwendeten öffentlichen Cloud.

- **(Citrix Hypervisor, GCP und VMware vSphere)** Installieren Sie Anwendungen auf der Vorlagen-VM, und fahren Sie die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages.
- **(Azure):** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM vom Azure-Portal aus herunter. Stellen Sie sicher, dass der Energiestatus der Vorlagen-VM als **gestoppt (Zuordnung aufgehoben)** angezeigt wird. Merken Sie sich den Namen der Ressourcengruppe. Sie benötigen diesen Namen später, um Ihr Masterimage in Azure zu finden.



- **(AWS)** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM vom AWS EC2-Portal aus herunter. Stellen Sie sicher, dass der Instanzstatus der Vorlagen-VM als **gestoppt** angezeigt wird. Klicken Sie mit der rechten Maustaste auf die Vorlagen-VM und wählen Sie **Image > Image erstellen** aus. Geben Sie nach Bedarf Informationen ein und nehmen Sie die Einstellungen vor. Klicken Sie auf **Image erstellen**.

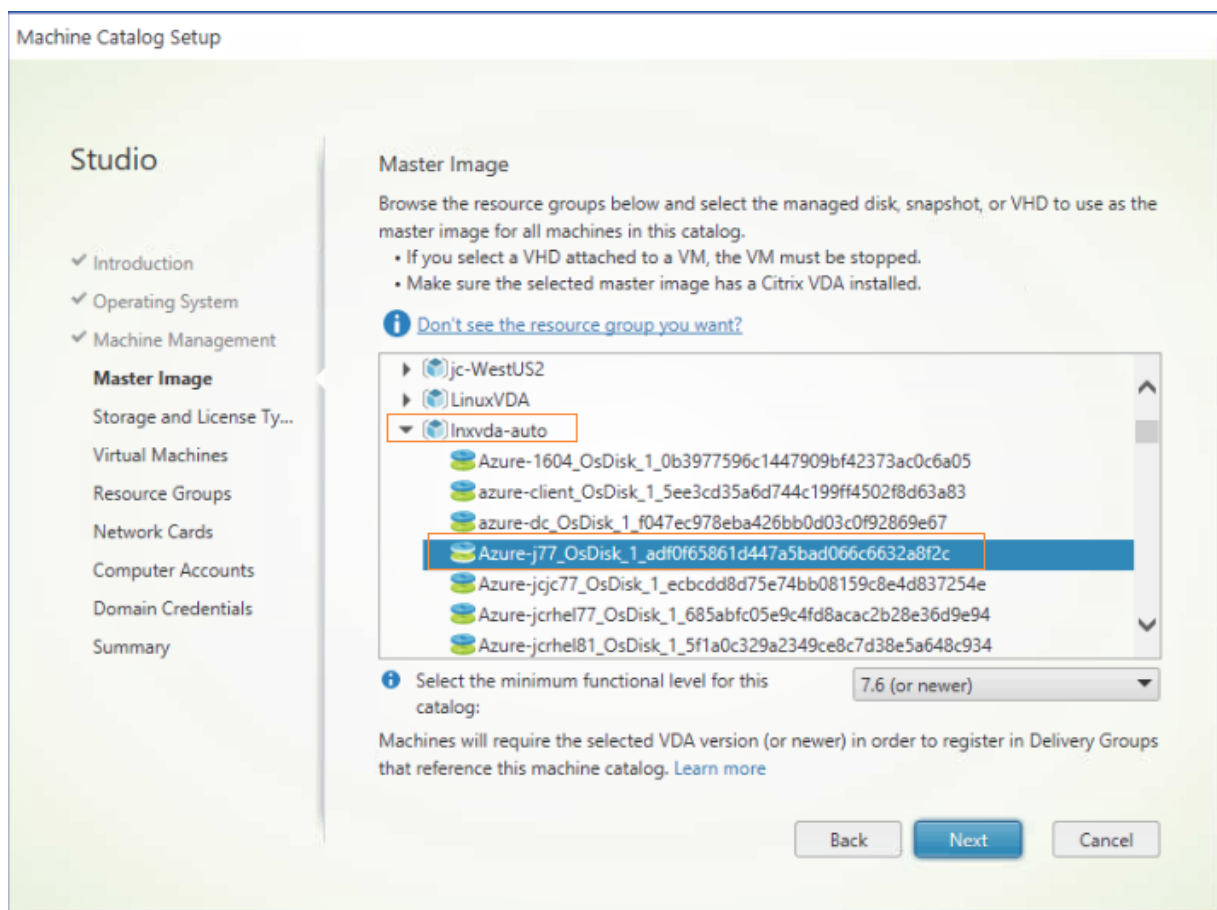
- **(Nutanix)** Fahren Sie unter Nutanix AHV die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages.

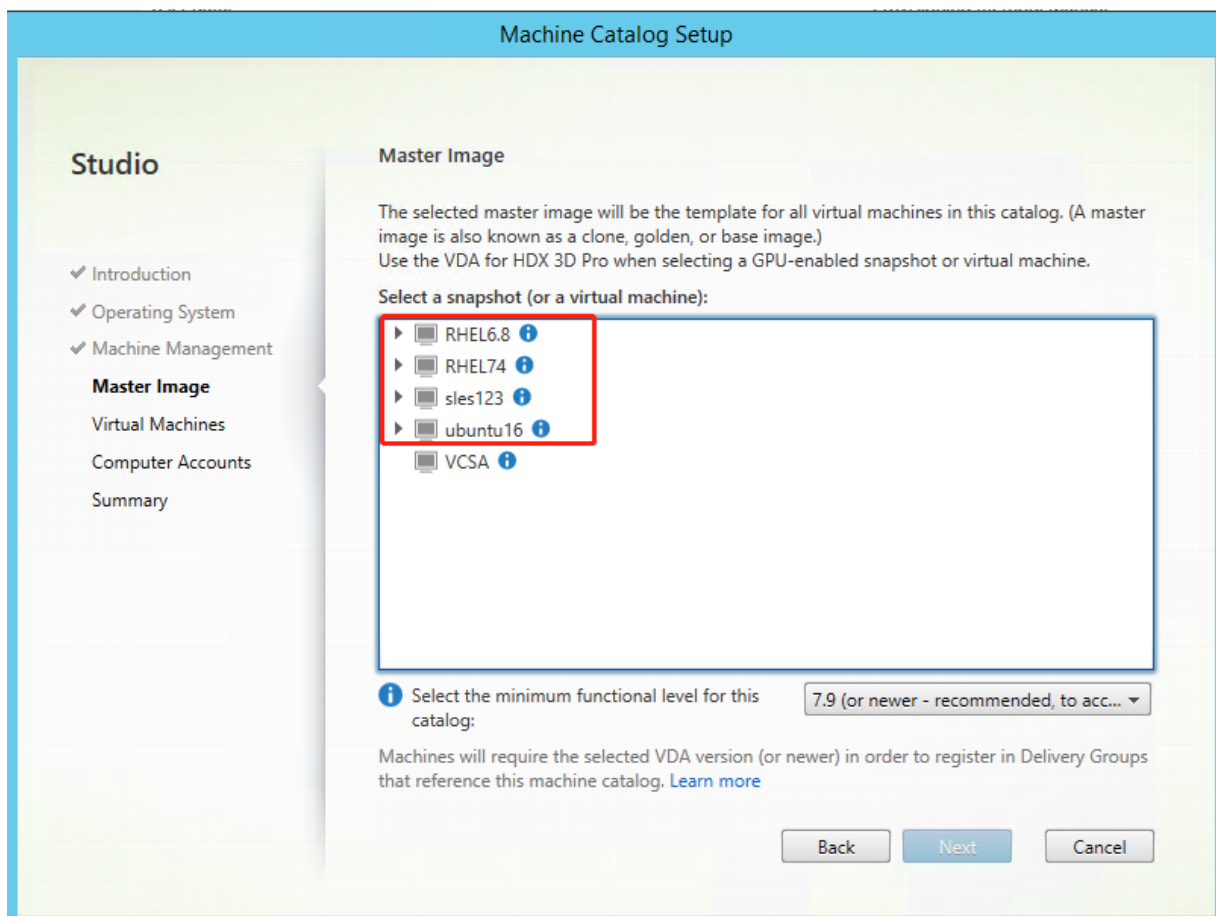
Hinweis:

Sie müssen den Namen von Acropolis-Snapshots zur Verwendung in Citrix Virtual Apps and Desktops **XD_** voranstellen. Verwenden Sie bei Bedarf die Acropolis-Konsole, um die Snapshots umzubenennen. Nach Umbenennen von Snapshots starten Sie den **Assistenten zum Erstellen von Katalogen** neu, damit eine aktualisierte Liste angezeigt wird.

Schritt 4: Maschinenkatalog erstellen

Erstellen Sie einen Maschinenkatalog in Citrix Studio und geben Sie die Anzahl der VMs im Katalog an. Wählen Sie beim Erstellen des Maschinenkatalogs Ihr Masterimage. Im Folgenden sind Beispiele aufgeführt:





Wählen Sie auf der für Nutanix eindeutigen Seite **Container** den Container aus, den Sie zuvor für die Vorlagen-VM angegeben haben. Wählen Sie auf der Seite **Masterimage** den Snapshot des Images aus. Prüfen Sie auf der Seite **Virtuelle Maschinen** die Anzahl der virtuellen CPUs und die Anzahl der Kerne pro vCPU.

Hinweis:

Wenn die Erstellung des Maschinenkatalogs auf dem Delivery Controller lange dauert, fahren Sie in Nutanix Prism die Maschine mit dem Präfix **Preparation** manuell hoch. Dadurch wird der Erstellungsprozess fortgesetzt.

Führen Sie nach Bedarf weitere Konfigurationsaufgaben aus. Weitere Informationen finden Sie unter [Erstellen eines Maschinenkatalogs mit Studio](#).

Schritt 5: Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Sie gibt die Benutzer an, die diese Maschinen verwenden können, und die für

die Benutzer verfügbaren Anwendungen und Desktops. Weitere Informationen finden Sie unter [Bereitstellungsgruppen erstellen](#).

Update des Linux VDAs mit MCS

Um MCS zum Aktualisieren des Linux VDAs zu verwenden, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie .NET Runtime 6.0 installiert haben, bevor Sie Ihren Linux VDA auf die aktuelle Version aktualisieren.
2. Aktualisieren Sie Ihren Linux VDA auf der Vorlagenmaschine:

Hinweis:

Mit dem Feature [Linux VDA-Selbstupdate](#) können Sie auch automatische Softwareupdates planen. Fügen Sie hierzu der Datei `etc/xdl/mcs/mcs_local_setting.reg` auf der Vorlagenmaschine Befehlszeilen hinzu.

Beispiel:

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
  SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" -
  force
2
3 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
  SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "Immediately"
  - force
4
5 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
  SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-
  Url>" - force
6
7 create -k "HKLM\System\CurrentControlSet\Control\Citrix\
  SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local-
  Certificate-Path-of-PortalAzureCom>" --force
8 <!--NeedCopy-->
```

RHEL 7 und CentOS 7:

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

RHEL 8:

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

SUSE:

```
1 sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
2 <!--NeedCopy-->
```

Ubuntu 18.04:

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

Ubuntu 20.04:

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

3. Bearbeiten Sie `/etc/xdl/mcs/mcs.conf` und `/etc/xdl/mcs/mcs_local_setting.reg`.
4. Erstellen Sie einen neuen Snapshot.
5. Wählen Sie in Citrix Studio den neuen Snapshot aus, um Ihren Maschinenkatalog zu aktualisieren. Warten Sie auf jeden Maschineneustart. Starten Sie eine Maschine nicht manuell neu.

Kennwortaktualisierung für Maschinenkonten automatisieren

Kennwörter von Maschinenkonten laufen standardmäßig 30 Tage nach der Erstellung des Maschinenkatalogs ab. Gehen Sie folgendermaßen vor, um das Ablauf von Kennwörtern zu verhindern und die Aktualisierung von Maschinenkennwörtern zu automatisieren:

1. Fügen Sie `/etc/xdl/mcs/mcs.conf` den folgenden Eintrag hinzu, bevor Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` ausführen.

`UPDATE_MACHINE_PW="enabled"`
2. Öffnen Sie nach dem Ausführen von `/opt/Citrix/VDA/sbin/deploymcs.sh` `/etc/cron.d/mcs_update_password` um die Uhrzeit und Frequenz der Aktualisierung festzulegen. In der Standardeinstellung werden die Kennwörter von Maschinenkonten wöchentlich jeden Sonntag um 2:30 Uhr aktualisiert.

Nach jeder Kennwortaktualisierung wird der Ticketcache auf dem Delivery Controller ungültig und evtl. der folgende Fehler in `/var/log/xdl/jproxy.log` angezeigt:

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

Um den Fehler zu beseitigen, leeren Sie den Ticketcache regelmäßig. Sie können einen Task zur Cachebereinigung auf allen Delivery Controllern oder auf dem Domänencontroller planen.

Aktivieren von FAS auf von MCS erstellten VMs

Sie können FAS auf mit MCS erstellten VMs aktivieren, die auf den folgenden Distributionen ausgeführt werden:

	Winbind	SSSD	Centrify	PBIS
RHEL 8	Ja	Nein	Nein	Ja
RHEL 7, CentOS 7	Ja	Ja	Nein	Ja
Ubuntu 20.04, Ubuntu 18.04	Ja	Nein	Nein	Nein
Debian 11.3, Debian 10.9	Ja	Nein	Nein	Nein
SUSE 15.3	Ja	Nein	Nein	Nein
SUSE 15.2	Ja	Nein	Nein	Nein

Aktivieren Sie FAS, wenn Sie ein Masterimage auf der Vorlagen-VM vorbereiten

1. Importieren Sie das Stammzertifizierungsstellenzertifikat.

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

2. Führen Sie `ctxfascfg.sh` aus. Weitere Informationen finden Sie unter [Ausführen von ctfascfg.sh](#).
3. Legen Sie Variablen in `/etc/xdl/mcs/mcs.conf` fest.

Hinweis:

Legen Sie alle erforderlichen Variablen in `/etc/xdl/mcs/mcs.conf` fest, da diese Variablen beim VM-Start aufgerufen werden.

- a) Legen Sie für `Use_Existing_Configurations_Of_Current_VDA` den Wert `Y` fest.
 - b) Legen Sie für die Variable `FAS_LIST` Ihre FAS-Serveradresse oder mehrere FAS-Serveradressen fest. Trennen Sie mehrere Adressen durch Semikolons und schließen Sie die Adresse oder Adressen in einfache Anführungszeichen ein, z. B. `FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'`.
 - c) Legen Sie die anderen Variablen wie erforderlich fest, z. B. `VDI_MODE`.
4. Führen Sie das Skript `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.

Aktivieren von FAS auf einer von MCS erstellten VM

Wenn FAS auf dem Vorlagencomputer nicht wie zuvor beschrieben aktiviert ist, können Sie FAS auf jeder von MCS erstellten VM aktivieren.

Um FAS auf einer von MCS erstellten VM zu aktivieren, führen Sie die folgenden Schritte aus:

1. Legen Sie Variablen in `/etc/xdl/mcs/mcs.conf` fest.

Hinweis:

Legen Sie alle erforderlichen Variablen in `/etc/xdl/mcs/mcs.conf` fest, da diese Variablen beim VM-Start aufgerufen werden.

- a) Legen Sie für `Use_Existing_Configurations_Of_Current_VDA` den Wert `Y` fest.
 - b) Legen Sie für die Variable `FAS_LIST` Ihre FAS-Serveradresse fest.
 - c) Legen Sie die anderen Variablen wie erforderlich fest, z. B. `VDI_MODE`.
2. Importieren Sie das Stammzertifizierungsstellenzertifikat.

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

3. Führen Sie das Skript `/opt/Citrix/VDA/sbin/ctxfascfg.sh` aus. Weitere Informationen finden Sie unter [Ausführen von ctxfascfg.sh](#).

Erstellen von Linux-VMs mit Citrix Provisioning

October 5, 2022

Dieser Artikel enthält Informationen zum Streaming von Linux-Zielgeräten. Mit diesem Feature können Sie virtuelle Linux-Desktops direkt in der Citrix Virtual Apps and Desktops-Umgebung bereitstellen.

Die folgenden Linux-Distributionen werden unterstützt:

- Ubuntu 20.04
- Ubuntu 18.04
- RHEL 8.4
- RHEL 7.9
- SUSE 15.2
- SUSE 15.3

Wichtig:

- Wir empfehlen die Verwendung des neuesten Installationspakets von Citrix Provisioning. Verwenden Sie das entsprechende Paket für Ihre Linux-Distribution. Citrix Provisioning Server 2109 oder höher ist erforderlich, um den Linux Streaming Agent 2109 und höher verwenden zu können.

- Wenn Sie Citrix Provisioning zum Streamen von Linux-Zielgeräten verwenden, erstellen Sie eine separate Startpartition auf dem freigegebenen Datenträgerimage, damit die bereitgestellten Geräte wie erwartet gestartet werden können.
- Vermeiden Sie es, Partitionen mit **btrfs** zu formatieren. GRUB2 hat Probleme beim Auffinden von **btrfs**-Partitionen. **GRUB** steht für **G**Rand **U**nified **B**ootloader.

Weitere Informationen finden Sie unter [Streaming von Linux-Zielgeräten](#) in der Dokumentation zu Citrix Provisioning.

Konfigurieren von Delivery Controllern für XenDesktop 7.6 und frühere Versionen

October 5, 2022

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

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:

```
1 .\Update-BrokerServiceConfig.ps1
2 <!--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:

```
1 Set-ExecutionPolicy Unrestricted
2 <!--NeedCopy-->
```

Das Skript **Update-BrokerServiceConfig.ps1** aktualisiert die Brokerdienstkonfigurationsdatei mit den 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:

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

Richtlinien- und LDAP-Servereinstellungen

October 5, 2022

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.

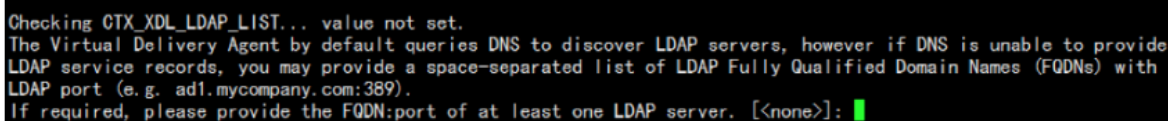
LDAP-Servereinstellung auf dem VDA

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:

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

Geben Sie alle LDAP-Server im empfohlenen Format ein: durch Leerzeichen getrennte Liste der vollqualifizierten Domännennamen (FQDN) der LDAP-Server mit LDAP-Port (z. B. ad1.mycompany.com:389 ad2.mycompany.com:389).



```
Checking CTX_XDL_LDAP_LIST... value not set.
The Virtual Delivery Agent by default queries DNS to discover LDAP servers, however if DNS is unable to provide
LDAP service records, you may provide a space-separated list of LDAP Fully Qualified Domain Names (FQDNs) with
LDAP port (e.g. ad1.mycompany.com:389).
If required, please provide the FQDN:port of at least one LDAP server. [<none>]:
```

Sie können diese Einstellung auch mit dem Befehl **ctxreg** direkt in die Registrierung schreiben:

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

Konfigurieren

October 5, 2022

In diesem Abschnitt werden die Features des Linux VDA, ihre Konfiguration und die Problembehandlung beschrieben.

Verwaltung

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [CEIP](#)
- [HDX Insight](#)
- [Integration mit dem Citrix Telemetriedienst](#)
- [Linux VDA-Selbstupdate für Citrix DaaS Standard für Azure](#)
- [Metriken für Linux-VM und Linux-Sitzung](#)
- [Protokollsammlung](#)
- [Sitzungsspiegelung](#)
- [Monitor Service Daemon](#)
- [Tools und Hilfsprogramme](#)
- [Andere](#)
 - [Unterstützung für Citrix Workspace-App für HTML5](#)
 - [Erstellen einer virtuellen Python3-Umgebung](#)
 - [Integrieren von NIS in Active Directory](#)
 - [IPv6](#)
 - [LDAPS](#)
 - [Xauthority](#)

Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

October 5, 2022

Wenn Sie an dem Programm teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, um die Qualität und Leistung der Citrix Produkte zu verbessern. Außerdem wird eine Kopie der anonymen Daten zur schnellen und effizienten Analyse an Google Analytics (GA) gesendet. GA ist standardmäßig deaktiviert.

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-->
```

- **GASwitch**

Die Registrierungseinstellung, mit der das GA aktiviert oder deaktiviert wird (Standardwert = 1):

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: **GASwitch**

Wert: 1 = deaktiviert , 0 = aktiviert

Wenn nicht angegeben, ist GA deaktiviert.

Sie können auf einem Client den folgenden Befehl ausführen, um GA zu aktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
  Citrix\CEIP" -v "GASwitch" -d "0"
2 <!--NeedCopy-->
```

- **DataPersistPath**

Die Registrierungseinstellung zur Steuerung des Datenspeicherpfads (Standard = /var/xdm/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.

Datenpunkt	Schlüsselname	Beschreibung
Gebietsschema des Systems	system_locale	Textzeichenfolge, die das Gebietsschema der Maschine angibt.
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.
CPU-Frequenz	cpu_frequency	Gleitkommazahl, die die CPU-Frequenz in MHz angibt.
Größe des physischen Speichers	memory_size	Ganzzahl, die die Größe des physischen Speichers in KB angibt.
Anzahl der gestarteten Sitzungen	session_launch	Ganzzahl, die die Anzahl der gestarteten Sitzung (angemeldet oder wieder verbunden) 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.
Ressourcentyp	resource_type	Textzeichenfolge, die den Ressourcentyp der gestarteten Sitzung angibt: Desktop oder <appname>
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.

Datenpunkt	Schlüsselname	Beschreibung
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 Typ der Citrix Workspace-App angibt.
Receiver-Clientversion	receiver_version	Textzeichenfolge, die die Version der Citrix Workspace-App angibt, die zum Starten der Sitzung verwendet wurde.
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.
GFX -Anbietertyp	gfx_provider_type	Textzeichenfolge, die den Grafikanbietertyp der Sitzung angibt.
Zahl der Spiegelungen	shadow_count	Ganzzahl, die angibt, wie oft eine Sitzung gespiegelt wurde.
Vom Benutzer ausgewählte Sprache	ctxism_select	Zusammengesetzte lange Zeichenfolge, die alle von den Benutzern ausgewählten Sprachen enthält.
Anzahl der Smartcardumleitungen	scard_redirecting_count	Ganzzahl, die angibt, wie oft die Smartcardumleitung für Sitzungsanmeldungen und Benutzerauthentifizierung für Apps in der Sitzung verwendet wird

HDX Insight

October 5, 2022

Übersicht

Der Linux VDA unterstützt teilweise das [HDX Insight](#)-Feature.

Installation

Keine abhängigen Pakete müssen installiert werden.

Verwendung

HDX Insight analysiert die ICA-Meldungen, die über den Citrix ADC zwischen der Citrix Workspace-App und dem Linux VDA weitergeleitet werden. Alle HDX Insight-Daten entstammen dem virtuellen NSAP-Kanal und werden unkomprimiert gesendet. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert.

Mit den folgenden Befehlen deaktivieren bzw. aktivieren Sie den virtuellen NSAP-Kanal:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\  
   VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000000"  
   --force  
2 <!--NeedCopy-->
```

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\  
   VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"  
   --force  
2 <!--NeedCopy-->
```

Problembehandlung

Es werden keine Datenpunkte angezeigt

Es gibt zwei mögliche Ursachen:

- HDX Insight ist nicht richtig konfiguriert.
Möglicherweise ist AppFlow nicht auf dem Citrix ADC aktiviert oder eine falsche Citrix ADC-Instanz ist in Citrix ADM 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.

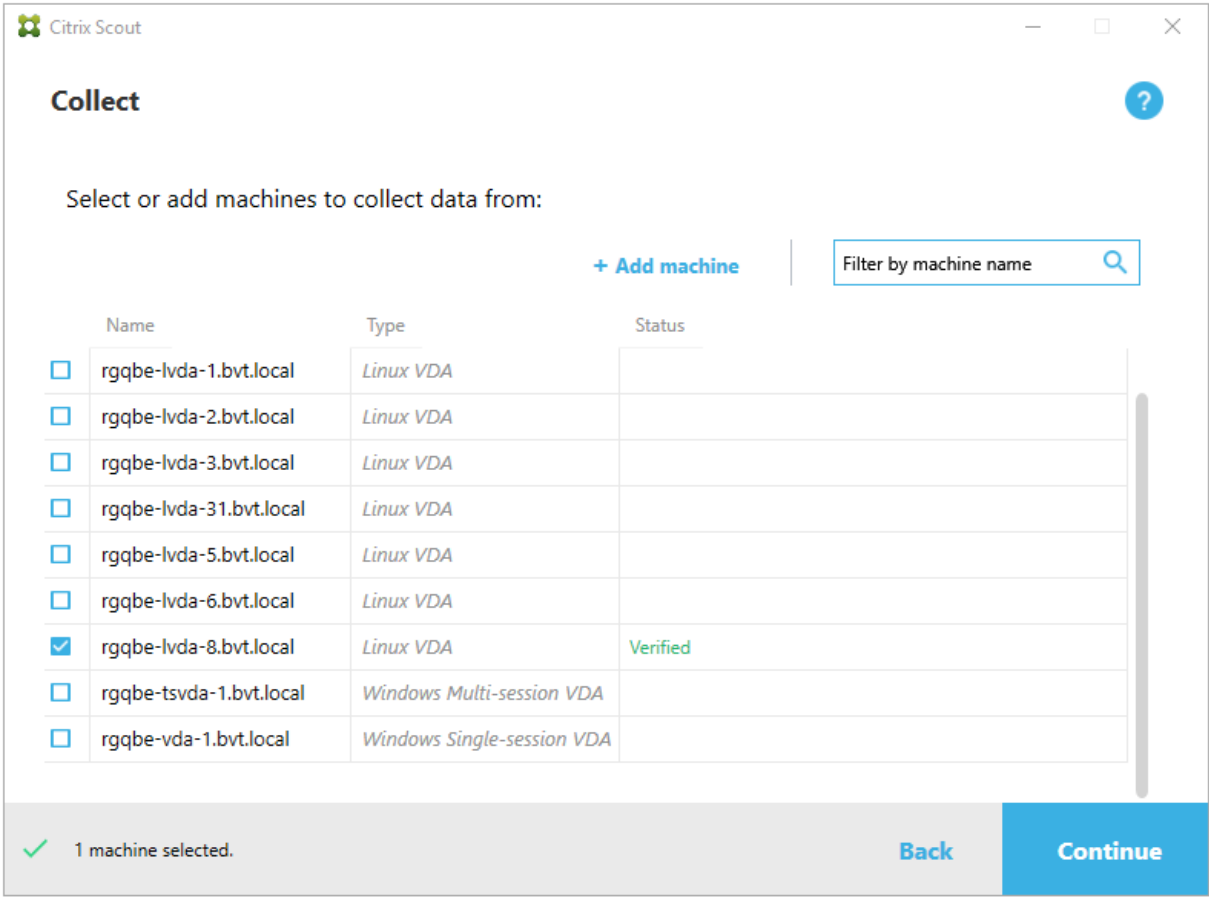
Es werden keine Anwendungsdatenpunkte angezeigt

Stellen Sie sicher, dass der virtuelle Seamlesskanal aktiviert ist und eine Seamlessanwendung ausgeführt wird.

Integration mit dem Citrix Telemetriedienst

October 5, 2022

Wenn der Citrix Telemetriedienst (`ctxtelemetry`) in die Linux VDA-Software integriert ist, können Sie Citrix Scout ausführen, um mit dem Skript `/opt/Citrix/vda/bin/xdlcollect.sh` Protokolle zum Linux VDA zu erfassen.



Hinweis:

Nach dem Upgrade von einer Linux VDA-Version bis einschließlich 1912 müssen Sie `/opt/Citrix/VDA/sbin/ctxsetup.sh` erneut ausführen, um die Variablen für den Citrix Telemetriedienst (`ctxtelemetry`) zu konfigurieren. Weitere Hinweise zu den Variablen finden Sie unter [Easy Install](#).

Aktivieren und Deaktivieren des Citrix Telemetriediensts

- Um den Dienst zu aktivieren, führen Sie den Befehl **`sudo systemctl enable ctxtelemetry.socket`** aus.
- Um den Dienst zu deaktivieren, führen Sie **`sudo systemctl disable ctxtelemetry.socket`** aus.

Ports

Der Citrix Telemetriedienst (`ctxtelemetry`) verwendet standardmäßig den TCP/IP-Port 7503, um auf Citrix Scout zu überwachen. Er verwendet den TCP/IP-Port 7502 auf dem Delivery Controller, um mit Citrix Scout zu kommunizieren.

Sie können die Standardports verwenden oder bei der Installation des Linux VDA die Ports über die folgenden Variablen ändern.

- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

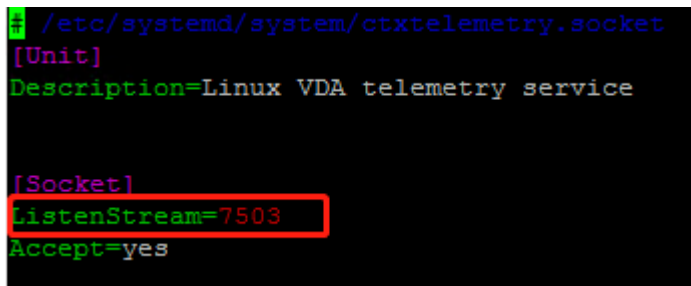
Gehen Sie folgendermaßen vor, um die Ports nach der Installation des Linux VDA zu ändern:

1. Führen Sie den folgenden Befehl aus, um den Port für die Kommunikation mit Scout zu ändern.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
  VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number>
  -t REG_DWORD
2 <!--NeedCopy-->
```

2. Um den Socketport für das Überwachen auf Scout zu ändern, führen Sie den folgenden Befehl aus, um die Datei `ctxtelemetry.socket` zu öffnen und zu bearbeiten.

```
1 sudo vi /etc/systemd/system/ctxtelemetry.socket
2 <!--NeedCopy-->
```



```
/etc/systemd/system/ctxtelemetry.socket
[Unit]
Description=Linux VDA telemetry service

[Socket]
ListenStream=7503
Accept=yes
```

3. Führen Sie die folgenden Befehle aus, um den Socketport neu zu starten.

```
1 sudo systemctl daemon-reload
2 sudo systemctl stop ctxtelemetry.socket
3 sudo systemctl start ctxtelemetry.socket
4 <!--NeedCopy-->
```

4. Aktivieren Sie die neuen Ports in Ihrer Firewall-Konfiguration.

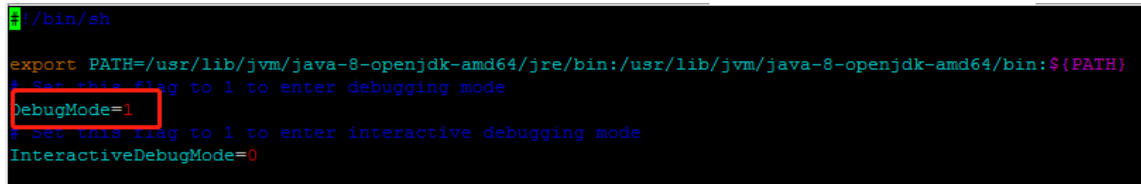
Wenn Sie beispielsweise Ubuntu verwenden, führen Sie den Befehl **sudo ufw allow 7503** aus, um Port 7503 zu aktivieren.

Debugmodus

Wenn der Citrix Telemetriedienst nicht einwandfrei funktioniert, können Sie den Debugmodus aktivieren, um die Ursache zu ermitteln.

1. Um den Debugmodus zu aktivieren, führen Sie den folgenden Befehl aus, um die Datei `ctxtelemetry` zu öffnen, und ändern Sie dann den Wert für “DebugMode” in 1.

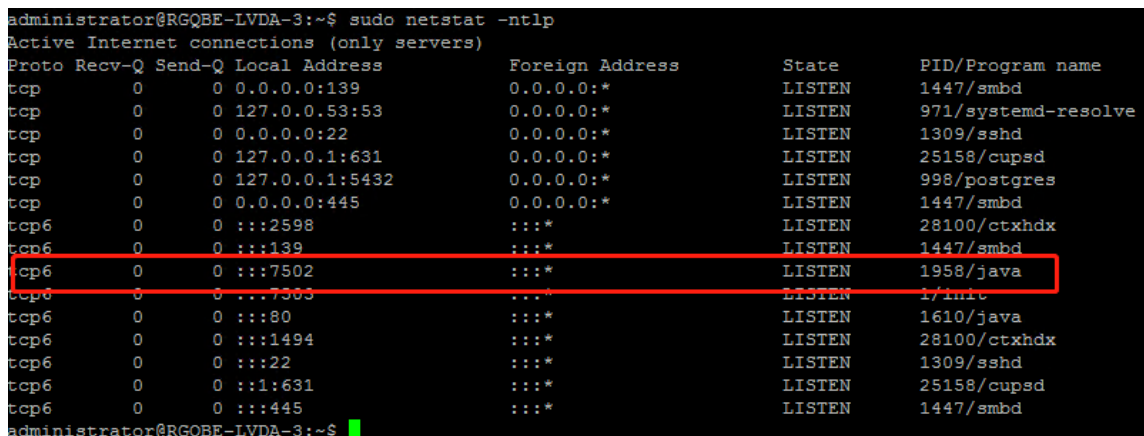
```
1 sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
2 <!--NeedCopy-->
```



```
#!/bin/sh

export PATH=/usr/lib/jvm/java-8-openjdk-amd64/jre/bin:/usr/lib/jvm/java-8-openjdk-amd64/bin:${PATH}
# Set this flag to 1 to enter debugging mode
DebugMode=1
# Set this flag to 1 to enter interactive debugging mode
InteractiveDebugMode=0
```

2. Beenden Sie den Citrix Telemetriedienst manuell oder warten Sie 15 Minuten, bis der Dienst automatisch beendet wird.



```
administrator@RGQBE-LVDA-3:~$ sudo netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1447/smbd
tcp        0      0 127.0.0.0:53:53         0.0.0.0:*               LISTEN      971/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1309/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      25158/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      998/postgres
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1447/smbd
tcp6       0      0 :::2598                 :::*                   LISTEN      28100/ctxhdx
tcp6       0      0 :::139                  :::*                   LISTEN      1447/smbd
tcp6       0      0 :::7502                  :::*                   LISTEN      1958/java
tcp6       0      0 :::7303                  :::*                   LISTEN      1/init
tcp6       0      0 :::80                   :::*                   LISTEN      1610/java
tcp6       0      0 :::1494                  :::*                   LISTEN      28100/ctxhdx
tcp6       0      0 :::22                   :::*                   LISTEN      1309/sshd
tcp6       0      0 :::1:631                 :::*                   LISTEN      25158/cupsd
tcp6       0      0 :::445                   :::*                   LISTEN      1447/smbd
administrator@RGQBE-LVDA-3:~$
```

In diesem Beispiel können Sie die folgenden Befehle ausführen, um den Citrix Telemetriedienst zu beenden.

```
1 sudo netstat -ntlp
2 Kill -9 1958
3 <!--NeedCopy-->
```

3. Um den Citrix Telemetriedienst neu zu starten, wählen Sie den Linux VDA in Scout und suchen Sie `telemetry-debug.log` in `/var/log/xdl/`.

Dienstwartezeit

Der `systemd`-Daemon, der den Socketport öffnet, startet standardmäßig und nutzt nur wenige Ressourcen. Der Citrix Telemetriedienst wird standardmäßig beendet und nur gestartet, wenn eine Protokollsammlungsanforderung vom Delivery Controller eintrifft. Nach Abschluss der Protokollsammlung wird der Dienst beendet, sofern für eine Dauer von 15 Minuten keine neue Sammlungsanforderung eingeht. Sie können die Wartezeit über den folgenden Befehl konfigurieren. Der Mindestwert beträgt 10 Minuten. Wenn Sie einen unter 10 Minuten Wert festlegen, wird der

Mindestwert von 10 Minuten wirksam. Nachdem Sie die Wartezeit festgelegt haben, beenden Sie den Dienst und starten Sie ihn neu.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\  
   VirtualDesktopAgent" -v "TelemetryServiceIdleTimeoutInMinutes" -d <  
   number> -t REG_DWORD  
2 <!--NeedCopy-->
```

Tests zur Überprüfung

Vor Ausführung einer Sammlung wird automatisch jede ausgewählte Maschine überprüft. Diese Prüfung gewährleistet, dass die Anforderungen erfüllt sind. Besteht eine Maschine den Test nicht, wird in Scout eine Meldung mit einem Maßnahmenvorschlag angezeigt. Weitere Informationen finden Sie unter [Tests zur Überprüfung](#) in der Citrix Scout-Dokumentation.

Linux VDA-Selbstupdate für Citrix DaaS Standard für Azure

November 22, 2023

Mit diesem Feature wird die Linux VDA-Software automatisch sofort oder zu einem geplanten Zeitpunkt aktualisiert. Dies ist dann von Vorteil, wenn Sie Linux VDAs in Citrix DaaS Standard für Azure (früher Citrix Virtual Apps and Desktops Standard für Azure) erstellen. Sie haben keine Administratorprivilegien für die VMs in Azure. Weitere Informationen finden Sie unter [Erstellen von Linux VDAs in Citrix DaaS Standard für Azure](#).

Konfiguration

Führen Sie die folgenden Schritte aus, um die Funktion zu nutzen:

Schritt 1: Hochladen von Updateinformationen und neuen VDA-Paketen in den Azure-Container

Schritt 1a: Erstellen Sie einen Container für Ihr Azure-Speicherkonto und legen Sie die Container-Zugriffsebene auf **Blob (anonymer Lesezugriff nur für Blobs)**.

Hinweis:

Azure-Container und Blobs werden ausschließlich von Kunden gepflegt und verwaltet. Citrix haftet nicht für deren Sicherheit. Um Datensicherheit und Kosteneffizienz zu gewährleisten,

legen Sie die Container-Zugriffsebene nach jedem **Selbstupdate** auf **Privat (kein anonymer Zugriff)** fest.

Schritt 1b: Geben Sie die VDA-Updateinformationen in eine JSON-Datei mit dem Namen "Update-Info.json" ein. Beispiel:

```
1 {
2
3   "Version": "21.04.200.4",
4   "Distributions": [
5   {
6
7     "TargetOS": "RHEL7_9",
8     "PackageName": "",
9     "PackageHash": ""
10  }
11  ,
12  {
13
14    "TargetOS": "UBUNTU18_04",
15    "PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",
16    "PackageHash": "4148
17      cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"
18  }
19  ,
20  {
21    "TargetOS": "UBUNTU20_04",
22    "PackageName": "",
23    "PackageHash": ""
24  }
25  ]
26 }
27
28
29 <!--NeedCopy-->
```

Version gibt die neue VDA-Version an und **Distributions** ein Array von Updateobjekten. Jedes Objekt enthält drei Elemente:

- **TargetOS:** muss "RHEL7_9"(für RHEL 7, CentOS 7 und Amazon Linux 2), "UBUNTU18_04"oder "UBUNTU20_04"sein. `ctxmonitorservice` erkennt keine anderen Distributionen.
- **PackageName:** Vollständiger Name des VDAs -Pakets der angegebenen Version.
- **PackageHash:** mit dem Befehl `shasum -a 256 <pkgname>` berechneter SHA-256-Wert.

Schritt 1c: Laden Sie die JSON-Datei und die neue Version der Linux VDA-Pakete in Ihren Azure-Container hoch.

Schritt 2: Aktivieren des Selfupdate-Features für das Masterimage oder auf jedem VDA

Standardmäßig ist **Selfupdate** deaktiviert. Wenn Sie Linux VDAs in Citrix DaaS Standard für Azure erstellen, muss die Feature-Aktivierung für das Masterimage durchgeführt werden. Aktivieren Sie an-
dernfalls das Feature direkt für jeden Ziel-VDA.

Zum Aktivieren des **Selbstupdates** führen Sie einen Befehl nach dem folgenden Muster zum Bear-
beiten des Registrierungsschlüssels unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Self
aus.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\  
   Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0  
   x00000001" --force  
2  
3 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\  
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "ScheduledTime" -d "  
   Immediately" --force  
4  
5 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\  
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "Url" -d "<Your-Azure-  
   Container-Url>" --force  
6  
7 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\  
   Control\Citrix\SelfUpdate" -t "REG_SZ" -v "CaCertificate" -d "<Local  
   -Certificate-Path-of-PortalAzureCom>" --force  
8 <!--NeedCopy-->
```

In der folgenden Tabelle werden die Registrierungseinstellungen beschrieben.

Registrierungseinstellung	Beschreibung
fEnabled	Diese Einstellung ist erforderlich. Standardmäßig ist der Wert 0 und das Selbstupdate damit deaktiviert. Sie können den Wert auf 1 setzen, um das Selbstupdate zu aktivieren.
URL	Diese Einstellung ist erforderlich. Sie legt die URL des Azure-Containers zum Abrufen von Updateinformationen und neuen VDA-Paketen fest.

Registrierungseinstellung	Beschreibung
ScheduledTime	Diese Einstellung ist erforderlich. Sie können sie auf Immediately oder NextStart festlegen. Immediately bedeutet, dass ein Update sofort nach dem Herunterladen von VDA-Paketen ausgeführt wird. Diese Option eignet sich für hohe Download-Geschwindigkeiten und dringliche Updates. Sie kann jedoch Benutzer stören, wenn beim Herunterladen von Paketen Sitzungen laufen. NextStart bedeutet, dass ein Update beim nächsten Start von <code>ctxmonitorservice</code> ausgeführt wird. Diese Option eignet sich für niedrige Download-Geschwindigkeiten und nicht dringliche Updates.
CaCertificate	Diese Einstellung ist optional. Sie legt den vollständigen Pfad eines PEM-Zertifikats zur Prüfung der URL des Azure-Containers fest. Bei Azure-Blobs kann dies das Zertifikat von portal.azure.com sein, das aus dem Browser abgerufen und dann in PEM konvertiert wird. Aus Sicherheitsgründen empfehlen wir, diese Registrierungseinstellung hinzuzufügen. Sie wird jedoch nur unter Ubuntu unterstützt. Unter RHEL fehlt die Verknüpfung von NSS-Bibliotheken für den Befehl <code>curl</code> . Legen Sie auf jeden Fall die minimalen Privilegien für das Zertifikat fest.

Wenn `ctxmonitorservice` neu gestartet wird, ruft es zuerst über **Url** die Datei UpdateInfo.json und aus dieser dann die Updateversion ab. `ctxmonitorservice` vergleicht dann die Updateversion mit der aktuellen Version. Ist die aktuelle Version älter, lädt der Dienst die neue Version des VDAs -Pakets von Azure herunter und speichert sie lokal. Danach führt er ein Update gemäß der Einstellung **ScheduledTime** aus. In On-Premises-Bereitstellungen können Sie `ctxmonitorservice` neu starten, um ein Update auszulösen. In Citrix DaaS Standard für Azure haben Sie hingegen keine Administratorprivilegien für VMs und `ctxmonitorservice` kann erst nach dem Neustart der VDA-Maschine neu gestartet werden. Wenn ein Update fehlschlägt, wird der VDA auf die bestehende Version zurückgesetzt.

Hinweis:

- Die für das Masterimage konfigurierten Registrierungseinstellungen können nicht geändert werden.
- Wenn alle VMs in einer Umgebung gleichzeitig ein Paket herunterladen, kann dies zur Überlastung des lokalen Netzwerks führen.
- Benutzerdaten gehen verloren, wenn sowohl ein Update als auch das Rollback fehlschlagen.
- Wenn ein Update fehlschlägt, das Rollback jedoch gelingt, haben Benutzer im selben Netzwerk möglicherweise verschiedene Linux VDA-Versionen. Das ist nicht optimal.
- Updates erfordern in der Regel mehrere Minuten. In Citrix Studio gibt es keine Statusanzeige.

Metriken für Linux-VM und Linux-Sitzung

December 9, 2022

Die folgende Tabelle enthält Metriken, die für Linux-VMs und Linux-Sitzungen verfügbar sind.

Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Anmeldedauer	2109	Der Wert gibt an, wie lange Benutzer bei der Anmeldung über die Citrix Workspace-App warten müssen, bis eine Sitzung einsatzbereit ist. Um die Metrik einer Sitzung anzuzeigen, gehen Sie zur Registerkarte Überwachen von Citrix DaaS (früher Citrix Virtual Apps and Desktops Service). Überwachen ist als Director-Konsole verfügbar, um Citrix Virtual Apps and Desktops-Bereitstellungen (Aktuelles Release und LTSR) zu überwachen und zu warten. Klicken Sie auf der Registerkarte Überwachen im Bereich Durchschnittl. Anmeldedauer auf Verlaufstrend anzeigen . Legen Sie auf der Seite Anmeldungsleistung Filterbedingungen fest und klicken Sie auf Übernehmen , um Metriken darzustellen.	Nur in “Überwachen” verfügbar.

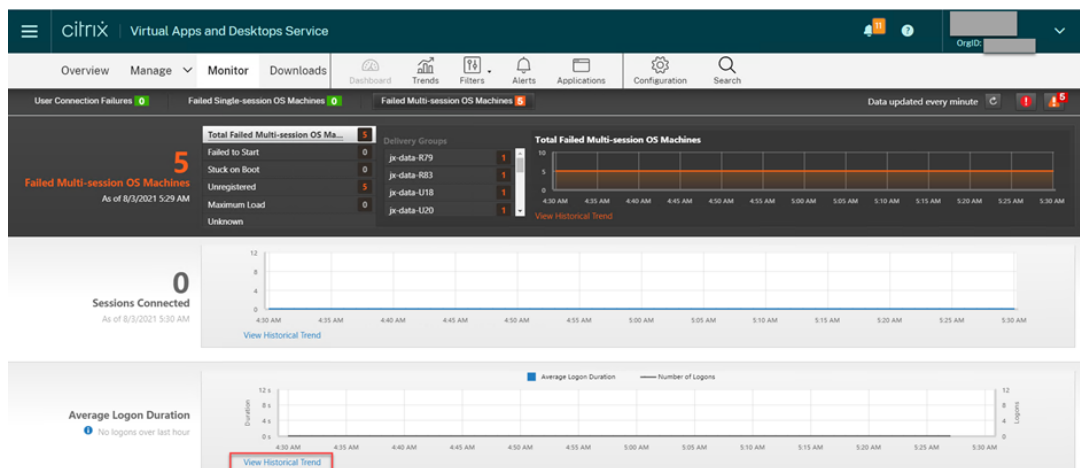
Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Anzahl autom. Sitzungswiederverbindun- gen	2109	<p>In der Ansicht Trends können Sie die Anzahl automatischer Wiederverbindungen einer Sitzung anzeigen. Legen Sie Bedingungen fest und klicken Sie auf Übernehmen, um die Suchergebnisse zu beschränken. In der Spalte Anzahl autom. Sitzungswiederverbindungen wird die Anzahl der automatischen Wiederverbindungen einer Sitzung angezeigt. Die automatische Wiederverbindung ist aktiviert, wenn die Richtlinie Sitzungszuverlässigkeit oder Client automatisch wieder verbinden aktiviert ist. Weitere Hinweise zur Wiederverbindung von Sitzungen finden Sie unter Sitzungen. Weitere Informationen zu Richtlinien finden Sie unter Einstellungen der Richtlinie “Automatische Wiederverbindung von Clients” und Einstellungen der Richtlinie “Sitzungszuverlässigkeit”.</p>	Verfügbar in Citrix Director und in “Überwachen” .

Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Leerlaufzeit	2103	Um auf diese Metrik zuzugreifen, öffnen Sie die Seite Alle Sitzungen durch Auswahl von Filter > Sitzungen > Alle Sitzungen .	Verfügbar in Citrix Director und in “Überwachen”.
Metriken einer Linux-VM	2103	Die folgenden Metriken für Linux-VMs sind verfügbar: Anzahl der CPU-Kerne, Speichergröße, Festplattenkapazität sowie aktuelle und historische CPU- und Speicherauslastung	Verfügbar in Citrix Director und in “Überwachen”.
Protokoll	1909	Das Transportprotokoll einer Linux-Sitzung wird im Bereich Sitzungsdetails als UDP oder TCP angezeigt.	Verfügbar in Citrix Director und in “Überwachen”.
ICA RTT	1903	Die ICA-Rundtripzeit (RTT) misst die Zeit zwischen dem Drücken einer Taste und der Anzeige der Reaktion am Endpunkt. Um ICA RTT-Metriken zu erhalten, erstellen Sie in Citrix Studio die Richtlinien ICA-Roundtripberechnung und Intervall für ICA-Roundtripberechnung .	Verfügbar in Citrix Director und in “Überwachen”.

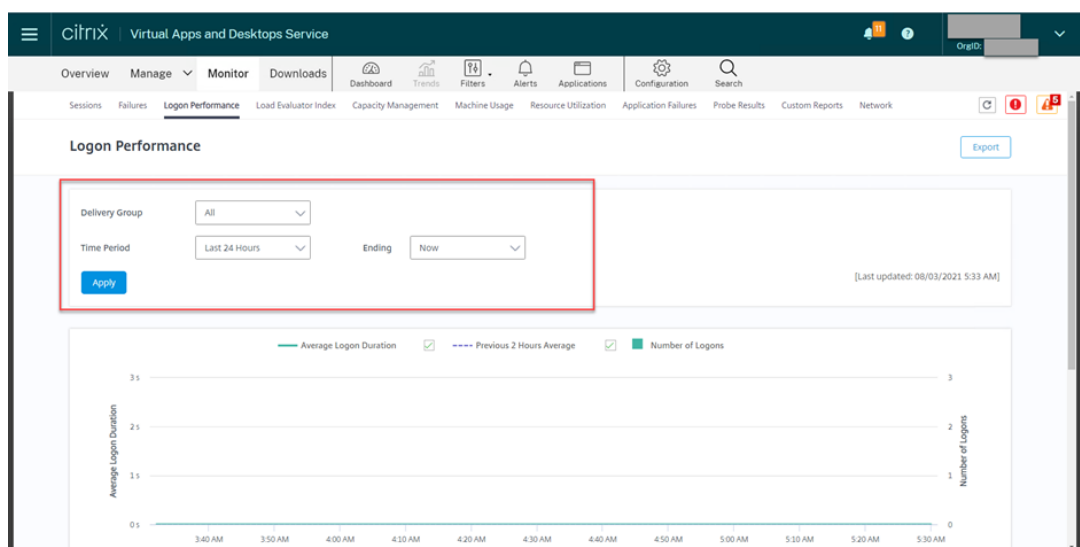
Beispiele für den Zugriff auf verschiedene Metriken in Citrix Director und in “Überwachen”

- Anmeldedauer

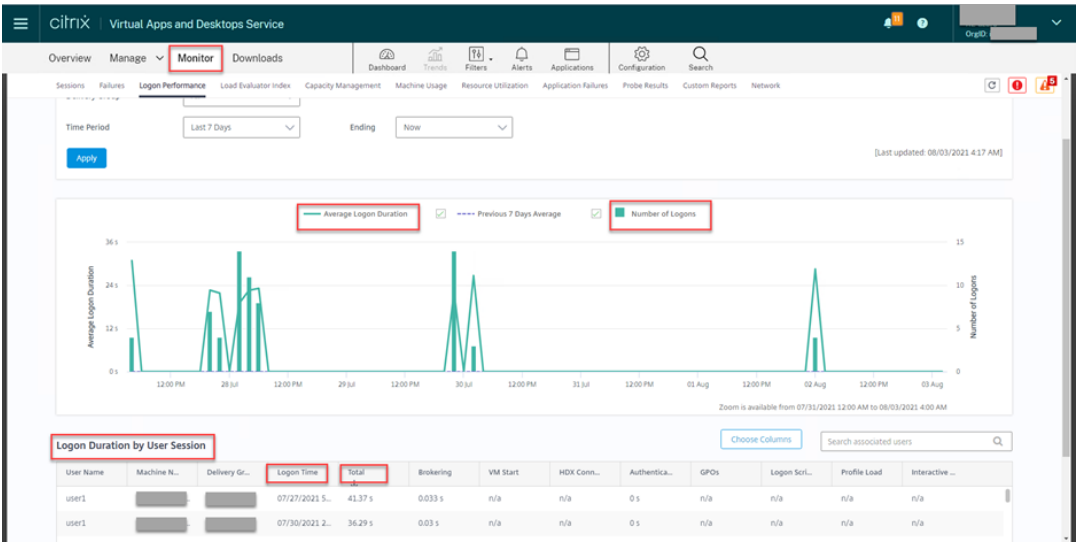
1. Klicken Sie auf der Registerkarte **Überwachen** von Citrix DaaS im Bereich **Durchschnittl. Anmeldedauer** auf **Verlaufstrend anzeigen**.



2. Legen Sie auf der Seite **Anmeldungsleistung** Filterbedingungen fest.

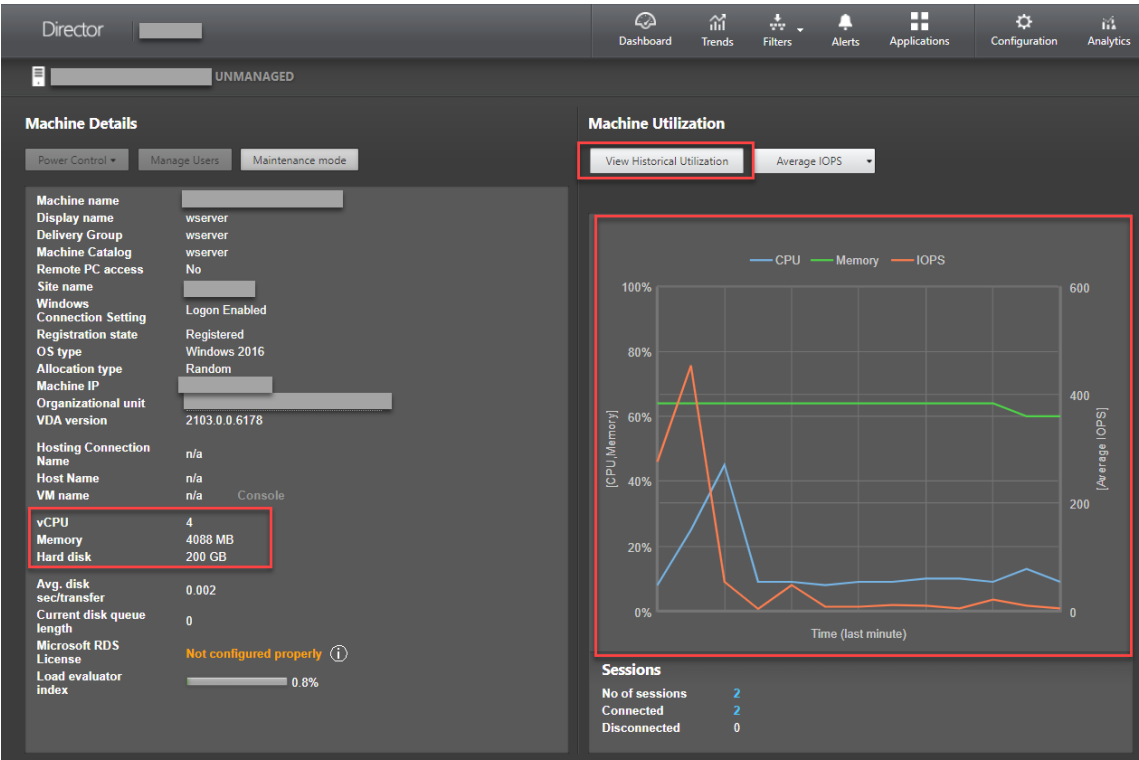


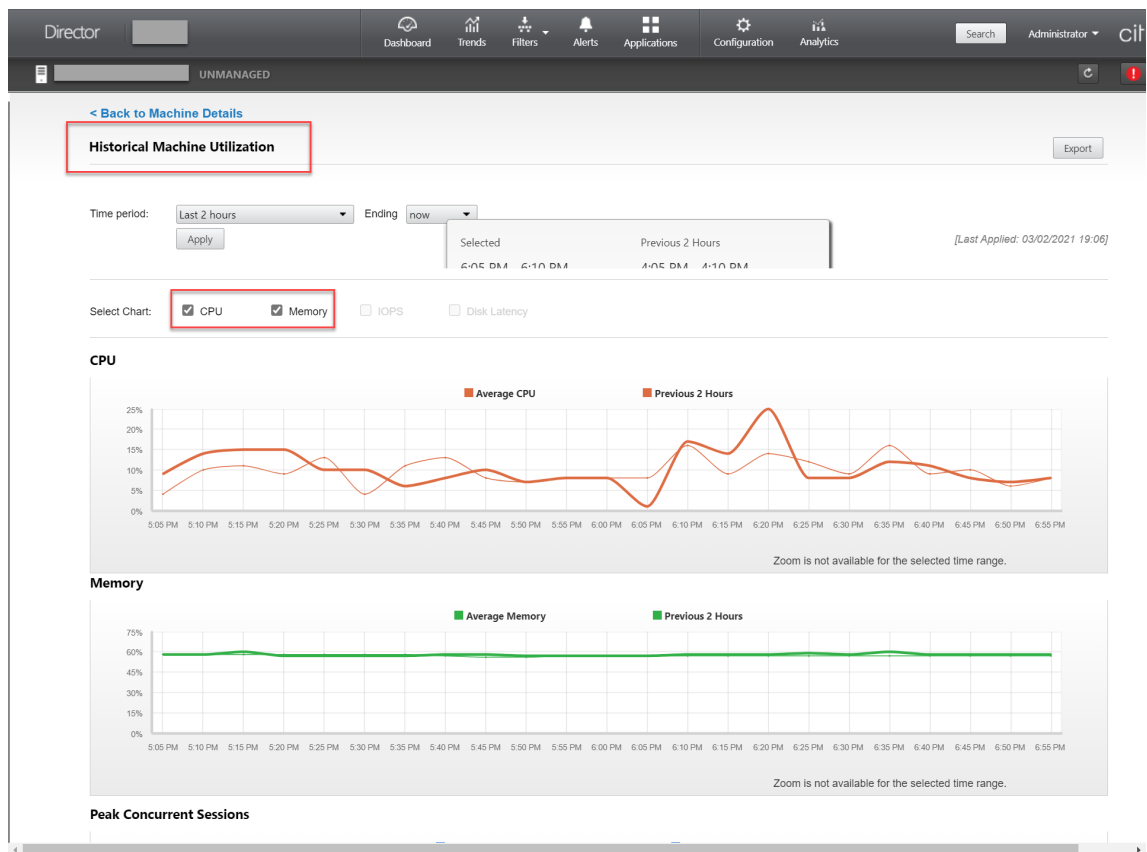
3. Klicken Sie auf **Übernehmen**, um die Metriken zur Anmeldedauer darzustellen.



- Angaben zur Anzahl der CPU-Kerne, Speichergröße und Festplattenkapazität sowie aktuelle und historische Daten zur CPU- und Speicherauslastung

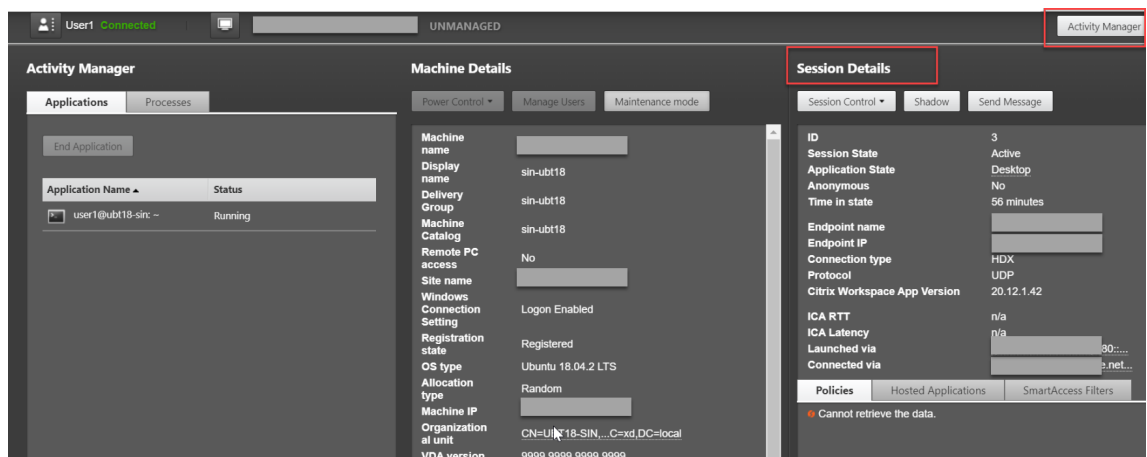
Um auf diese Metriken einer Linux-VM zuzugreifen, suchen Sie die VM in Citrix Director oder in Überwachen und überprüfen dann den Bereich **Maschinendetails**. Beispiel:





- ICA RTT, Protokoll

Um die Metriken einer Linux-Sitzung anzuzeigen, öffnen Sie die Seite **Alle Sitzungen** durch Auswahl von **Filter > Sitzungen > Alle Sitzungen**, oder greifen Sie auf den Bereich **Sitzungsdetails** zu. Um auf den Bereich **Sitzungsdetails** zuzugreifen, öffnen Sie die Seite **Alle Sitzungen** und klicken Sie auf eine Zielsitzung, um die Ansicht **Aktivitätsmanager** aufzurufen. Beispiel:

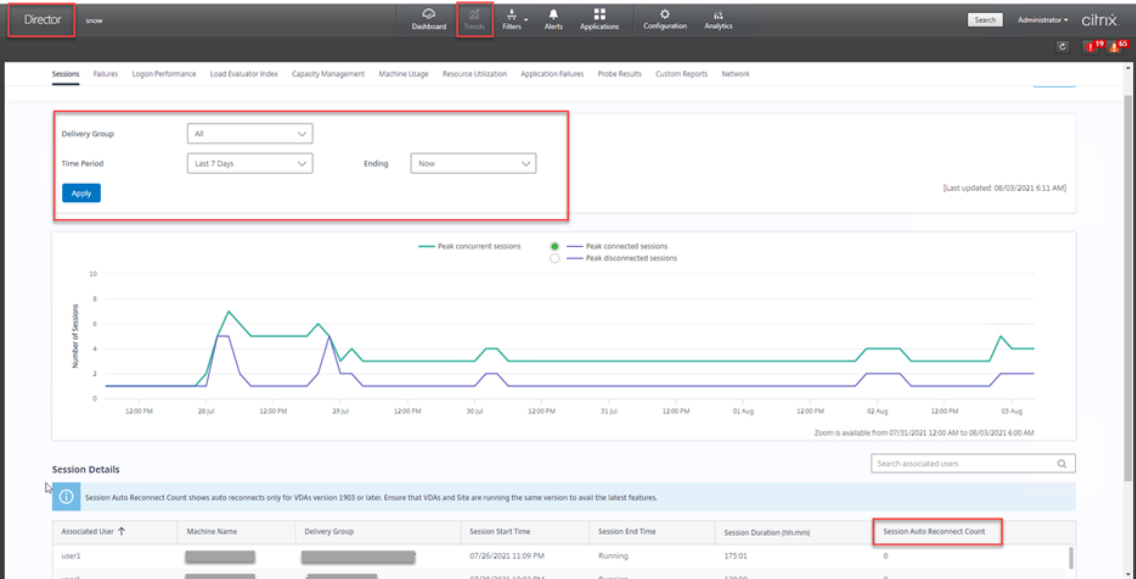


- Anzahl autom. Sitzungswiederverbindungen

In der Ansicht **Trends** können Sie die Anzahl automatischer Wiederverbindungen einer Sitzung

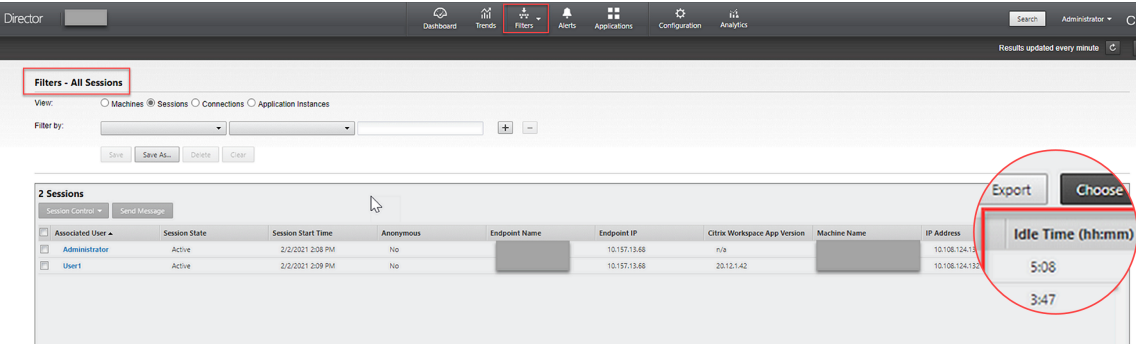
anzeigen. Legen Sie Bedingungen fest und klicken Sie auf **Übernehmen**, um die Suchergebnisse zu beschränken.

In der Spalte **Anzahl autom. Sitzungswiederverbindungen** wird die Anzahl der automatischen Wiederverbindungen einer Sitzung angezeigt. Beispiel:



- Leerlaufzeit

Beispiel:



Protokollsammlung

October 5, 2022

Übersicht

Das Sammeln von Protokollen ist für den Linux VDA standardmäßig aktiviert.

Konfiguration

Der `ctxlogd`-Daemon und das `setlog`-Hilfsprogramm sind 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-Hilfsprogramm

Das Sammeln von Protokollen wird mit dem `setlog`-Hilfsprogramm konfiguriert. Es ist an 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:

```
1 setlog help
2 <!--NeedCopy-->
```

Werte Standardmäßig ist **Log Output Path** auf `/var/log/xdm/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:

```
1 setlog values
2
3 log_path (Log Output Path) = /var/log/xdm/hdx.log
4
5 log_size (Max Log Size (MiB)) = 200
6
7 log_count (Max Old Log Files) = 2
8 <!--NeedCopy-->
```

Anzeigen oder Festlegen eines einzelnen `setlog`-Werts:

```
1 setlog value <name> [<value>]
2 <!--NeedCopy-->
```

Beispiel:

```
1 setlog value log_size 100
2 <!--NeedCopy-->
```


Ebenen Standardmäßig sind Protokollebenen auf **warning** festgelegt (Groß-/Kleinschreibung wird nicht beachtet).

Führen Sie den folgenden Befehl aus, um Protokollebenen für verschiedene Komponenten anzuzeigen:

```
1 setlog levels
2 <!--NeedCopy-->
```

Sie können die Protokollebenen (einschließlich Disabled, Inherited, Verbose, Information, Warnings, Errors und Fatal Errors) mit dem folgenden Befehl festlegen:

```
1 setlog level <class> [<level>]
2 <!--NeedCopy-->
```

Protokollebene	Befehlsparameter (Groß-/Kleinschreibung unerheblich)
Deaktiviert	none
Inherited	inherit
Verbose	verbose
Information	info
Warnings	warning
Errors	error
Fatal Errors	fatal

Mit der Variable **<class>** wird eine Komponente des Linux VDA angegeben. Um alle Komponenten einzubeziehen, legen Sie “all” fest: Beispiel:

```
1 setlog level all error
2 <!--NeedCopy-->
```

Flags Flags werden wie folgt festgelegt:

```
1 setlog flags
2
3 DATE = true
4
5 TIME = true
6
7 NAME = true
8
9 PID = true
10
```

```
11 TID = false
12
13 SID = true
14
15 UID = false
16
17 GID = false
18
19 CLASS = false
20
21 LEVEL = false
22
23 FUNC = true
24
25 FILE = false
26 <!--NeedCopy-->
```

Anzeigen der aktuellen Flags:

```
1 setlog flags
2 <!--NeedCopy-->
```

Anzeigen oder Festlegen eines einzelnen Protokoll-Flags:

```
1 setlog flag <flag> [<state>]
2 <!--NeedCopy-->
```

Wiederherstellen der Standardeinstellungen Wiederherstellen der Standardeinstellungen für alle Ebenen, Flags und Werte:

```
1 setlog default
2 <!--NeedCopy-->
```

Wichtig:

Der `ctxlogd`-Dienst wird mit der Datei `/var/xdm/ctxlog` konfiguriert, die nur von Root-Benutzern erstellt werden kann. Andere Benutzer haben keine Schreibrechte für diese Datei. Wir empfehlen 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/xdm/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`:

```
1 Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
  configuration file.
2
3 Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
  =exited, status=1/FAILURE
4
5 Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.
6
7 Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
8 <!--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.

Sitzungsspiegelung

October 5, 2022

Die Sitzungsspiegelung ermöglicht es Domänenadministratoren, ICA-Sitzungen von Benutzern in einem Intranet anzuzeigen. Dabei wird unter Einsatz von noVNC eine Verbindung mit den ICA-Sitzungen hergestellt.

Hinweis:

Zur Verwendung des Features ist Citrix Director 7.16 oder höher erforderlich.

Installation und Konfiguration

Abhängigkeiten

Für die Sitzungsspiegelung sind zwei neue Elemente, `python-websockify` und `x11vnc`, erforderlich. Installieren Sie `python-websockify` und `x11vnc` nach der Installation des Linux VDA manuell.

Für RHEL 7.x und Amazon Linux2:

Führen Sie die nachstehenden Befehle aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
1 sudo pip3 install websockify
2 sudo yum install x11vnc
3 <!--NeedCopy-->
```

Zum Auflösen von `python-websockify` und `x11vnc` aktivieren Sie das EPEL-Repository (Extra Packages for Enterprise Linux) und das optionale RPM-Repository unter RHEL 7.x:

- EPEL

Das EPEL-Repository ist für `x11vnc` erforderlich. Führen Sie folgenden Befehl aus, um das EPEL-Repository zu aktivieren:

```
1 yum install https://dl.fedoraproject.org/pub/epel/epel-release-  
   latest-7.noarch.rpm  
2 <!--NeedCopy-->
```

- Optionale RPMs

Führen Sie den folgenden Befehl aus, um das optionale `RPMs`-Repository zum Installieren einiger Abhängigkeitspakete von `x11vnc` zu aktivieren:

```
1 subscription-manager repos --enable rhel-7-server-optional-rpms  
   --enable rhel-7-server-extras-rpms  
2 <!--NeedCopy-->
```

Für RHEL 8.x:

Führen Sie die nachstehenden Befehle aus, um `python-websocketify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren.

```
1 sudo pip3 install websocketify  
2 sudo yum install x11vnc  
3 <!--NeedCopy-->
```

Zum Auflösen von `x11vnc` aktivieren Sie die EPEL- und CodeReady Linux Builder-Repositories:

```
1 dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-  
   release-latest-8.noarch.rpm  
2  
3 subscription-manager repos --enable "codeready-builder -for-rhel-8-  
   x86_64-rpms"  
4 <!--NeedCopy-->
```

Ubuntu:

Führen Sie die nachstehenden Befehle aus, um `python-websocketify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
1 sudo pip3 install websocketify  
2 sudo apt-get install x11vnc  
3 <!--NeedCopy-->
```

SUSE:

Führen Sie die nachstehenden Befehle aus, um `python-websocketify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
1 sudo pip3 install websocketify  
2 sudo zipper install x11vnc
```

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

Für Debian:

Führen Sie die nachstehenden Befehle aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
1 sudo pip3 install websockify
2 sudo apt-get install x11vnc
3 <!--NeedCopy-->
```

Port

Die Sitzungsspiegelung wählt automatisch verfügbare Ports aus dem Bereich 6001–6099 für den Aufbau von Verbindungen vom Linux VDA mit `Citrix Director` aus. Daher ist die Anzahl der ICA-Sitzungen, die Sie gleichzeitig spiegeln können, auf 99 begrenzt. Stellen Sie sicher, dass genügend Ports zur Verfügung stehen, insbesondere wenn mehrere Sitzungen gespiegelt werden.

Registrierung

Die folgende Tabelle enthält die relevanten Registrierungseinträge:

Registrierung	Beschreibung	Standardwert
EnableSessionShadowing	Aktiviert oder deaktiviert die Sitzungsspiegelung	1 (aktiviert)
ShadowingUseSSL	Legt fest, ob die Verbindung zwischen Linux VDA und Citrix Director verschlüsselt werden soll.	0 (deaktiviert)

Führen Sie den Befehl `ctxreg` auf dem Linux VDA aus, um die Registrierungswerte zu ändern. Um beispielsweise die Sitzungsspiegelung zu deaktivieren, führen Sie den folgenden Befehl aus:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\VirtualDesktopAgent" -v "EnableSessionShadowing" -d 0x00000000
```

SSL

Für die noVNC-Verbindung zwischen Linux VDA und Citrix Director wird das WebSocket-Protokoll verwendet. Ob bei der Sitzungsspiegelung `ws://` oder `wss://` ausgewählt wird, hängt vom o. g. Reg-

istrierungswert “ShadowingUseSSL” ab. Standardmäßig wird `ws://` ausgewählt. Aus Sicherheitsgründen empfehlen wir jedoch die Verwendung von `wss://` und die Installation von Zertifikaten auf jedem Citrix Director-Client und jedem Linux VDA-Server. Citrix übernimmt keinerlei Haftung für die Sicherheit bei Spiegelung von Linux VDA-Sitzungen mit `ws://`.

Beschaffung von Server- und SSL-Stammzertifikat Zertifikate müssen von einer vertrauenswürdigen Zertifizierungsstelle signiert werden.

Ein separates Serverzertifikat einschließlich Schlüssel ist für jeden Linux VDA-Server erforderlich, auf dem Sie SSL konfigurieren möchten. Da durch ein Serverzertifikat ein ganz bestimmter Computer identifiziert wird, müssen Sie den vollqualifizierten Domännennamen (FQDN) jedes Servers kennen. Sie können stattdessen ein Platzhalterzertifikat für die gesamte Domäne verwenden. In diesem Fall müssen Sie zumindest den Domännennamen kennen.

Ein Stammzertifikat ist auch für jeden Citrix Director-Client erforderlich, der mit dem Linux VDA kommuniziert. Stammzertifikate erhalten Sie von derselben Zertifizierungsstelle, die auch die Serverzertifikate ausgibt.

Sie können Server- und Clientzertifikate von den folgenden Zertifizierungsstellen installieren:

- Eine Zertifizierungsstelle, die mit Ihrem Betriebssystem gebündelt ist
- Eine Unternehmenszertifizierungsstelle (eine Zertifizierungsstelle, die Ihr Unternehmen Ihnen zugänglich macht)
- Eine Zertifizierungsstelle, die nicht mit Ihrem Betriebssystem gebündelt ist

Fragen Sie das Sicherheitsteam Ihres Unternehmens, mit welcher Methode Zertifikate abgerufen werden.

Wichtig:

- Der allgemeine Name (CN) für ein Serverzertifikat muss in Form des FQDN des Linux VDA oder mindestens eines richtigen Platzhalterzeichens plus Domänenzeichen angegeben werden. Beispiel: `vda1.basedomain.com` oder `*.basedomain.com`.
- Hashalgorithmen einschließlich SHA1 und MD5 sind für einige Browser zu schwach für Signaturen in digitalen Zertifikaten. Daher wird SHA-256 als Mindeststandard angegeben.

Installieren eines Stammzertifikats auf jedem Citrix Director-Client Die Sitzungsspiegelung verwendet denselben registrierungsbasierten Zertifikatsspeicher wie IIS. Sie können daher Zertifikate wahlweise mit IIS oder dem Zertifikat-Snap-In der Microsoft Management Console (MMC) installieren. Wenn Sie ein Zertifikat von einer Zertifizierungsstelle erhalten haben, rufen Sie den IIS-Assistenten für Webserverzertifikate wieder auf. Der Assistent führt den Prozess fort und installiert das Zertifikat. Sie können auch Zertifikate mit der MMC anzeigen und importieren und das Zertifikat als eigenständiges

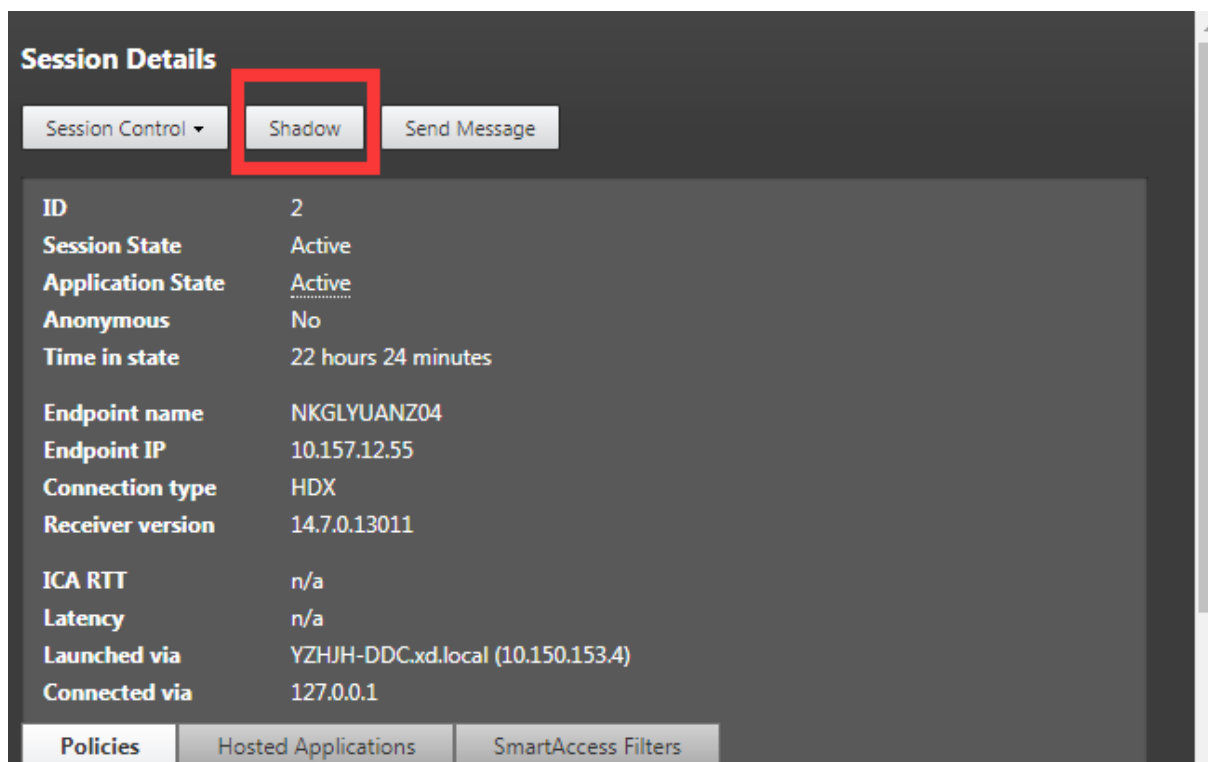
Snap-In hinzufügen. Bei Internet Explorer und Google Chrome werden die unter dem Betriebssystem installierten Zertifikate standardmäßig importiert. Bei Mozilla Firefox müssen Sie die Root-SSL-Zertifikate über die Registerkarte **Berechtigungen** des Zertifikatsmanagers importieren.

Installieren Sie ein Serverzertifikat und den zugehörigen Schlüssel auf jedem Linux VDA-Server

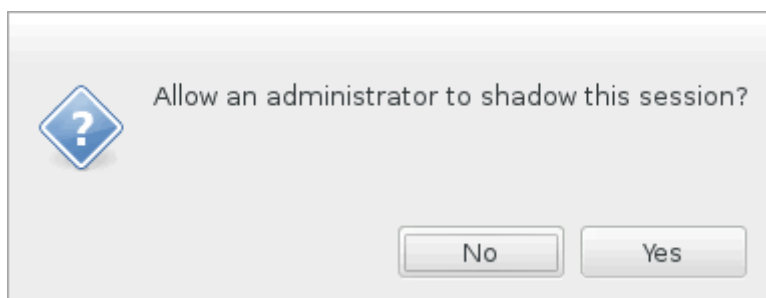
Benennen Sie die Serverzertifikate "shadowingcert.*" und die Schlüsseldatei "shadowingkey.*" (* gibt das Format an, z. B. shadowingcert.pem und shadowingkey.key). Legen Sie Serverzertifikate und Schlüsseldateien im Pfad **/etc/xdm/shadowingssl** ab und schützen Sie sie ordnungsgemäß mit eingeschränkten Berechtigungen. Ein Fehler bei Namen oder Pfad führt dazu, dass der Linux VDA das Zertifikat bzw. die Schlüsseldatei nicht findet und einen Verbindungsfehler mit **Citrix Director** verursacht.

Verwendung

Suchen Sie in **Citrix Director** die Zielsitzung und klicken Sie in der Ansicht **Sitzungsdetails** auf **Spiegeln**, um eine Spiegelungsanforderung an den Linux VDA zu senden.



Wenn die Verbindung initialisiert wurde, wird auf dem ICA-Sitzungsclient (nicht dem **Citrix Director**-Client) eine Aufforderung an den Benutzer zur Autorisierung des Spiegelns der Sitzung angezeigt.



Wenn der Benutzer auf **Ja** klickt, wird unter [Citrix Director](#) ein Fenster mit dem Hinweis angezeigt, dass die ICA-Sitzung gespiegelt wird.

Weitere Informationen zur Verwendung finden Sie in der [Dokumentation für Citrix Director](#).

Einschränkungen

- Die Sitzungsspiegelung ist nur für die Verwendung in einem Intranet vorgesehen. Sie funktioniert nicht in externen Netzwerken, auch nicht über Citrix Gateway. Citrix übernimmt keinerlei Haftung bei Spiegelung von Linux VDA-Sitzungen in einem externen Netzwerk.
- Wenn die Sitzungsspiegelung aktiviert ist, kann ein Domänenadministrator die ICA-Sitzungen anzeigen, hat jedoch keine Berechtigung zum Schreiben oder Steuern.
- Wenn ein Administrator in [Citrix Director](#) auf **Spiegeln** klickt, wird dem Benutzer eine Aufforderung zum Zulassen der Spiegelung der Sitzung angezeigt. Eine Sitzung kann nur gespiegelt werden, wenn der Sitzungsbenutzer die Berechtigung erteilt.
- Für die o. g. Aufforderung gilt ein Timeout von 20 Sekunden. Nach Ablauf des Timeouts schlägt sie fehl.
- Eine Sitzung kann nur von einem Administrator gespiegelt werden. Wenn Administrator B beispielsweise eine Spiegelungsanforderung für einen Sitzungsadministrator A sendet, wird die Aufforderung zum Zulassen erneut auf dem Benutzergerät angezeigt. Stimmt der Benutzer zu, wird die Spiegelungsverbindung von Administrator A beendet und eine neue Spiegelungsverbindung für Administrator B erstellt. Wenn ein Administrator eine weitere Spiegelungsanforderung für dieselbe Sitzung sendet, kann auch eine neue Spiegelungsverbindung erstellt werden.
- Installieren Sie zum Verwenden der Sitzungsspiegelung [Citrix Director](#) 7.16 oder höher.
- [Citrix Director](#)-Clients verwenden beim Herstellen einer Verbindung mit dem Linux VDA-Server den FQDN anstelle der IP-Adresse. Daher muss der [Citrix Director](#)-Client in der Lage sein, den FQDN des Linux VDA-Servers aufzulösen.

Problembehandlung

Wenn die Sitzungsspiegelung fehlschlägt, debuggen Sie sowohl auf dem **Citrix Director**-Client als auch auf dem Linux VDA.

Citrix Director-Client

Prüfen Sie mit den Entwicklertools des Browsers die Ausgabeprotokolle auf der Registerkarte **Konsole**. Oder überprüfen Sie die Antwort der ShadowLinuxSession-API auf der Registerkarte **Netzwerk**. Wenn die Aufforderung zum Abrufen der Zulassung beim Benutzer angezeigt wird, der Verbindungsaufbau jedoch fehlschlägt, senden Sie manuell einen Ping an den FQDN des VDA, um zu überprüfen, ob **Citrix Director** den FQDN auflösen kann. Bei Problemen mit der **wss://**-Verbindung sollten Sie Ihre Zertifikate überprüfen.

Linux VDA

Vergewissern Sie sich, dass auf eine Spiegelungsanforderung hin die Aufforderung zum Abrufen der Zulassung beim Benutzer angezeigt wird. Ist dies nicht der Fall, überprüfen Sie die Dateien `vda.log` und `hdx.log` auf Hinweise. Gehen Sie folgendermaßen vor, um die Datei `vda.log` zu erhalten:

1. Suchen Sie die Datei `/etc/xdl/ctx-vda.conf`. Kommentieren Sie die folgende Zeile aus, um die `vda.log`-Konfiguration zu aktivieren:

```
Log4jConfig="/etc/xdl/log4j.xml"
```

2. Öffnen Sie `/etc/xdl/log4j.xml`, suchen Sie den Teil `com.citrix.dmc` und ändern Sie "info" wie folgt in "trace":

```
1  <!-- Broker Agent Plugin - Director VDA plugin Logger -->
2
3  <logger name="com.citrix.dmc">
4
5      <level value="trace"/>
6
7  </logger>
8  <!--NeedCopy-->
```

3. Führen Sie den Befehl `service ctxvda restart` aus, um den `ctxvda`-Dienst neu zu starten.

Im Fall eines Fehlers beim Verbindungsaufbau:

1. Überprüfen Sie, ob eine Firewall-Beschränkung vorliegt, die das Öffnen des Ports durch die Sitzungsspiegelung verhindert.

2. Vergewissern Sie sich, dass Sie die Zertifikate und Schlüsseldateien ordnungsgemäß benannt und für das SSL-Szenario im richtigen Verzeichnis abgelegt haben.
3. Stellen Sie sicher, dass zwischen 6001 und 6099 genügend Ports für neue Spiegelungsanforderungen vorhanden sind.

Monitor Service Daemon

October 5, 2022

Der Monitor Service Daemon überwacht wichtige Dienste durch periodisch durchgeführte Scans. Beim Erkennen einer Ausnahme werden Dienstprozesse vom Daemon angehalten oder neu gestartet, und Prozesse werden zur Freigabe von Ressourcen bereinigt. Die erkannten Ausnahmen werden in der Datei **/var/log/xdl/ms.log** aufgezeichnet.

Konfiguration

Der Monitor Service Daemon wird automatisch gestartet, wenn Sie den VDA starten.

Sie können das Feature mit Administratorrechten über die Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** unter **/opt/Citrix/VDA/sbin** konfigurieren.

Starten Sie den Monitor Service Daemon über folgenden Befehl neu, damit die Änderungen in den Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** wirksam werden.

```
1 service ctxmonitorservice restart
2 <!--NeedCopy-->
```

- **scanningpolicy.conf**

Diese Konfigurationsdatei aktiviert oder deaktiviert den Monitor Service Daemon. Sie legt das Diensterkennungsintervall fest und gibt an, ob erkannte Ausnahmen repariert werden sollen.

- MonitorEnable: true/false (Standardwert: true)
- DetectTime: 20 (Einheit: Sekunden, Standardwert: 20, Mindestwert: 5)
- AutoRepair: true/false (Standardwert: true)
- MultBalance: false
- ReportAlarm: false

- **rulesets.conf**

Diese Konfigurationsdatei legt fest, welche Dienste überwacht werden. Vier Dienste werden standardmäßig überwacht, wie in der folgenden Bildschirmaufnahme zu sehen ist.



```
MonitorUser: all
MonitorType: 3
ProcessName: ctxhdx
Operation: 4
DBRecord: false

MonitorUser: all
MonitorType: 3
ProcessName: ctxvda
Operation: 4
DBRecord: false

MonitorUser: all
MonitorType: 3
ProcessName: ctxpolicyd
Operation: 4
DBRecord: false

MonitorUser: all
MonitorType: 3
ProcessName: Xorg
Operation: 8
DBRecord: false
```

Legen Sie die folgenden Felder fest, um die zu überwachenden Dienste zu konfigurieren.

- **MonitorUser:** all
- **MonitorType:** 3
- **ProcessName:** <> (Der Prozessname darf nicht leer sein und muss exakt übereinstimmen.)
- **Operation:** 1/2/4/8 (1 = Dienst bei erkannter Ausnahme anhalten. 2 = Dienst bei erkannter Ausnahme abbrechen. 4 = Dienst neu starten. 8 = Xorg-Prozess bereinigen.)
- **DBRecord:** false

- **whitelist.conf**

Die in der Datei **rulesets.conf** angegebenen Zieldienste müssen auch in der Datei **whitelist.conf** konfiguriert werden. Die konfigurierte Positivliste agiert als zweiter Sicherheitsfilter.

Zum Konfigurieren der Positivliste fügen Sie nur die Prozessnamen (die exakt übereinstimmen müssen) in die Datei **whitelist.conf** ein. Ein Beispiel sehen Sie im folgenden Screenshot.

```
ctxcdmnd  
ctxcdmmount  
ctxcdmstat  
ctxceip  
ctxclipboard  
ctxconnect  
ctxcredentialctl  
ctxctl  
ctxcupsd  
ctxdisconnect  
ctxeuem  
ctxfiletransfer  
ctxgfx  
ctxhdx  
ctxism  
ctxlogd  
ctxlogin  
ctxmonitorservice  
ctxmrvc  
ctxpolicyd  
ctxscardsd  
ctxvhcid  
ctxvda  
Xorg
```

Hinweis:

Beenden Sie erst den Monitor Service Daemon mit dem Befehl `service ctxmonitorservice stop`, bevor Sie die Dienste `ctxvda`, `ctxhdx` und `ctxpolicyd` anhalten. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Tools und Hilfsprogramme

May 4, 2023

Hilfsprogramm zur Abfrage von Sitzungsdaten

Wir bieten ein Hilfsprogramm (`ctxsdcutil`), mit dem Sie Sitzungsdaten für jeden Linux VDA abfragen können. Führen Sie den Befehl `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]` aus, um die folgenden Daten aller Sitzungen oder einer bestimmten Sitzung auf einem VDA abzufragen. Das Argument `[-c]` bedeutet, dass Daten im Sekundentakt abgefragt werden.

- **Eingabebandbreite für Sitzung**

- **Ausgabebandbreite für Sitzung**
- **Ausgabeübertragungsrate für Sitzung**
- **Latenz - zuletzt gemessen**
- **Roundtripzeit**
- **Ausgabebandbreite für Thinwire**
- **Ausgabebandbreite für Audio**
- **Ausgabebandbreite für Drucker**
- **Eingabebandbreite für Laufwerk**
- **Ausgabebandbreite für Laufwerk**

Das xdlcollect-Bashskript

Das `xdlcollect`-Bashskript zum Sammeln der Protokolle ist in die Linux VDA-Software integriert und unter `/opt/Citrix/VDA/bin` zu finden. Nach der Installation des Linux VDA können Sie den Befehl `bash /opt/Citrix/VDA/bin/xdlcollect.sh` ausführen, um Protokolle zu sammeln. Nach Abschluss der Protokollsammlung wird eine komprimierte Protokolldatei in dem Ordner mit dem Skript generiert. Das `xdlcollect` Bash-Skript kann fragen, ob Sie die komprimierte Protokolldatei in Citrix Insight Services (CIS) hochladen möchten. Wenn Sie zustimmen, gibt `xdlcollect` nach Abschluss des Uploads eine `upload_ID` zurück. Die komprimierte Protokolldatei wird beim Upload nicht von Ihrem lokalen Computer entfernt. Andere Benutzer können mit der `upload_ID` auf die Protokolldatei in CIS zugreifen.

XDPing

Das Linux-**XDPing**-Tool ist eine Befehlszeilenanwendung. Sie können damit das Prüfen auf häufige Konfigurationsprobleme in einer Linux VDA-Umgebung automatisieren.

Das Linux **XDPing**-Tool führt mehr als 150 Einzeltests im System durch, die wie folgt kategorisiert werden können:

- Überprüfen, ob die Systemanforderungen für Linux VDA erfüllt sind
- Identifizieren und Anzeigen von Maschineninformationen einschließlich der Linux-Distributionen
- Überprüfen der Linux-Kernel-Kompatibilität
- Überprüfen, ob bekannte Probleme mit der Linux-Distribution vorliegen, die die Funktion des Linux VDA beeinträchtigen können
- Überprüfen des Security-Enhanced Linux (SELinux)-Modus und der Kompatibilität
- Identifizieren von Netzwerkschnittstellen und Überprüfen der Netzwerkeinstellungen

- Überprüfen der Speicherpartitionierung und des verfügbaren Speicherplatzes
- Überprüfen der Konfiguration von Maschinenhost und Domänenname
- Überprüfen der DNS-Konfiguration und Durchführen von Suchtests
- Identifizieren zugrunde liegender Hypervisoren und Überprüfen der Konfiguration virtueller Maschinen. Unterstützung für:
 - Citrix Hypervisor
 - Microsoft Hyper-V
 - VMware vSphere
- Überprüfen der Zeiteinstellungen und der Betriebsbereitschaft der Netzwerkzeitsynchronisierung
- Überprüfen, ob der PostgreSQL-Dienst ordnungsgemäß konfiguriert und betriebsbereit ist
- Überprüfen, ob die Firewall aktiviert ist und die erforderlichen Ports offen sind
- Überprüfen der Kerberos-Konfiguration und Durchführen von Authentifizierungstests
- Überprüfen der LDAP-Suchumgebung für die Gruppenrichtlinienengine
- Überprüfen, ob die Active Directory-Integration ordnungsgemäß eingerichtet und die aktuelle Maschine mit der Domäne verbunden ist. Unterstützung für:
 - Samba Winbind
 - Dell Quest Authentication Services
 - Centrify DirectControl
 - SSSD
- Überprüfen der Integrität des Linux-Computerobjekts in Active Directory
- Überprüfen der PAM-Konfiguration (Pluggable Authentication Module)
- Überprüfen des Coredump-Musters
- Überprüfen, ob alle vom Linux VDA benötigten Pakete installiert sind
- Identifizieren des Linux VDA-Pakets und Überprüfen der Integrität der Installation
- Überprüfen der Integrität der PostgreSQL-Registrierungsdatenbank
- Überprüfen, ob die Linux VDA-Dienste ordnungsgemäß konfiguriert und betriebsbereit sind
- Überprüfen der Integrität der VDA- und HDX-Konfiguration
- Test jedes konfigurierten Delivery Controllers, um zu prüfen, ob der Brokerdienst erreichbar und betriebsbereit ist und reagiert
- Überprüfen, ob die Maschine bei der Delivery Controller-Farm registriert ist
- Überprüfen des Zustands jeder aktiven oder getrennten HDX-Sitzung
- Scannen von Protokolldateien auf Linux VDA-bezogene Fehler und Warnungen
- Prüfen der Eignung der Version von Xorg

Verwenden des Linux XDPing-Tools

Hinweis:

Durch Ausführen von `ctxsetup.sh` wird **XDPing** nicht installiert. Sie können `sudo /opt/Citrix/VDA/bin/xdping` ausführen, um **XDPing** zu installieren.

Der Befehl erstellt auch die für **XDPing** erforderliche virtuelle Python3-Umgebung. Wenn durch den Befehl keine virtuelle Python3-Umgebung erstellt wird, erstellen Sie sie gemäß den Anweisungen unter [Erstellen einer virtuellen Python3-Umgebung](#) manuell.

Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des Pip-Tools auftreten können, sollten Sie die folgenden vertrauenswürdigen Hosts zur Datei `/etc/pip.conf` hinzufügen:

```
[global]
trusted-host =
    pypi.org
    files.pythonhosted.org
```

XDPing enthält die einzelne ausführbare Datei `xdping`, die über die Befehlsshell ausgeführt wird.

Zur Anzeige der Befehlszeilenoptionen verwenden Sie die Option `-h`:

```
1 sudo /opt/Citrix/VDA/bin/xdping -h
2 <!--NeedCopy-->
```

Zum Ausführen aller Tests führen Sie `xdping` ohne Befehlszeilenoptionen aus:

```
1 sudo /opt/Citrix/VDA/bin/xdping
2 <!--NeedCopy-->
```

Zum Überprüfen der Umgebung, bevor Sie das Linux VDA-Paket installieren, führen Sie die Tests `pre-flight` aus:

```
1 sudo /opt/Citrix/VDA/bin/xdping --preflight
2 <!--NeedCopy-->
```

Um nur bestimmte Testkategorien auszuführen, z. B. die Zeit- und Kerberos-Tests, verwenden Sie die Option `-T`:

```
1 sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
2 <!--NeedCopy-->
```

Zum Untersuchen eines bestimmten XenDesktop Controllers:

```
1 sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
2 <!--NeedCopy-->
```

Beispielausgabe Dies ist die Beispielausgabe eines ausgeführten Kerberos-Tests:

sudo xdping -T kerberos

```

Root User -----
  User:          root
  EUID:          0
  Verify user is root                                     [Pass]

Kerberos -----
  Kerberos version: 5
  Verify Kerberos available                             [Pass]
  Verify Kerberos version 5                             [Pass]
  KRB5CCNAME:    [Not set]
                  Distro default FILE:/tmp/krb5cc_%{uid}
  KRB5CCNAME type: [Supported]
  KRB5CCNAME format: [Default]
  Verify KRB5CCNAME cache type                           [Pass]
  Verify KRB5CCNAME format                               [Pass]
  Configuration file: /etc/krb5.conf [Exists]

  Verify Kerberos configuration file found                [Pass]
  Keytab file:   /etc/krb5.keytab [Exists]
  Default realm: XD2.LOCAL
  Default realm KDCs: [NONE SPECIFIED]
  Default realm domains: [NONE SPECIFIED]
  DNS lookup realm: [Enabled]
  DNS lookup KDC: [Enabled]
  Weak crypto: [Disabled]
  Clock skew limit: 300 s
  Verify system keytab file exists                        [Pass]
  Verify default realm set                               [Pass]
  Verify default realm in upper-case                     [Pass]
  Verify default realm not EXAMPLE.COM                   [Pass]
  Verify default realm domain mappings                   [Pass]
  Verify default realm master KDC configured             [Pass]
  Verify Kerberos weak crypto disabled                   [Pass]
  Verify Kerberos clock skew setting                     [Pass]
  Default ccache: [Not set]
                  Distro default FILE:/tmp/krb5cc_%{uid}
  Default ccache type: [Supported]
  Default ccache format: [Default]
  Verify default credential cache cache type              [Pass]
  Verify default credential cache format                  [Pass]
  UPN system key [MYVDA1$@██████████]: [MISSING]
  SPN system key [host/██████████/1]: [Exists]
  Verify Kerberos system keys for UPN exist               [ERROR]
  No system keys were found for the user principal name (UPN) of
  the machine account. For the Linux VDA to mutually authenticate
  with the Delivery Controller, the system keytab file must
  contain keys for both the UPN and host-based SPN of the machine
  account.

```



```
Verify Kerberos system keys for SPN exist [Pass]
Kerberos login: [FAILED AUTHENTICATION]
    Keytab contains no suitable keys for MYVDA1$@>
    while getting initial credentials
Verify KDC authentication [ERROR]
Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
from the KDC authentication service for the machine account UPN
MYVDA1$@>. Check that the Kerberos configuration is
valid and the keys in the system keytab are current.

Summary -----
The following tests did not pass:
Verify Kerberos system keys for UPN exist [ERROR]
Verify KDC authentication [ERROR]
```

Sonstiges

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Unterstützung für Citrix Workspace-App für HTML5](#)
- [Erstellen einer virtuellen Python3-Umgebung](#)
- [Integrieren von NIS in Active Directory](#)
- [IPv6](#)
- [LDAPS](#)
- [Xauthority](#)

Unterstützung für Citrix Workspace-App für HTML5

October 5, 2022

Sie können die Citrix Workspace-App für HTML5 verwenden, um in Linux auf virtuelle Apps und Desktops direkt zuzugreifen, ohne dass Ihr Client mit Citrix Gateway verbunden ist. Weitere Informationen über die Citrix Workspace-App für HTML5 finden Sie in der [Citrix-Dokumentation](#).

Aktivieren des Features

Das Feature ist in der Standardeinstellung deaktiviert. Gehen Sie folgendermaßen vor, um es zu aktivieren:

1. Aktivieren Sie in Citrix StoreFront die Citrix Workspace-App für HTML5.

Das ausführliche Verfahren finden Sie im Schritt 1 des Knowledge Center-Artikels [CTX208163](#).

2. Aktivieren Sie WebSocket-Verbindungen.

- a) Legen Sie in Citrix Studio für die Richtlinie **WebSockets-Verbindungen** die Einstellung **Zugelassen** fest.

Sie können auch die anderen WebSocket-Richtlinien festlegen. Eine vollständige Liste der WebSocket-Richtlinien finden Sie unter [WebSockets-Richtlinieneinstellungen](#).

- b) Starten Sie auf dem VDA den `ctxvda`-Dienst und den `ctxhdx`-Dienst neu –in dieser Reihenfolge –damit die Einstellungen wirksam werden.
- c) Führen Sie auf dem VDA den folgenden Befehl aus, um zu überprüfen, ob der WebSocket-Listener ausgeführt wird.

```
netstat -an | grep 8008
```

Wenn der WebSocket-Listener ausgeführt wird, ähnelt die Befehlsausgabe der folgenden:

```
tcp 0 0 :::8008 :::* LISTEN
```

Hinweis: Sie können auch die TLS-Verschlüsselung aktivieren, um WebSocket-Verbindungen zu sichern. Weitere Informationen zum Aktivieren der TLS-Verschlüsselung finden Sie unter [Schützen von Benutzersitzungen mit TLS](#).

Virtuelle Python3-Umgebung erstellen

November 22, 2023

Beim Verbinden mit dem Netzwerk können Sie den Befehl `sudo /opt/Citrix/VDA/bin/xdping` oder `/opt/Citrix/VDA/sbin/enable_ldaps.sh` ausführen, um eine virtuelle Python3-Umgebung zu erstellen. Wird durch die Befehle keine virtuelle Python3-Umgebung erstellt, können Sie sie selbst ohne Netzwerkverbindung manuell erstellen. In diesem Artikel werden die Voraussetzungen und Schritte zum Erstellen einer virtuellen Python3-Umgebung ohne Netzwerkverbindung beschrieben.

Voraussetzungen

- Sie müssen über Administratorrechte verfügen, um auf das Verzeichnis `/opt/Citrix/VDA/sbin/ctxpython3` zugreifen zu können.
- Die WHL-Dateien von Python3-Paketen sind vorhanden. Sie finden die WHL-Dateien zum Download unter <https://pypi.org/>.

Virtuelle Python3-Umgebung erstellen

Führen Sie die folgenden Schritte aus, um eine virtuelle Python3-Umgebung zu erstellen:

1. Installieren Sie Python3-Abhängigkeiten.

Amazon Linux 2:

```
1 yum -y install python3 python3-devel krb5-devel gcc
2 <!--NeedCopy-->
```

Für RHEL:

```
1 yum -y install python36-devel krb5-devel gcc
2 <!--NeedCopy-->
```

Hinweis:

Möglicherweise müssen Sie ein bestimmtes Repository aktivieren, um einige Abhängigkeiten zu installieren. Für RHEL 7 führen Sie den Befehl `subscription-manager repos --enable rhel-7-server-optional-rpms` aus. Für RHEL 8 führen Sie den Befehl `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms` aus.

Für Ubuntu, Debian:

```
1 apt-get -y install python3-dev python3-pip python3-venv libkrb5-
  dev
2 <!--NeedCopy-->
```

SUSE:

```
1 zypper -n install lsb-release python3-devel python3-setuptools
  krb5-devel gcc libffi-devel libopenssl-devel
2 <!--NeedCopy-->
```

2. Erstellen Sie eine virtuelle Python3-Umgebung.

Hinweis:

Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des Pip-Tools auftreten können, sollten Sie die folgenden vertrauenswürdigen Hosts zur Datei `/etc/pip.conf` hinzufügen:

```
[global]
trusted-host =
pypi.org
files.pythonhosted.org
```

Für Amazon Linux 2, Debian, RHEL, Ubuntu:

```
1 sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
2 <!--NeedCopy-->
```

SUSE:

```
1 export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin
2
3 sudo mkdir -p /usr/lib/mit/include/gssapi/
4
5 sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/
  gssapi/gssapi_ext.h
6
7 sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
8 <!--NeedCopy-->
```

3. Installieren Sie LDAPS-Abhängigkeiten.

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
  upgrade pip==21.3.1
2
3 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
  cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi
  ==1.7.3 ldap3==2.9.1 pyasn1==0.4.8 pycparser==2.21 six==1.16.0
4 <!--NeedCopy-->
```

4. Installieren Sie **XDPing-Abhängigkeiten.**

```
1 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
  upgrade pip==21.3.1
2
3 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
  asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator
  ==5.1.1 gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging
  ==21.3 pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser
  ==2.21 pyparsing==3.0.8 scrap==1.4.1 six==1.16.0 termcolor
  ==1.1.0
4
5 sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /
  opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

Integrieren von NIS in Active Directory

October 5, 2022

In diesem Artikel wird beschrieben, wie NIS in Windows Active Directory (AD) auf dem Linux VDA über SSSD integriert wird. Der Linux VDA ist eine Komponente von Citrix Virtual Apps and Desktops. Daher passt er eng in die Windows AD-Umgebung.

Zur Verwendung von NIS statt AD als UID- und GID-Anbieter müssen die Kontoinformationen (Benutzername-/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](#).

Was ist 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.

Integrieren von NIS in Active Directory

Führen Sie die folgenden Schritte aus, um NIS in AD zu integrieren:

Schritt 1: Hinzufügen von Linux VDA als NIS-Client

Konfigurieren Sie den NIS-Client:

```
1 yum -y install ypbind rpcbind oddjob-mkhomedir
2 <!--NeedCopy-->
```

Legen Sie die NIS-Domäne fest:

```
1 ypdomainname nis.domain
2 echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
3 <!--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**:

```
1 sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
  nis.domain --enablemkhomedir --update
2 <!--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:

```
1 sudo systemctl start rpcbind ypbind
2
3 sudo systemctl enable rpcbind ypbind
4 <!--NeedCopy-->
```

Vergewissern Sie sich, dass die NIS-Konfiguration richtig ist:

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

Prüfen Sie, ob die Kontoinformationen über den NIS-Server zur Verfügung stehen:

```
1 getent passwd nisaccount
2 <!--NeedCopy-->
```

Hinweis:

nisaccount ist das tatsächliche NIS-Konto auf dem NIS-Server. Stellen Sie sicher, dass die UID, GID, das Homeverzeichnis und die Login-Shell ordnungsgemäß konfiguriert sind.

Schritt 2: Beitritt zur Domäne und Erstellen einer 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 Anbieterdokumentation zu RHEL oder CentOS. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

Treten Sie der Domäne bei und erstellen Sie eine Hostschlüsseltable 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:

```
--enablekrb5kdc dns --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
winbind offline logon = no
```

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:

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

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

Schritt 3: 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/sss/sssd.conf Muster einer **sssd.conf**-Konfiguration (weitere Optionen können bei Bedarf hinzugefügt werden):

```
1 [sssd]
2 config_file_version = 2
3 domains = EXAMPLE
4 services = nss, pam
5
6 [domain/EXAMPLE]
7 # Uncomment if you need offline logins
8 # cache_credentials = true
9 re_expression = (((?P<domain>[^\[]+)\.?(?P<name>.+)) | ((?P<name>[^\[]+)\.?(?P<domain>.+)) | (^?(?P<name>[^\[]+)\.?$))
10 id_provider = proxy
11 proxy_lib_name = nis
12 auth_provider = ad
13 access_provider = ad
14
15 # Should be specified as the long version of the Active Directory
    domain.
16 ad_domain = EXAMPLE.COM
17
18 # Kerberos settings
19 krb5_ccachedir = /tmp
20 krb5_ccname_template = FILE:%d/krb5cc_%U
21
22 # Uncomment if service discovery is not working
23 # ad_server = server.ad.example.com
24
25 # Comment out if the users have the shell and home dir set on the AD
    side
26 default_shell = /bin/bash
27 fallback_homedir = /home/%d/%u
28
29 # Uncomment and adjust if the default principal SHORTNAME$@REALM is not
    available
30 # ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
31 <!--NeedCopy-->
```

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/sss/sssd.conf
chmod 0600 /etc/sss/sssd.conf
restorecon /etc/sss/sssd.conf
```


Schritt 4: Konfigurieren von NSS/PAM

RHEL/CentOS:

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

```
1 authconfig --enablesssd --enablesssdauth --enablemkhomedir --update
2
3 sudo systemctl start sssd
4
5 sudo systemctl enable sssd
6 <!--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.

Schritt 5: 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:

```
1 sudo klist -ke
2 <!--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:

```
1 sudo kinit -k MACHINE$@REALM
2 <!--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:

```
1 sudo klist -ke
```

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

Schritt 6: Überprüfen der Benutzerauthentifizierung

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

```
1 sudo getent passwd DOMAIN\username
2 <!--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.

```
1 sudo ssh localhost -l DOMAIN\username
2
3 id -u
4 <!--NeedCopy-->
```

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

```
1 ls /tmp/krb5cc_{
2 uid }
3
4 <!--NeedCopy-->
```

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

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

IPv6

October 5, 2022

Der Linux VDA unterstützt IPv6 ebenso wie Citrix Virtual Apps and Desktops. Beachten Sie bei der Verwendung dieses Features Folgendes:

- Für Umgebungen mit dualtem 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 "HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD"
  -v "ControllerRegistrationIPv6Netmask"
3 <!--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 IPv6-Bereitstellung in Citrix Virtual Apps and Desktops finden Sie unter [IPv4/IPv6-Unterstützung](#).

Problembehandlung

Überprüfen Sie die grundlegende IPv6-Netzwerkumgebung und prüfen Sie mit ping6, ob AD und Delivery Controller erreichbar sind.

LDAPS

October 5, 2022

LDAPS ist die sichere Version des Lightweight Directory Access Protocol (LDAP), wobei die LDAP-Kommunikation mit TLS/SSL verschlüsselt wird.

Standardmäßig wird die LDAP-Kommunikation zwischen Client- und Serveranwendungen nicht verschlüsselt. Mit LDAPS schützen Sie den Inhalt von LDAP-Abfragen zwischen Linux VDA- und LDAP-Server.

Die folgenden Linux VDA-Komponenten benötigen LDAPS:

- Brokeragent: Registrierung des Linux VDA bei einem Delivery Controller
- Richtlinienendienst: 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

Hinweis:

Mit folgendem Befehl können Sie einen Überwachungszyklus für die LDAP-Server festlegen. Der Standardwert ist 15 Minuten. Stellen Sie den Wert auf mindestens 10 Minuten ein.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent" -v "ListOfLDAPServersMonitorPeroid" -t "
  REG_DWORD" -d "0x0000000f" --force
2 <!--NeedCopy-->
```

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:

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](#).

Wenn Sie eine Zertifikatauthentifizierungshierarchie mit mehreren Ebenen verwenden, besitzen Sie nicht automatisch das geeignete Zertifikat für die LDAPS-Authentifizierung auf dem Domänencontroller.

Informationen zum Aktivieren von LDAPS für Domänencontroller über eine Zertifikatauthentifizierungshierarchie mit mehreren Ebenen finden Sie im Artikel [LDAP over SSL \(LDAPS\) Certificate](#).

Aktivieren der Stammzertifizierungsstelle für Clients

Der Client muss ein Zertifikat einer Zertifizierungsstelle verwenden, dem der LDAP-Server vertraut. Importieren Sie das Stammzertifizierungsstellenzertifikat in einen 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 auf dem 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:

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
2 <!--NeedCopy-->
```

- Aktivieren von LDAP über SSL/TLS mit Kanalbindung:

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
2 <!--NeedCopy-->
```

Hinweis:

Das Stammzertifizierungsstellenzertifikat für die Kanalbindung muss im PEM-Format vorliegen. Wenn durch Aktivieren von LDAPS keine virtuelle Python3-Umgebung erstellt wird, erstellen Sie sie gemäß den Anweisungen unter [Erstellen einer virtuellen Python3-Umgebung](#) manuell.

Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des Pip-Tools auftreten können, sollten Sie die folgenden vertrauenswürdigen Hosts zur Datei `/etc/pip.conf` hinzufügen:

```
[global]
trusted-host =
pypi.org
files.pythonhosted.org
```

- Fallback auf LDAP ohne SSL/TLS

```
1 /opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
2 <!--NeedCopy-->
```

Der Java-Schlüsselspeicher für LDAPS ist in `/etc/xdm/.keystore`. Unter anderem sind folgende Registrierungsschlüssel betroffen:

```
1 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers
2
3 HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy
4
5 HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS
6
7 HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore
8
9 HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
10 <!--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, Centrifry 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 Port 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. Betroffene Konfigurationsdateien sind **/etc/samba/smb.conf** und **/etc/openldap/ldap.conf** (für RHEL) oder **/etc/ldap/ldap.conf** (für Ubuntu). Nehmen Sie an den Dateien die folgenden Änderungen vor:

- smb.conf

```
ldap ssl = start tls
ldap ssl ads = yes
client ldap sasl wrapping = plain
```
- ldap.conf

```
TLS_REQCERT never
```

Alternativ können Sie sicheres LDAP mit SASL GSSAPI Sign and Seal konfigurieren; es kann jedoch nicht neben TLS/SSL existieren. Um SASL-Verschlüsselung zu verwenden, ändern Sie die Konfiguration für **smb.conf**:

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

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 Sie die LDAPS-bezogenen Schlüssel versehentlich ohne **enable_ldaps.sh** aktualisiert haben, 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. Wir empfehlen das mit base64 verschlüsselte PEM-Format, wenn ein Problem mit dem Zertifikatsformat 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/xdm/.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.

Xauthority

October 5, 2022

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 Local-host 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 befindet sich im Homeverzeichnis jedes Benutzers. 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:

```
1 # xauth -f ~/.Xauthority
2
3 # > list
4
5 # > us01msip06:107 MIT-MAGIC-COOKIE-1
   fb228d1b695729242616c5908f11624b
6 <!--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 Cookie Nummern in Xorg enthält.

Konfigurieren von Xauthority

Um **Xauthority** im Linux VDA für X11-Remoteanzeige zu aktivieren, müssen Sie die zwei folgenden Registrierungsschlüssel erstellen:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
   XauthEnabled" -d "0x00000001" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
   -d "0x00000001" --force
4 <!--NeedCopy-->
```

Übergeben Sie die `.Xauthority`-Datei nach dem Aktivieren von **Xauthority** manuell oder durch Bereitstellen eines freigegebenen Homeverzeichnisses an den **XClient**:

- Manuelle Übergabe der `.Xauthority`-Datei an den XClient

Nach dem Start einer ICA-Sitzung generiert der Linux VDA die `.Xauthority`-Datei für den XClient und speichert die Datei im Homeverzeichnis des Anmeldebenutzers. Sie können die `.Xauthority`-Datei auf die remote XClient-Maschine 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:

```
1 export DISPLAY={
2   Display number stored in the Xauthority file }
3
4
5 export XAUTHORITY={
6   the file path of .Xauthority }
7
8 <!--NeedCopy-->
```

Hinweis:

Wenn die Umgebungsvariable **XAUTHORITY** nicht festgelegt ist, wird standardmäßig die Datei `~/.Xauthority` verwendet.

- Übergabe der `.Xauthority`-Datei an den XClient durch Bereitstellen eines freigegebenen Homeverzeichnisses

Eine bequeme Methode ist das Bereitstellen eines freigegebenen Homeverzeichnis für den Benutzer, der sich anmeldet. Wenn der Linux VDA eine ICA-Sitzung startet, wird die `.Xauthority`-Datei im Homeverzeichnis des Anmeldebenutzers erstellt. Wenn dieses Homeverzeichnis für den XClient freigegeben ist, muss der Benutzer diese `.Xauthority`-Datei nicht manuell an den XClient übergeben. 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:

```
1 ps aux | grep -i xorg
2 <!--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:

```
1 /var/xdl/xauth/.Xauthority110
2 <!--NeedCopy-->
```

Zeigen Sie Cookies mit dem Befehl **Xauth** an:

```
1 Xauth -f /var/xdl/xauth/.Xauthority110
2 <!--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 und der Anzeigenummer des veröffentlichten Desktops.

Führen Sie zum Beispiel den folgenden Befehl auf der XClient-Maschine aus:

```
1 telnet 10.158.11.11 6160
2 <!--NeedCopy-->
```

Die Portnummer ist die Summe von 6000 + <display number>.

Wenn dieser Telnet-Vorgang fehlschlägt, wird die Anfrage möglicherweise von der Firewall blockiert.

Authentifizierung

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Authentifizierung mit Azure Active Directory](#)
- [Single-Sign-On-Authentifizierung per Double-Hop](#)
- [Verbundauthentifizierungsdienst](#)
- [Anmeldeinformationen für den Sitzungsstart](#)
- [Smartcards](#)
- [Nicht authentifizierte Sitzungen](#)

Authentifizierung mit Azure Active Directory

October 5, 2022

Hinweis:

Dieses Feature ist nur für von Azure gehostete VDAs verfügbar.

Je nach Bedarf können Sie zwei Arten von Linux-VDAs in Azure bereitstellen:

- Mit Azure AD DS verbundene VMs. Die VMs sind mit einer verwalteten Domäne von Azure Active Directory (AAD) Domain Services (DS) verbunden. Benutzer melden sich mit ihren Domänenanmeldeinformationen bei den VMs an.
- Nicht-domänengebundene VDAs. Die VMs werden in den AAD-Identitätsdienst integriert, um die Benutzerauthentifizierung bereitzustellen. Benutzer melden sich mit ihren AAD-Anmeldeinformationen bei den VMs an.

Weitere Informationen zu AAD DS und AAD finden Sie in diesem [Microsoft-Artikel](#).

In diesem Artikel erfahren Sie, wie Sie den AAD-Identitätsdienst auf nicht in Domänen eingebundenen VDAs aktivieren und konfigurieren.

Unterstützte Distributionen

- Ubuntu 20.04, 18.04

- RHEL 8.4, 7.9
- SUSE 15.x
- Debian 10

Weitere Informationen finden Sie in [diesem Microsoft-Artikel](#).

Bekannte Probleme und Workarounds

Unter Red Hat 8.3 und 7.9 kann das PAM (Pluggable Authentication Module) `pam_loginuid.so` nach der AAD-Benutzerauthentifizierung `loginuid` nicht festlegen. Dieses Problem hindert AAD-Benutzer am Zugriff auf VDA-Sitzungen.

Kommentieren Sie in `/etc/pam.d/remote` die Zeile `Session required pam_loginuid.so` aus, um das Problem zu umgehen. Der folgende Screenshot enthält ein Beispiel.

```
##PAM-1.0
auth    substack    password-auth
auth    include     postlogin
account required    pam_nologin.so
account include     password-auth
password include     password-auth
# pam_selinux.so close should be the first session rule
session required     pam_selinux.so close
#session required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session required     pam_selinux.so open
session required     pam_namespace.so
session optional     pam_keyinit.so force revoke
session include     password-auth
session include     postlogin
```

Schritt 1: Erstellen einer Vorlagen-VM im Azure-Portal

Erstellen Sie eine Vorlagen-VM und installieren Sie die Azure-Befehlszeilenschnittstelle auf der VM.

1. Erstellen Sie im Azure-Portal eine Vorlagen-VM. Aktivieren Sie auf der Registerkarte **Management** die Option **Login with Azure AD**, bevor Sie auf **Review + create** klicken.

Home > Create a resource >

Create a virtual machine

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center
Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
[Learn more](#)

✓ Your subscription is protected by Azure Security Center standard plan.

Monitoring

Boot diagnostics ☒ Enable with managed storage account (recommended)
☐ Enable with custom storage account
☐ Disable

Enable OS guest diagnostics ☐

Identity

System assigned managed identity ☒
System managed identity must be on to login with Azure AD credentials.
[Learn more](#)

Azure AD

Login with Azure AD ☒
RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. [Learn more](#)

Azure AD login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH certificates. You can use Azure CLI or Cloud Shell from the Azure Portal. [Learn more](#)

Auto-shutdown

Enable auto-shutdown ☐

Backup

Enable backup ☐

Guest OS updates

Patch orchestration options
Some patch orchestration options are not available for this image. [Learn more](#)

[Review + create](#) < Previous Next : Advanced >

2. Installieren Sie die Azure-Befehlszeilenschnittstelle auf der Vorlagen-VM.
Weitere Informationen finden Sie in [diesem Microsoft-Artikel](#).

Schritt 2: Vorbereiten eines Masterimages auf der Vorlagenmaschine

Um ein Masterimage vorzubereiten, müssen Sie zunächst **Schritt 3: Vorbereiten eines Masterimages** unter [Verwenden von MCS zum Erstellen von Linux-VMs in Azure](#) ausführen.

Schritt 3: Festlegen der Vorlagen-VM als nicht-domänengebunden

Nachdem Sie ein Masterimage erstellt haben, führen Sie die folgenden Schritte aus, um die VM als nicht-domänengebunden zu definieren:

1. Führen Sie das folgende Skript an der Eingabeaufforderung aus.

```
1 Modify /var/xdl/mcs/mcs_util.sh
2 <!--NeedCopy-->
```

2. Suchen Sie nach `function read_non_domain_joined_info()`, und ändern Sie den Wert für `NonDomainJoined` in 2. Der folgende Codeblock ist ein Beispiel.

```
1 function read_non_domain_joined_info()
2 {
3
4 log "Debug: Enter read_non_domain_joined_info"
5 # check if websocket enabled
6 TrustIdentity=`cat ${
7 id_disk_mnt_point }
8 ${
9 ad_info_file_path }
10 | grep '[TrustIdentity]' | sed 's/\s//g'`
11 if [ "$TrustIdentity" == "[TrustIdentity]" ]; then
12 NonDomainJoined=2
13 fi
14 ...
15 }
16
17 <!--NeedCopy-->
```

3. Speichern Sie die Änderung.
4. Fahren Sie die Vorlagen-VM herunter.

Schritt 4: Erstellen der Linux-VMs aus der Vorlagen-VM

Nach dem Vorbereiten der nicht-domänengebundenen Vorlagen-VM führen Sie die folgenden Schritte aus, um VMs zu erstellen:

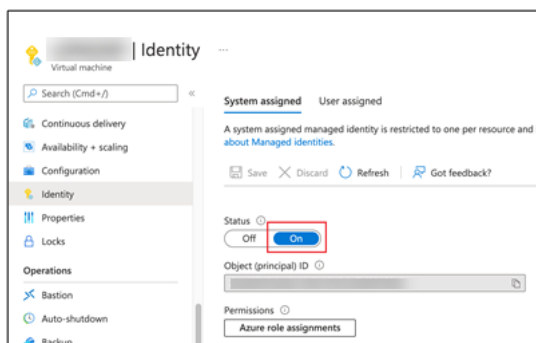
1. Melden Sie sich bei Citrix Cloud an.
2. Doppelklicken Sie auf Citrix DaaS, und greifen Sie auf die Verwaltungskonsole “Vollständige Konfiguration” zu.
3. Wählen Sie unter **Maschinenkataloge** die Verwendung von MCS (Maschinenerstellungsdiensten) zum Erstellen der Linux-VMs aus der Vorlagen-VM aus. Weitere Informationen finden Sie unter [Nicht in Domänen eingebundene VDAs](#) im Citrix DaaS-Dokument.

Schritt 5: Zuweisen von AAD-Benutzerkonten zu den Linux-VMs

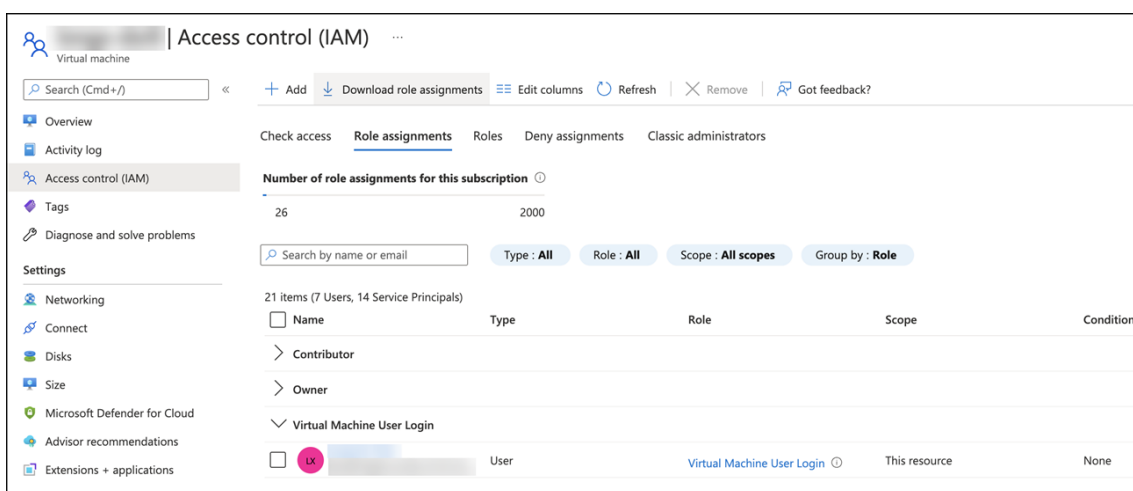
Nachdem Sie die nicht in Domänen eingebundenen VMs erstellt haben, weisen Sie ihnen AAD-Benutzerkonten zu.

Gehen Sie folgendermaßen vor, um einer VM AAD-Benutzerkonten zuzuweisen:

1. Greifen Sie mit einem Administratorkonto auf die VM zu.
2. Aktivieren Sie auf der Registerkarte **Identify > System assigned** die Option **System Identity**.



3. Suchen Sie auf der **Registerkarte Access control (IAM) > Role assignments** den Bereich **Virtual Machine User Login** und fügen Sie die AAD-Benutzerkonten nach Bedarf hinzu.

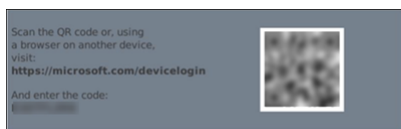


Anmeldung bei nicht-domänengebundenen VDAs

Endbenutzer in Ihrer Organisation haben zwei Möglichkeiten, sich bei einem nicht-domänengebundenen VDA anzumelden. Hier ist eine detaillierte Schrittfolge:

1. Starten Sie die Workspace-App und melden Sie sich am Workspace an, indem Sie den AAD-Benutzernamen und das zugehörige Kennwort eingeben. Die Workspace-Seite wird angezeigt.
2. Doppelklicken Sie auf einen nicht-domänengebundenen Desktop. Die Anmeldeseite von AAD wird angezeigt.

Die Seite variiert je nach festgelegtem Anmeldemodus auf dem VDA: “Device Code” oder “AAD account/password”. Standardmäßig erfolgt die Authentifizierung von AAD-Benutzern auf Linux-VDAs über den Anmeldemodus “Device Code”. Als Administrator können Sie den Anmeldemodus bei Bedarf in “AAD account/password” ändern. Die dafür erforderliche Schrittfolge ist im folgenden Abschnitt beschrieben.



3. Melden Sie sich je nach Anweisung auf dem Bildschirm mit einem der folgenden Verfahren an der Desktopsitzung an:

- Scannen Sie den QR-Code und geben Sie den Code ein.
- Geben Sie den AAD-Benutzernamen und das zugehörige Kennwort ein.

Ändern des Anmeldemodus in “AAD account/password”

Standardmäßig werden AAD-Benutzer auf Linux-VDA mit Gerätecodes authentifiziert. Weitere Informationen finden Sie in diesem [Microsoft-Artikel](#). Führen Sie folgende Schritte aus, um den Anmeldemodus in *AAD account/password* zu ändern:

Führen Sie folgenden Befehl auf dem VDA aus, suchen Sie den Schlüssel `AADAcctPwdAuthEnable`, und ändern Sie den Wert in `0x00000001`.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
  Services\CitrixBrokerAgent\WebSocket" -t "REG_DWORD" -v "
  AADAcctPwdAuthEnable" -d "0x00000001" --force
2
3 <!--NeedCopy-->
```

Hinweis:

Dieser Ansatz funktioniert nicht für Microsoft-Konten oder Konten mit aktivierter zweistufiger Authentifizierung.

Single-Sign-On-Authentifizierung per Double-Hop

October 5, 2022

Die Benutzerdaten für den Zugriff auf einen StoreFront-Store können in das AuthManager-Modul der Citrix Workspace-App für Linux und Citrix Receiver für Linux 13.10 eingefügt werden. Sie können nach der Injektion den Client verwenden, um auf virtuelle Desktops und Anwendungen innerhalb einer Sitzung mit einem virtuellen Linux-Desktop zuzugreifen, ohne ein zweites Mal Benutzeranmeldinformationen einzugeben.

Hinweis:

Dieses Feature wird von der Citrix Workspace-App für Linux und Citrix Receiver für Linux 13.10 unterstützt.

Aktivieren des Features:

1. Installieren Sie auf dem Linux VDA die Citrix Workspace-App für Linux oder Citrix Receiver für Linux 13.10.

Laden Sie die App von der [Citrix Downloadseite](#) für Citrix Workspace oder für Citrix Receiver herunter.

Der Standardinstallationspfad ist /opt/Citrix/ICAClient/. Wenn Sie die App an einem anderen Pfad installieren, legen Sie die Umgebungsvariable ICAROOT fest, sodass sie auf den tatsächlichen Installationspfad verweist.

2. Fügen Sie in der Citrix StoreFront-Verwaltungskonsole die **HTTP Basic**-Authentifizierungsmethode für den Zielstore hinzu.

Manage Authentication Methods - two

Select the methods which users will use to authenticate and access resources. i

	Method	Settings
<input checked="" type="checkbox"/>	User name and password i	⚙️ ▼
<input type="checkbox"/>	SAML Authentication	⚙️ ▼
<input type="checkbox"/>	Domain pass-through <small>Can be enabled / disabled separately on Receiver for Web sites</small>	
<input type="checkbox"/>	Smart card <small>Can be enabled / disabled separately on Receiver for Web sites</small>	
<input checked="" type="checkbox"/>	HTTP Basic	
<input type="checkbox"/>	Pass-through from NetScaler Gateway	⚙️ ▼

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options. Advanced ▼

OK Cancel

3. Fügen Sie der AuthManager-Konfigurationsdatei (\$ICAROOT/config/AuthManConfig.xml) den folgenden Schlüssel hinzu, um die HTTP Basic-Authentifizierung zuzulassen:

```
1 <Protocols>
2   <HTTPBasic>
3     <Enabled>True</Enabled>
4   </HTTPBasic>
5 </Protocols>
6 <!--NeedCopy-->
```

4. Führen Sie die folgenden Befehle aus, um das Stammzertifikat im angegebenen Verzeichnis zu installieren.

```
1 cp rootcert.pem $ICAROOT/keystore/cacerts/
2 $ICAROOT/util/ctx_rehash $ICAROOT/keystore/cacerts/
3 <!--NeedCopy-->
```

5. Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

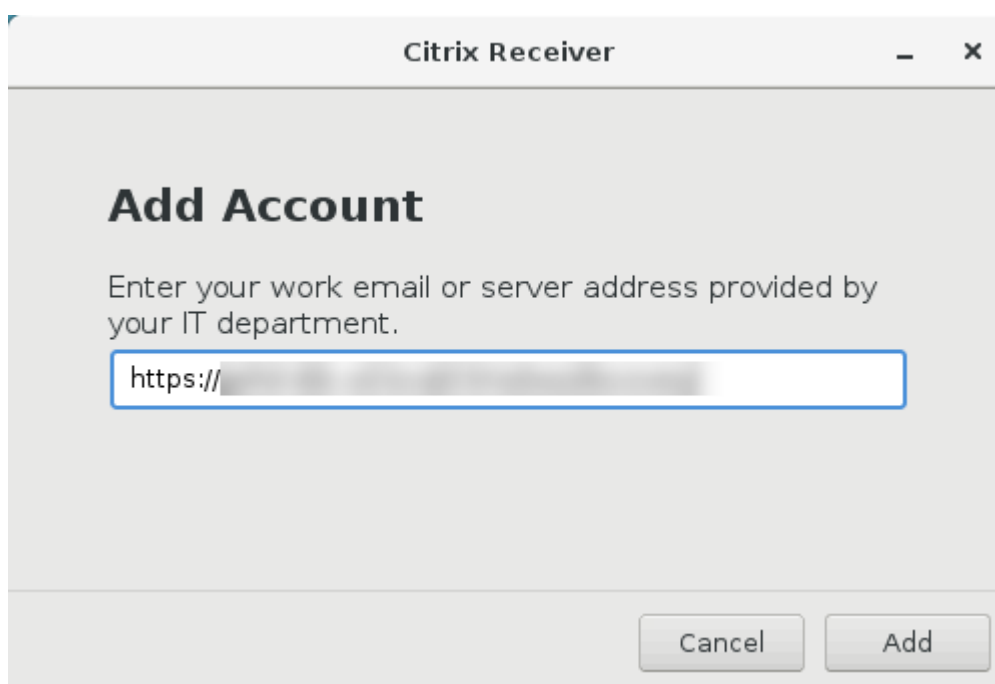
```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
   x00000001"
2 <!--NeedCopy-->
```

6. Starten Sie eine virtuelle Linux-Desktopsitzung und starten Sie die Citrix Workspace-App für Linux oder Citrix Receiver für Linux 13.10 innerhalb dieser Sitzung.

Beim ersten Start der Citrix Workspace-App werden Sie aufgefordert, ein Store-Konto anzugeben. Später werden Sie automatisch bei dem zuvor angegebenen Store angemeldet.

Hinweis:

Geben Sie eine HTTPS-URL als Storekonto an.



Verbundauthentifizierungsdienst

February 9, 2024

Mit dem Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) können Sie Benutzer authentifizieren, die sich bei einem Linux VDA anmelden. Der Linux VDA verwendet dieselbe Windows-Umgebung wie der Windows VDA für das FAS-Anmeldefeature. Informationen zur Konfiguration der Windows-Umgebung für FAS finden Sie unter [Verbundauthentifizierungsdienst](#). Dieser Artikel enthält zusätzliche Informationen speziell für den Linux VDA.

Hinweis:

- Der Linux VDA bietet keine Unterstützung für die Richtlinie **In-session Behavior**.
- Der Linux VDA verwendet kurze Verbindungen, um Daten an FAS-Server zu übertragen.
- Ab Release 2206 können Sie den FAS-Port auf dem Linux VDA über CTX_XDL_FAS_LIST in der Datei ctxsetup.sh anpassen. Weitere Informationen finden Sie im Linux VDA-Installationsartikel zur Ihrer Distribution.

Konfigurieren des FAS auf dem Linux VDA

FAS-Unterstützung unter RHEL 8

FAS ist abhängig von dem Modul pam_krb5, das unter RHEL 8 veraltet ist. Zur Verwendung von FAS unter RHEL 8 erstellen Sie das Modul pam_krb5 wie folgt:

1. Laden Sie den Quellcode pam_krb5-2.4.8-6 von der folgenden Website herunter:

https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.

2. Erstellen und installieren Sie das Modul pam_krb5 unter RHEL 8.

```
1 yum install make gcc krb5-devel pam-devel autoconf libtool
2 rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
3 tar xvfz pam_krb5-2.4.8.tar.gz
4 cd pam_krb5-2.4.8
5 ./configure --prefix=/usr
6 make
7 make install
8 <!--NeedCopy-->
```

3. Überprüfen Sie, ob pam_krb5.so unter /usr/lib64/security/ vorliegt.

```
1 ls -l /usr/lib64/security | grep pam_krb5
2 <!--NeedCopy-->
```

Einrichten von FAS-Servern

Um FAS bei einer Neuinstallation von Linux VDA zu verwenden, geben Sie den FQDN jedes FAS-Servers ein, wenn Sie `ctxinstall.sh` oder `ctxsetup.sh` ausführen. Da der Linux VDA die AD-Gruppenrichtlinie nicht unterstützt, geben Sie stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern an. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen.

Zum Aktualisieren einer vorhandenen Linux VDA-Installation können Sie `ctxsetup.sh` erneut ausführen, um die FAS-Server einzurichten. Sie können die FAS-Server auch über die folgenden Befehle einrichten. Starten Sie anschließend den `ctxvda`-Dienst neu, um die Einstellung zu übernehmen.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ"
   -v "Addresses" -d "<Your-FAS-Server-List>" --force
2
3 service ctxjproxy restart
4
5 service ctxvda restart
6 <!--NeedCopy-->
```

Um die FAS-Server über `ctxreg` zu aktualisieren, führen Sie die folgenden Befehle aus:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
   VirtualDesktopAgent\Authentication\UserCredentialService" -v "
   Addresses" -d "<Your-FAS-Server-List>"
2
3 service ctxjproxy restart
4
5 service ctxvda restart
6 <!--NeedCopy-->
```

Installieren von Zertifikaten

Für die Überprüfung von Benutzerzertifikaten installieren Sie das Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate auf dem VDA. Beispiel: Zum Installieren des Stammzertifizierungsstellenzertifikats rufen Sie das AD-Stammzertifikat aus dem vorherigen Schritt **Abrufen des ZS-Zertifikats von der Microsoft-Zertifizierungsstelle (in AD)** ab oder laden Sie es im DER-Format vom Stammzertifizierungsstellenserver <http://CA-SERVER/certsrv> herunter.

Hinweis:

Die folgenden Befehle gelten auch für die Konfiguration eines Zwischenzertifikats.

Mit diesem oder einem ähnlichen Befehl können Sie eine DER-Datei (.crt, .cer, .der) in PEM konvertieren.

```
1 sudo openssl x509 -inform der -in root.cer -out root.pem
2 <!--NeedCopy-->
```

Anschließend installieren Sie mit diesem oder einem ähnlichen Befehl das Stammzertifizierungsstellenzertifikat im Verzeichnis `openssl`:

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

Hinweis:

Speichern Sie das Stammzertifizierungsstellenzertifikat nicht im Verzeichnis `/root`. Andernfalls besitzt FAS keine Leseberechtigung für das Stammzertifizierungsstellenzertifikat.

Ausführen von `ctxfascfg.sh`

Führen Sie das Skript `ctxfascfg.sh` aus, um FAS zu konfigurieren:

```
1 sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
2 <!--NeedCopy-->
```

Es werden Umgebungsvariablen hinzugefügt, damit `ctxfascfg.sh` im stillen Modus ausgeführt werden kann:

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis:** Die Active Directory-Integrationsmethode; das entspricht `CTX_EASYINSTALL_ADINTEGRATIONWAY`, wenn `CTX_EASYINSTALL_ADINTEGRATIONWAY` angegeben wurde. Wenn `CTX_EASYINSTALL_ADINTEGRATIONWAY` nicht angegeben ist, verwendet `CTX_FAS_ADINTEGRATIONWAY` die eigene Werteinstellung.
- **CTX_FAS_CERT_PATH =<certificate path>:** Gibt den vollständigen Pfad an, in dem Stammzertifikate und alle Zwischenzertifikate gespeichert werden.
- **CTX_FAS_KDC_HOSTNAME:** Gibt den Hostnamen des Schlüsselverteilungscenters (KDC) an, wenn Sie PBIS auswählen.
- **CTX_FAS_PKINIT_KDC_HOSTNAME:** Gibt den Hostnamen des PKINIT KDC an, der `CTX_FAS_KDC_HOSTNAME` ist, sofern nicht anders angegeben.

Wählen Sie die korrekte Active Directory-Integrationsmethode aus und geben Sie den korrekten Pfad zu den Zertifikaten ein (z. B. `/etc/pki/CA/certs/`).

Das Skript installiert die Pakete `krb5-pkinit` und `pam_krb5` und legt die relevanten Konfigurationsdateien fest.

Einschränkung

- FAS unterstützt eingeschränkte Linux-Plattformen und AD-Integrationsmethoden. Siehe folgende Tabelle:

	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	Ja	Ja	Ja	Ja
Debian 11.3, Debian 10.9	Ja	Nein	Nein	Nein
RHEL 8.4	Ja	Ja	Ja	Ja
RHEL 8.2	Ja	Ja	Ja	Ja
RHEL 7.9/CentOS 7.9	Ja	Ja	Ja	Ja
SLES 15.3	Ja	Nein	Ja	Nein
SLES 15.2	Ja	Nein	Ja	Nein
Ubuntu 20.04	Ja	Nein	Ja	Nein
Ubuntu 18.04	Ja	Nein	Ja	Nein

- FAS unterstützt den Sperrbildschirm noch nicht. Wenn Sie in einer Sitzung auf die Sperrschaltfläche klicken, können Sie sich mit FAS nicht erneut bei der Sitzung anmelden.
- Der Artikel [Übersicht über die Architekturen des Verbundauthentifizierungsdiensts](#) enthält eine Übersicht über die gebräuchlichen FAS-Architekturen, die in dieser Version unterstützt werden. Das **Einbinden über Azure AD mit Windows 10** ist nicht möglich.

Problembehandlung

Stellen Sie vor einer Problembehandlung des Verbundauthentifizierungsdiensts (FAS) sicher, dass der Linux VDA ordnungsgemäß installiert und konfiguriert ist und dass Sitzungen ohne FAS-Server erfolgreich im gemeinsamen Store per Kennwortauthentifizierung gestartet werden können.

Wenn Sitzungen ohne FAS-Server fehlerfrei ausgeführt werden, setzen Sie die HDX-Protokollebene der **Login**-Klasse auf VERBOSE und die VDA-Protokollebene auf TRACE. Informationen zum Aktivieren von Protokollen zur Ablaufverfolgung (Tracing) für Linux VDA finden Sie im Knowledge Center-Artikel [CTX220130](#).

Fehler bei der FAS-Serverkonfiguration

Der Start einer Sitzung über den FAS-Store schlägt fehl.

Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie ein Fehlerprotokoll folgender Art:

```
1 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [
    Logon Type] Federated Authentication Logon.
2
3 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas:
    entry
4
5 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start
    connect to server 0
6
7 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0:
    failed to connect: Connection refused.
8
9 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas:
    failed to connect to server [0], please confirm if fas service list
    is well configured in condb
10
11 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit
    , 43
12
13 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user:
    failed to validate fas credential
14
15 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate:
    failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER
16
17 <!--NeedCopy-->
```

Lösung Stellen Sie mit folgendem Befehl sicher, dass der Citrix Registrierungswert “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” auf <Your-FAS-Server-List> festgelegt ist.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
2 <!--NeedCopy-->
```

Wenn die Einstellung falsch ist, legen Sie sie erneut fest, wie weiter oben im Schritt [Einrichten von FAS-Servern](#) beschrieben.

Falsche Konfiguration des Zertifizierungsstellenzertifikats

Der Start einer Sitzung über den FAS-Store schlägt fehl. Ein graues Fenster wird für einige Sekunden angezeigt.



Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie ein Fehlerprotokoll folgender Art:

```
1 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: entry
2
3 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller:
   current process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]
4
5 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: entry
6
7 2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
   for response...
8
9 2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query
   to server success
10
11 2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
   get_public_certificate: exit
12
13 2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
   input size 1888
14
15 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
   output size 1415
16
17 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: get logon certificate success
18
19 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
   cache certificate success
20
21 2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
   get_logon_certificate: exit, 0
22
23 2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
   pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
24 <!--NeedCopy-->
```

Lösung Stellen Sie sicher, dass Sie den vollständigen Pfad, in dem das Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate gespeichert werden, korrekt in `/etc/krb5.conf` festgelegt haben. Der vollständige Pfad ist dem folgenden ähnlich:

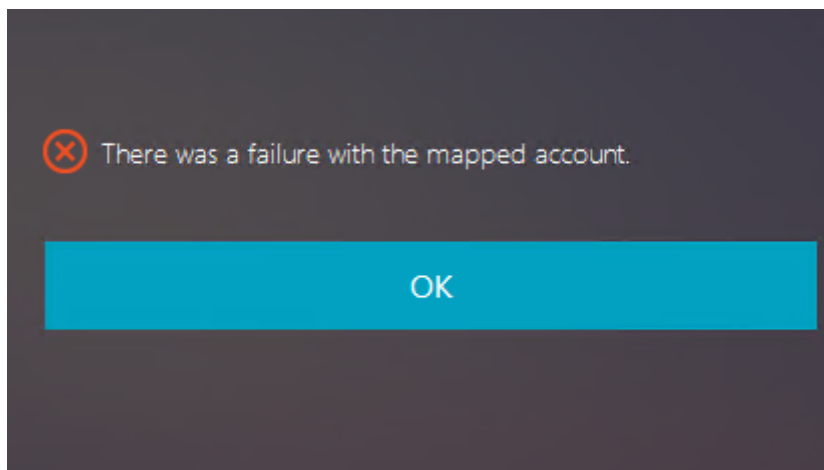
```
1  [realms]
2
3  EXAMPLE.COM = {
4
5
6      .....
7
8      pkinit_anchors = DIR:/etc/pki/CA/certs/
9
10     .....
11 }
12
13
14 <!--NeedCopy-->
```

Wenn die vorhandene Einstellung falsch ist, legen Sie sie erneut fest, wie weiter oben im Schritt [Installieren von Zertifikaten](#) beschrieben.

Überprüfen Sie auch, ob das Stammzertifizierungsstellenzertifikat gültig ist.

Kontozuordnungsfehler bei Spiegelung

FAS ist für die SAML-Authentifizierung konfiguriert. Der folgende Fehler kann auftreten, wenn ein Benutzer der Active Directory-Verbunddienste (AD FS) den Benutzernamen und das Kennwort auf der AD FS-Anmeldeseite eingibt.

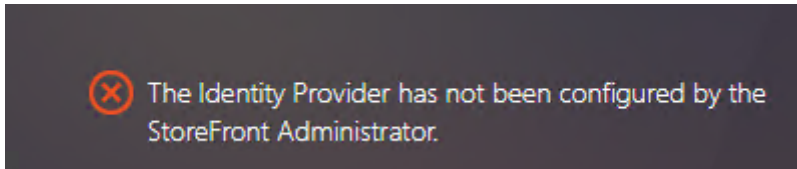


Die Fehlermeldung zeigt an, dass der Benutzer zwar erfolgreich in AD FS verifiziert wurde, aber kein gespiegeltes Konto für den Benutzer in AD konfiguriert ist.

Lösung Richten Sie das gespiegelte Konto in AD ein.

AD FS nicht konfiguriert

Bei einem Anmeldeversuch beim FAS-Store tritt folgender Fehler auf:



Das Problem tritt auf, wenn der FAS-Speicher für die SAML-Authentifizierung konfiguriert ist, aber die AD FS-Bereitstellung fehlt.

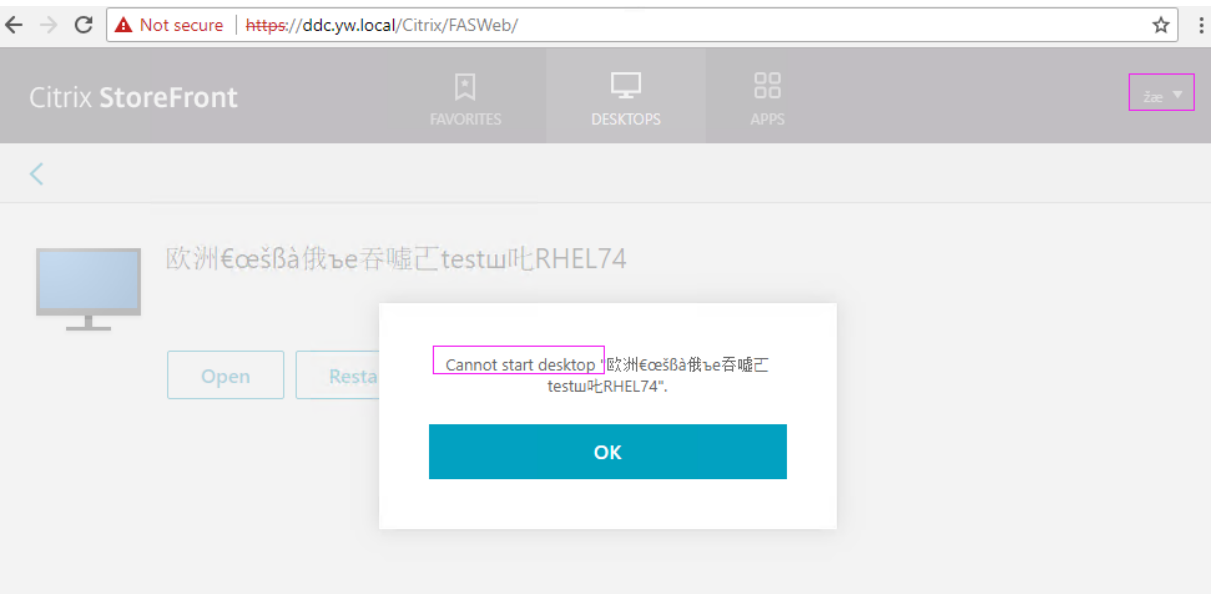
Lösung Stellen Sie den AD FS-Identitätsanbieter für den Verbundauthentifizierungsdienst (FAS) bereit. Weitere Informationen finden Sie unter [AD FS-Bereitstellung des Verbundauthentifizierungsdiensts](#).

Verwandte Informationen

- Der Artikel [Übersicht über die Architekturen des Verbundauthentifizierungsdiensts](#) enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Artikel mit Anleitungen finden Sie unter [Erweiterte Konfiguration des Verbundauthentifizierungsdiensts](#).

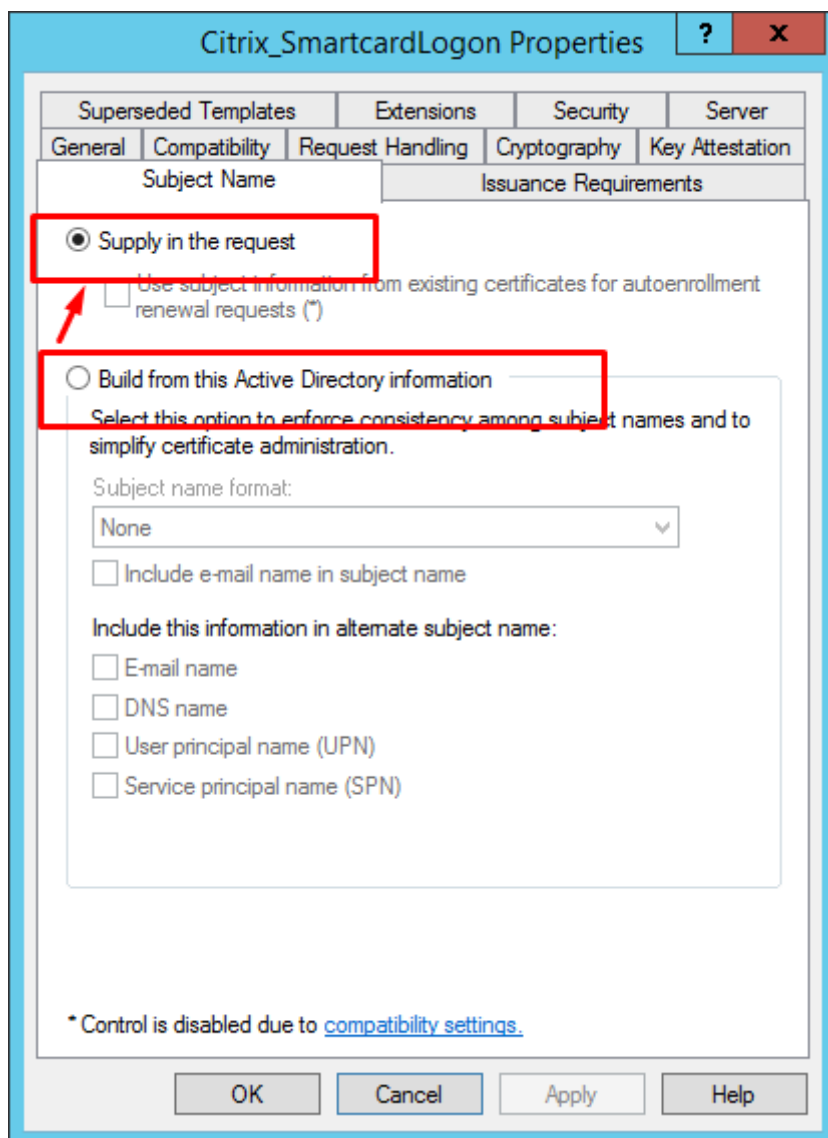
Bekanntes Problem

Beim Einsatz von FAS kann der Start einer veröffentlichten Desktop- oder App-Sitzung mit nicht-englischen Zeichen fehlschlagen.



Workaround

Klicken Sie im ZS-Tool mit der rechten Maustaste auf **Vorlagen verwalten** und ändern Sie die Vorlage für **Citrix_SmartcardLogon** von **Aus diesen Informationen in Active Directory erstellen** in **Informationen werden in der Anforderung angegeben**:



Authentifizierung ohne Single Sign-On

October 5, 2022

Dieser Artikel enthält eine Anleitung zum Aktivieren der Authentifizierung ohne Single Sign-On auf dem Linux VDA.

Übersicht

Standardmäßig ist auf dem Linux VDA Single Sign-On (SSO) aktiviert. Die Benutzer melden sich bei der Citrix Workspace-App und bei VDA-Sitzungen mit einem Satz Anmeldeinformationen an.

Sollen sich Benutzer bei VDA-Sitzungen mit einem anderen Satz Anmeldeinformationen anmelden, deaktivieren Sie SSO auf dem Linux VDA. In der folgenden Tabelle sind Kombinationen von Benutzerauthentifizierungsmethoden aufgeführt, die in Szenarien ohne SSO unterstützt werden.

Citrix Workspace-App	VDA-Sitzung
Benutzername	Benutzername
Smartcard	Benutzername
Benutzername	Smartcard

Unterstützte Distributionen

SSO kann nur für Linux-VDAs deaktiviert werden, die unter einer der folgenden Distributionen installiert sind:

- RHEL 8.4
- RHEL 7.9/CentOS 7.9
- Debian 10.9
- SUSE 15.3
- SUSE 15.2

Deaktivieren von SSO

Führen Sie den folgenden Befehl auf dem Linux VDA aus:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\  
   Control\Citrix\WinStations\tcp" -t "REG_DWORD" -v "  
   fPromptForDifferentUser" -d "0x00000001" --force  
2 <!--NeedCopy-->
```

Smartcards

October 24, 2022

Sie können eine mit dem Clientgerät verbundene Smartcard zur Anmeldung an einer virtuellen Linux-Desktopsitzung verwenden. Dieses Feature wurde in Form der Smartcardumleitung über den virtuellen ICA-Smartcardkanal implementiert. Sie können die Smartcard auch innerhalb der Sitzung verwenden. Anwendungsfälle umfassen das Hinzufügen einer digitalen Signatur zu einem Dokument, das Verschlüsseln oder Entschlüsseln einer E-Mail und die Authentifizierung bei einer Website.

Auf dem Linux VDA wird hierfür die gleiche Konfiguration wie auf dem Windows VDA verwendet. Weitere Informationen finden Sie unter [Konfigurieren der Smartcardumgebung](#) in diesem Artikel.

Hinweis:

Die Verwendung einer zugeordneten Smartcard in einer Linux VDA-Sitzung zur Anmeldung bei Citrix Gateway wird nicht unterstützt.

Voraussetzungen

Die Passthrough-Authentifizierung mit Smartcard erfordert die Erfüllung folgender Voraussetzungen:

- Der Linux VDA ist unter einer der folgenden Distributionen installiert:
 - RHEL 8
 - RHEL 7/CentOS 7
 - Ubuntu 20.04
 - Ubuntu 18.04
 - Debian 11.3
 - Debian 10.9

Stellen Sie nach Abschluss der VDA-Installation sicher, dass sich der VDA beim Delivery Controller registrieren kann und Sie die veröffentlichten Linux-Desktopsitzungen mit Windows-Anmeldeinformationen öffnen können.

- Es werden von OpenSC unterstützte Smartcards verwendet. Weitere Informationen finden Sie unter [Überprüfen der Kompatibilität der verwendeten Smartcards mit OpenSC](#).
- Citrix Workspace-App für Windows wird verwendet.

Überprüfen der Kompatibilität der verwendeten Smartcards mit OpenSC

OpenSC ist ein gebräuchlicher Treiber für Smartcards unter RHEL 7.4+. Als voll kompatibler Ersatz von CoolKey unterstützt OpenSC viele Arten von Smartcards (siehe [Smart Card Support in Red Hat Enterprise Linux](#)).

In diesem Artikel dient die YubiKey 4-Smartcard als Beispiel zur Veranschaulichung der Konfiguration. YubiKey 4 ist ein im Handel erhältliches und PIV-konformes USB-Gerät mit CCID-Funktion. YubiKey 4 wird vom OpenSC-Treiber unterstützt.



Wenn in Ihrer Organisation eine anspruchsvollere Smartcard benötigt wird, stellen Sie eine physische Maschine mit einer unterstützten Linux-Distribution und installiertem OpenSC-Paket bereit. Informationen zur Installation von OpenSC finden Sie unter [Installieren des Smartcardtreibers](#). Führen Sie die Smartcard ein und prüfen Sie mit folgendem Befehl, ob OpenSC Ihre Smartcard unterstützt:

```
1 pkcs11-tool --module opensc-pkcs11.so --list-slots
2 <!--NeedCopy-->
```

Konfiguration

Vorbereiten eines Stammzertifikats

Ein Stammzertifikat wird zur Überprüfung des Zertifikats auf der Smartcard verwendet. Führen Sie die folgenden Schritte aus, um ein Stammzertifikat herunterzuladen und zu installieren:

1. Rufen Sie (normalerweise von einem Zertifizierungsstellenserver) ein Stammzertifikat im PEM-Format ab.

Sie können eine DER-Datei (*.crt, *.cer, *.der) mithilfe des folgenden Befehls in PEM konvertieren. In dem Beispiel heißt die DER-Datei **certnew.cer**.

```
1 openssl x509 -inform der -in certnew.cer -out certnew.pem
2 <!--NeedCopy-->
```

2. Installieren Sie das Stammzertifikat im Verzeichnis `openssl`. Die Datei **certnew.pem** gilt hier als Beispiel.

```
1 cp certnew.pem <path where you install the root certificate>
2 <!--NeedCopy-->
```


Um einen Pfad für die Installation des Stammzertifikats zu erstellen, führen Sie `sudo mkdir -p <path where you install the root certificate>` aus.

Erstellen des Moduls pam_krb5 unter RHEL 8

Die Smartcardauthentifizierung ist abhängig vom Modul pam_krb5, das unter RHEL 8 veraltet ist. Zur Verwendung der Smartcardauthentifizierung unter RHEL 8 erstellen Sie das Modul pam_krb5 wie folgt:

1. Laden Sie den pam_krb5-2.4.8-6-Quellcode von https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html herunter.
2. Erstellen und installieren Sie das Modul pam_krb5 unter RHEL 8.

```
1 yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-  
  tools  
2 yum install gcc krb5-devel pam-devel autoconf libtool  
3 rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div  
4 tar xvfz pam_krb5-2.4.8.tar.gz  
5 cd pam_krb5-2.4.8  
6 ./configure --prefix=/usr  
7 make  
8 make install  
9 <!--NeedCopy-->
```

3. Überprüfen Sie, ob pam_krb5.so unter /usr/lib64/security/ vorliegt.

```
1 ls -l /usr/lib64/security | grep pam_krb5  
2 <!--NeedCopy-->
```

Konfigurieren der Smartcardumgebung

Sie können die Smartcardumgebung mit dem Skript ctxsmartlogon.sh oder auch manuell konfigurieren.

(Option 1) Konfigurieren der Smartcardumgebung mit dem Skript ctxsmartlogon.sh

Hinweis:

Das Skript ctxsmartlogon.sh fügt PKINIT-Informationen zum Standardbereich hinzu. Sie können diese Einstellung über die Konfigurationsdatei **/etc/krb5.conf** ändern.

Vor der ersten Verwendung von Smartcards konfigurieren Sie die Smartcardumgebung mit dem Skript ctxsmartlogon.sh.

Tipp:

Wenn Sie SSSD zum Domänenbeitritt verwendet haben, starten Sie den SSSD-Dienst nach dem Ausführen von `ctxsmartlogon.sh` neu.

```
1 sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
2 <!--NeedCopy-->
```

Die Ergebnisse ähneln der folgenden Anzeige:

```
#####
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#####
Step 1:Enable smart card logon.
Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
Please select which Active Directory integration method to use:
1: Winbind
2: SSSD
3: Centrify
Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
Installing, please wait...
[krb5-pkinit][pam_krb5] already installed.
[pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
Packages installed. [Success]
Step 4:Configure krb5.conf.
Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
/etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
/etc/pam.d/ctxfsc configure successfully.
/etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

Sie können Smartcards auch deaktivieren, indem Sie das Skript `ctxsmartlogon.sh` ausführen:

```
1 sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
2 <!--NeedCopy-->
```

Die Ergebnisse ähneln der folgenden Anzeige:

```
#####
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#####
Step 1:Enable smart card logon.
Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.
```

(Option 2) Manuelles Konfigurieren der Smartcardumgebung Auf dem Linux VDA wird dieselbe Smartcardumgebung verwendet wie auf dem Windows VDA. In der Umgebung müssen mehrere Kom-

ponenten konfiguriert werden: Domänencontroller, Microsoft-Zertifizierungsstelle, Internetinformationsdienste (IIS), Citrix StoreFront und Citrix Workspace-App. Informationen zur Konfiguration am Beispiel der YubiKey 4-Smartcard finden Sie im Knowledge Center-Artikel [CTX206156](#).

Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie sicher, dass Sie alle Komponenten ordnungsgemäß konfiguriert und den privaten Schlüssel und das Benutzerzertifikat auf die Smartcard heruntergeladen haben und dass Sie sich mit der Smartcard bei einem Windows VDA anmelden können.

Installieren der PC/SC Lite-Pakete PC/SC Lite ist eine Implementierung der PC/SC-Spezifikation (Personal Computer/Smartcard) unter Linux. Sie bietet eine Windows-Smartcardschnittstelle zur Kommunikation mit Smartcards und Lesegeräten. Die Smartcardumleitung des Linux VDAs ist auf PC/SC-Ebene implementiert.

Führen Sie den folgenden Befehl aus, um die PC/SC Lite-Pakete zu installieren:

RHEL 7/CentOS 7, RHEL 8:

```
1 yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
2 <!--NeedCopy-->
```

Ubuntu 20.04, Ubuntu 18.04, Debian 11.3, Debian 10.9:

```
1 apt-get install -y libpcsclite1 libccid
2 <!--NeedCopy-->
```

Installieren des Smartcardtreibers OpenSC ist ein gebräuchlicher Treiber für Smartcards. Wenn OpenSC nicht installiert ist, führen Sie den folgenden Befehl aus, um es zu installieren:

RHEL 7/CentOS 7, RHEL 8:

```
1 yum install opensc
2 <!--NeedCopy-->
```

Ubuntu 20.04, Ubuntu 18.04, Debian 11.3, Debian 10.9:

```
1 apt-get install -y opensc
2 <!--NeedCopy-->
```

Installieren der PAM-Module für die Authentifizierung per Smartcard Führen Sie den folgenden Befehl aus, um die Module pam_krb5 und krb5-pkinit zu installieren:

RHEL 7/CentOS 7:

```
1 yum install pam_krb5 krb5-pkinit
2 <!--NeedCopy-->
```

RHEL 8:

```
1 yum install krb5-pkinit
2 <!--NeedCopy-->
```

Ubuntu 20.04, Ubuntu 18.04:

```
1 apt-get install libpam-krb5 krb5-pkinit
2 <!--NeedCopy-->
```

Debian 11.3, Debian 10.9:

```
1 apt-get install -y libpam-krb5 krb5-pkinit
2 <!--NeedCopy-->
```

pam_krb5 ist ein austauschbares Authentifizierungsmodul, mit dem PAM-fähige Anwendungen Kennwörter prüfen und Ticket Granting Tickets vom Schlüsselverteilungscenter (KDC) abrufen können. krb5-pkinit enthält das PKINIT-Plug-In, mit dem Clients mit einem privaten Schlüssel und einem Zertifikat Anfangsanmeldeinformationen vom KDC abrufen können.

Konfigurieren des pam_krb5-Moduls Das pam_krb5-Modul interagiert mit dem KDC zum Abrufen von Kerberos-Tickets über Zertifikate auf Smartcards. Führen Sie den folgenden Befehl aus, um die pam_krb5-Authentifizierung in PAM zu aktivieren:

```
1 authconfig --enablekrb5 --update
2 <!--NeedCopy-->
```

Fügen Sie der Konfigurationsdatei **/etc/krb5.conf** PKINIT-Informationen entsprechend dem tatsächlichen Bereich hinzu:

Hinweis:

Die Option **pkinit_cert_match** gibt Übereinstimmungsregeln an, die das Clientzertifikat erfüllen muss, damit es zum Versuch der PKINIT-Authentifizierung verwendet wird. Die Syntax der Übereinstimmungsregeln ist:

[relation-operator] component-rule ...

wobei **relation-operator** entweder **&&** (= alle Komponentenregeln müssen erfüllt werden) sein kann oder **||** (nur eine Komponentenregel muss erfüllt werden).

Beispiel für eine generische krb5.conf-Datei:

```
1 EXAMPLE.COM = {
2
3
4     kdc = KDC.EXAMPLE.COM
5
6     auth_to_local = RULE:[1:$1@$0]
```

```
7
8     pkinit_anchors = FILE:<path where you install the root certificate
9                       >/certnew.pem
10
11     pkinit_kdc_hostname = KDC.EXAMPLE.COM
12
13     pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
14
15     pkinit_eku_checking = kpServerAuth
16 }
17
18 <!--NeedCopy-->
```

Die Konfigurationsdatei sieht in etwa folgendermaßen aus, nachdem Sie die PKINIT-Informationen hinzugefügt haben:

```
CTXDEV.LOCAL = {
    kdc = ctx-ad.ctxdev.local
    auth_to_local = RULE:[1:$1@$0]
    pkinit_kdc_hostname = ctx-ad.ctxdev.local
    pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
    pkinit_eku_checking = kpServerAuth
    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
}
```

Konfigurieren der PAM-Authentifizierung PAM-Konfigurationsdateien bestimmen, welche Module für die PAM-Authentifizierung verwendet werden. Um pam_krb5 als Authentifizierungsmodul hinzuzufügen, fügen Sie der Datei **/etc/pam.d/smartcard-auth** folgende Zeile hinzu :

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options
=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.
so
```

Die Konfigurationsdatei sieht in etwa folgendermaßen aus, nachdem Sie sie geändert haben, wenn SSSD verwendet wird:

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done  ignore=ignore default=die] pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account      required      pam_unix.so
account      sufficient    pam_localuser.so
account      sufficient    pam_succeed_if.so uid < 1000 quiet
account      [default=bad  success=ok user_unknown=ignore] pam_sss.so
account      [default=bad  success=ok auth_err=ignore user_unknown=ignore ignore=ignore] pam_krb5.so
account      required      pam_permit.so

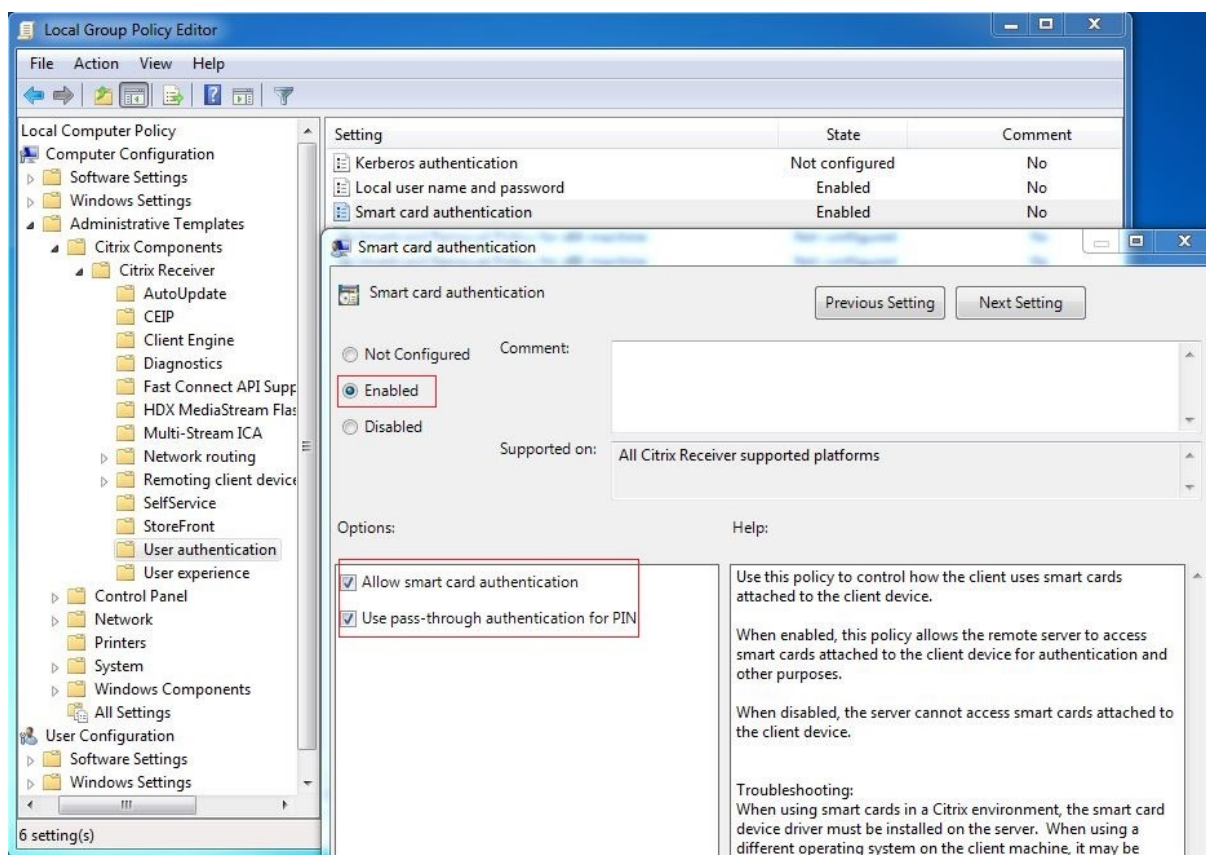
session      optional     pam_keyinit.so revoke
session      required      pam_limits.so
-session     optional     pam_systemd.so
#session     optional     pam_oddjob_mkhomedir.so umask=0077
session      optional     pam_mkhomedir.so umask=0077
session      [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session      required      pam_unix.so
session      optional     pam_sss.so
session      optional     pam_krb5.so

```

Optional: Single Sign-On per Smartcard

Single Sign-On ist ein Citrix Feature, mit dem die Passthrough-Authentifizierung in Starts von virtuellen Desktops und Anwendungen implementiert wird. Dadurch müssen Benutzer ihre PIN seltener eingeben. Konfigurieren Sie die Citrix Workspace-App, um SSO mit dem Linux VDA zu verwenden. Die Konfiguration ist die gleiche wie für den Windows-VDA. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX133982](#).

Aktivieren Sie die Smartcardauthentifizierung wie nachfolgend beschrieben, wenn Sie die Gruppenrichtlinie in der Citrix Workspace-App konfigurieren.



Anmeldung mit Schneller Smartcard

Das Schnelle-Smartcard-Feature ist eine Verbesserung gegenüber der alten HDX PC/SC-basierten Smartcardumleitung. Das Feature verbessert die Leistung, wenn Smartcards in WANs mit hoher Latenz verwendet werden. Weitere Informationen finden Sie unter [Smartcards](#).

Der Linux VDA unterstützt Schnelle Smartcards auf folgenden Versionen der Citrix Workspace-App:

- Citrix Receiver für Windows 4.12
- Citrix Workspace-App 1808 für Windows und höher

Aktivieren der Anmeldung mit Schneller Smartcard auf dem Client Die Anmeldung mit Schneller Smartcard ist standardmäßig auf dem VDA aktiviert und auf dem Client deaktiviert. Zum Aktivieren des Features auf dem Client fügen Sie folgenden Parameter in die Datei default.ica der zugehörigen StoreFront-Site ein:

```
1 [WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

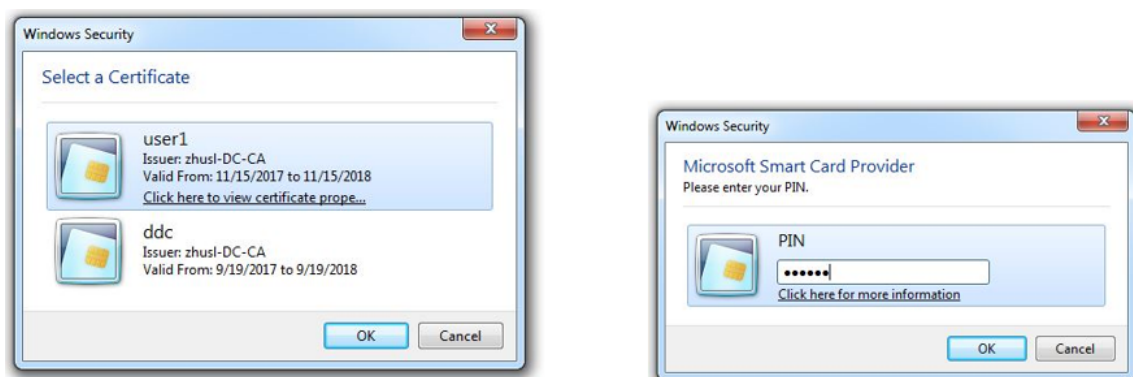
Deaktivieren der Anmeldung mit Schneller Smartcard auf dem Client Um die Anmeldung mit Schneller Smartcard auf dem Client zu deaktivieren, entfernen Sie den Parameter **SmartCardCryptographicRedirection** aus der Datei default.ica der zugehörigen StoreFront-Website.

Verwendung

Anmelden am Linux VDA mit einer Smartcard

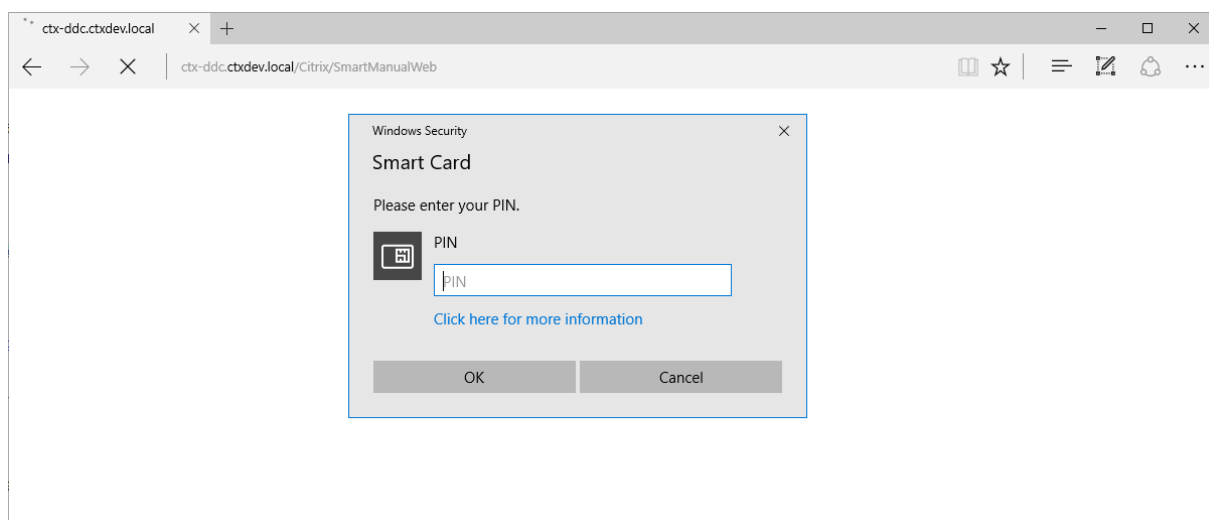
Sie können sich per Smartcard am Linux VDA in Szenarien mit und ohne Single Sign-On anmelden.

- Bei Verwendung von Single Sign-On werden Sie automatisch mit dem zwischengespeicherten Smartcardzertifikat und der PIN bei StoreFront angemeldet. Wenn Sie eine virtuelle Linux-Desktopsitzung in StoreFront starten, wird die PIN an den Linux VDA zur Smartcardauthentifizierung weitergeleitet.
- Wird kein Single Sign-On verwendet, werden Sie aufgefordert, ein Zertifikat auszuwählen und eine PIN einzugeben, um sich bei StoreFront anzumelden.



Wenn Sie eine Sitzung mit virtuellem Linux-Desktop in StoreFront starten, wird auf dem Linux VDA das nachfolgende Anmeldedialogfeld angezeigt. Der Benutzername wird aus dem Zertifikat auf der Smartcard extrahiert und Sie müssen die PIN zur Anmeldeauthentifizierung erneut eingeben.

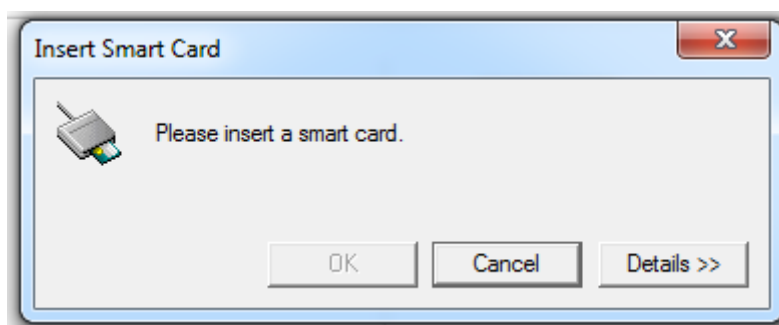
Dieses Verhalten ist mit dem des Windows VDA identisch.



Wiederherstellen der Verbindung mit einer Sitzung per Smartcard

Stellen Sie sicher, dass die Smartcard mit dem Clientgerät verbunden ist, um die Verbindung zu einer Sitzung wiederherzustellen. Andernfalls wird nur kurz ein graues Caching-Fenster auf dem Linux VDA angezeigt, da die erneute Authentifizierung ohne Smartcard fehlschlägt. In diesem Fall wird keine weitere Aufforderung angezeigt, um Sie daran zu erinnern, die Smartcard anzuschließen.

In StoreFront wird bei dem Versuch, eine Verbindung zu einer Sitzung ohne Smartcard wiederherzustellen, eventuell eine Warnmeldung in folgender Form ausgegeben:



Einschränkung

Richtlinie zum Entfernen der Smartcard

Derzeit wird auf dem Linux VDA nur das Standardverhalten für das Entfernen von Smartcards verwendet. Wenn Sie die Smartcard nach der Anmeldung beim Linux VDA entfernen, bleibt die Sitzung weiterhin verbunden und der Sitzungsbildschirm wird nicht gesperrt.

Unterstützung für andere Smartcards und die PKCS#11-Bibliothek

Obwohl nur die OpenSC-Smartcard in unserer Supportliste aufgeführt ist, können Sie versuchen, andere Smartcards und die PKCS#11 -Bibliothek zu verwenden, da Citrix eine generische Umleitungslösung für Smartcards bietet. Wechseln Sie zu Ihrer speziellen Smartcard oder der PKCS #11-Bibliothek:

1. Ersetzen Sie alle Instanzen von `opensc-pkcs11.so` durch Ihre PKCS#11-Bibliothek.
2. Führen Sie den folgenden Befehl aus, um den Pfad Ihrer PKCS#11-Bibliothek in der Registrierung festzulegen:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
   PKCS11LibPath" -d "PATH"
2 <!--NeedCopy-->
```

Wobei **PATH** auf Ihre PKCS#11-Bibliothek verweist, z. B. `/usr/lib64/pkcs11/opensc-pkcs11.so`

3. Deaktivieren Sie die Anmeldung mit Schneller Smartcard auf dem Client.

Nicht authentifizierte Sitzungen mit anonymen Benutzern

September 25, 2023

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 Workspace-App 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 [Citrix Virtual Apps and Desktops-Dokumentation](#).

Festlegen der Leerlaufzeit für nicht authentifizierte Sitzungen

Für nicht authentifizierte Sitzungen gilt ein Standardleerlaufzeit 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 gleichzeitiger 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:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber -d 0
   x00000020
2 <!--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:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet
   \Control\Citrix" -v MaxAnonymousUserNumber
2 <!--NeedCopy-->
```

Prüfen Sie, ob der Dienst **ncsd** ausgeführt wird und die Kennwortzwischenlagerung **passwd** zulässt:

```
1 ps uax | grep nscd
2 cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
3 <!--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:

```
1 [KDE Action Restrictions]
2 action/lock_screen=false
3 <!--NeedCopy-->
```

Wenn der Parameter `KDE Action Restrictions` jedoch in einer globalen `kdeglobals`-Datei wie `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals` als unveränderlich konfiguriert 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 auf der Seite [KDE System Administration/Kiosk/Keys](#).

Datei

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Kopieren und Einfügen von Dateien](#)
- [Dateiübertragung](#)

Kopieren und Einfügen von Dateien

October 5, 2022

Über Kontextmenü oder mit Tastenkombinationen können Benutzer Dateien zwischen einer Sitzung und einem lokalen Client kopieren und einfügen. Für dieses Feature ist Citrix Virtual Apps and Desktops 2006 oder höher und Citrix Workspace-App 1903 oder höher für Windows erforderlich.

Zum Kopieren und Einfügen von Dateien muss Folgendes sichergestellt werden:

- Die Anzahl von Dateien darf 20 nicht überschreiten.
- Die Dateigröße darf 200 MB nicht überschreiten.
- Der Nautilus-Dateimanager ist auf der Maschine verfügbar, auf dem Sie den Linux VDA installiert haben.

Unterstützte Linux-Distributionen

Das **Feature zum Kopieren und Einfügen von Dateien** ist für alle Linux-Distributionen verfügbar, die der Linux VDA unterstützt.

Relevante Richtlinien

Die folgenden Zwischenablagenrichtlinien sind für die Konfiguration des Features relevant. Weitere Informationen zu den Zwischenablagenrichtlinien finden Sie unter [Liste der unterstützten Richtlinien](#).

- Clientzwischenablagenumleitung
- Aktualisierungsmodus für die Zwischenablageauswahl
- Aktualisierungsmodus für die Primärauswahl

Hinweis:

Um die Funktion zum Kopieren und Einfügen von Dateien zu deaktivieren, legen Sie die Richtlinie zur **Clientzwischenablagenumleitung** in Citrix Studio auf **Nicht zugelassen** fest.

Einschränkungen

- Ausschneiden wird nicht unterstützt. Versuche des Ausschneidens einer Datei werden als Kopiervorgang behandelt.
- Drag & Drop wird nicht unterstützt.
- Das Kopieren von Verzeichnissen wird nicht unterstützt.
- Das Kopieren und Einfügen von Dateien muss einzeln ausgeführt werden. Erst wenn eine Datei kopiert und eingefügt wurde, kann die nächste Datei kopiert werden.

Dateiübertragung

October 5, 2022

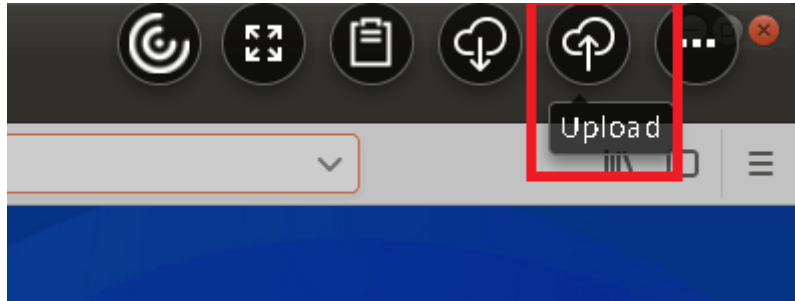
Dateiübertragungen zwischen dem Linux VDA und dem Clientgerät werden unterstützt. Diese Funktion ist verfügbar, wenn auf dem Clientgerät ein Webbrowser ausgeführt wird, der das HTML5-Sandbox-Attribut unterstützt. Das HTML5-Sandbox-Attribut ermöglicht Benutzern den Zugriff auf virtuelle Desktops und Apps mit der Citrix Workspace-App für HTML5 und für Chrome.

Hinweis:

Dateiübertragung ist für die Citrix Workspace-App für HTML5 und Chrome verfügbar.

Innerhalb von Sitzungen mit veröffentlichten Apps bzw. Desktops ermöglicht die Dateiübertragung das Hoch- und Herunterladen von Dateien zwischen Linux VDA und Clientgerät. Um Dateien vom Clientgerät auf den Linux VDA hochzuladen, klicken Sie auf der Symbolleiste der Citrix Workspace-App auf das Symbol **Hochladen** und wählen Sie die gewünschte Datei aus. Um Dateien vom Linux

VDA auf das Clientgerät herunterzuladen, klicken Sie auf das Symbol **Herunterladen**. Sie können während des Uploads und Downloads Dateien hinzufügen. Sie können bis zu 100 Dateien gleichzeitig übertragen.

**Hinweis:**

Zum Hochladen und Herunterladen von Dateien zwischen Linux VDA und Clientgerät müssen Sie die Symbolleiste der Citrix Workspace-App aktivieren.

Sie können eine Version der Citrix Workspace-App verwenden, mit der Sie Dateien per Drag & Drop verschieben können.

Der automatische Download ist eine Erweiterung der Dateiübertragung. Dateien, die Sie in das Verzeichnis **Auf eigenem Gerät speichern** auf dem VDA herunterladen oder verschieben, werden automatisch an das Clientgerät übertragen.

Hinweis:

Für den automatischen Download müssen die Richtlinien **Dateiübertragungen zwischen Desktop und Client zulassen** und **Dateien vom Desktop herunterladen** auf **Zulässig** festgelegt sein.

Beispiele von Anwendungsfällen für den automatischen Download:

- Download von Dateien in **Auf eigenem Gerät speichern**

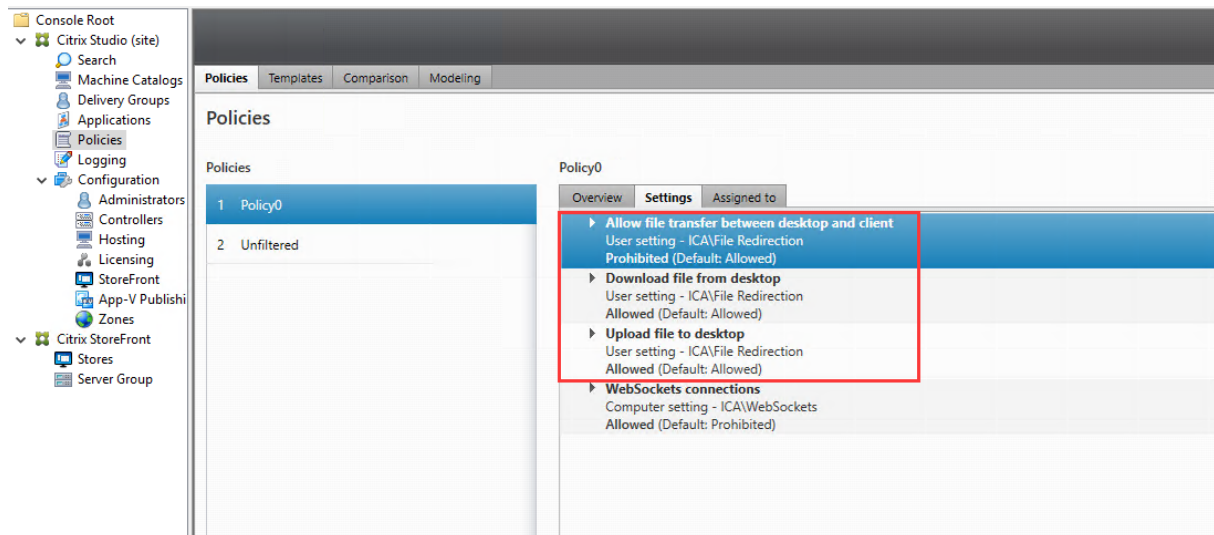
In Sitzungen mit veröffentlichten Desktops und Webbrowser-Apps können Sie von Websites heruntergeladene Dateien zur automatischen Übertragung auf das Clientgerät im Verzeichnis **Auf eigenem Gerät speichern** auf dem VDA speichern. Damit der automatische Download funktioniert, legen Sie das Standard-Downloadverzeichnis des Sitzungs-Webrowsers auf **Auf eigenem Gerät speichern** und in dem Webbrowser, in dem die Citrix Workspace-App für HTML5 oder Chrome ausgeführt wird, ein lokales Downloadverzeichnis fest.

- Verschieben oder Kopieren von Dateien in **Auf eigenem Gerät speichern**

Wählen Sie in Sitzungen mit veröffentlichten Desktops die Zieldateien aus und verschieben oder kopieren Sie diese in das Verzeichnis **Auf eigenem Gerät speichern**, damit sie auf dem Clientgerät verfügbar sind.

Dateiübertragungsrichtlinien

Sie können Citrix Studio verwenden, um die Dateiübertragungsrichtlinien festzulegen. In der Standardeinstellung ist die Dateiübertragung aktiviert.



Richtlinienbeschreibungen:

- **Dateiübertragungen zwischen Desktop und Client zulassen:** Ermöglicht oder hindert Benutzer daran, Dateien zwischen einer Citrix Virtual Apps and Desktops-Sitzung und den Geräten zu übertragen.
- **Dateien von Desktop herunterladen:** Ermöglicht oder hindert Benutzer daran, Dateien von einer Citrix Virtual Apps and Desktops-Sitzung zum Gerät herunterzuladen.
- **Dateien auf Desktop hochladen:** Ermöglicht oder hindert Benutzer daran, Dateien von den Geräten zu einer Citrix Virtual Apps and Desktops-Sitzung hochzuladen.

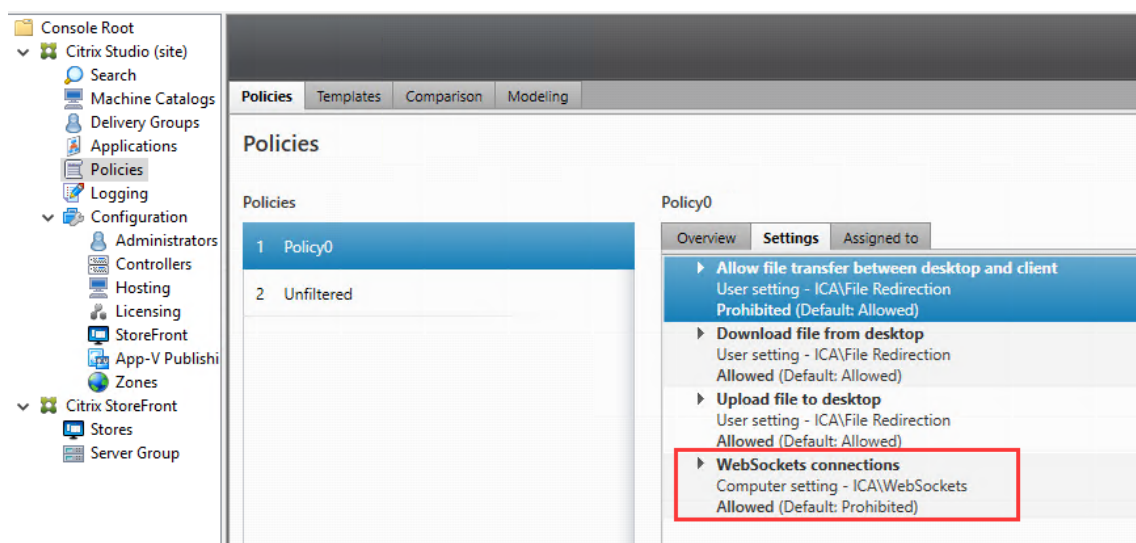
Hinweis:

Um sicherzustellen, dass die Richtlinien **Dateien von Desktop herunterladen** und **Dateien auf Desktop hochladen** angewendet werden, setzen Sie die Richtlinie **Dateiübertragungen zwischen Desktop und Client zulassen** auf **Zulässig**.

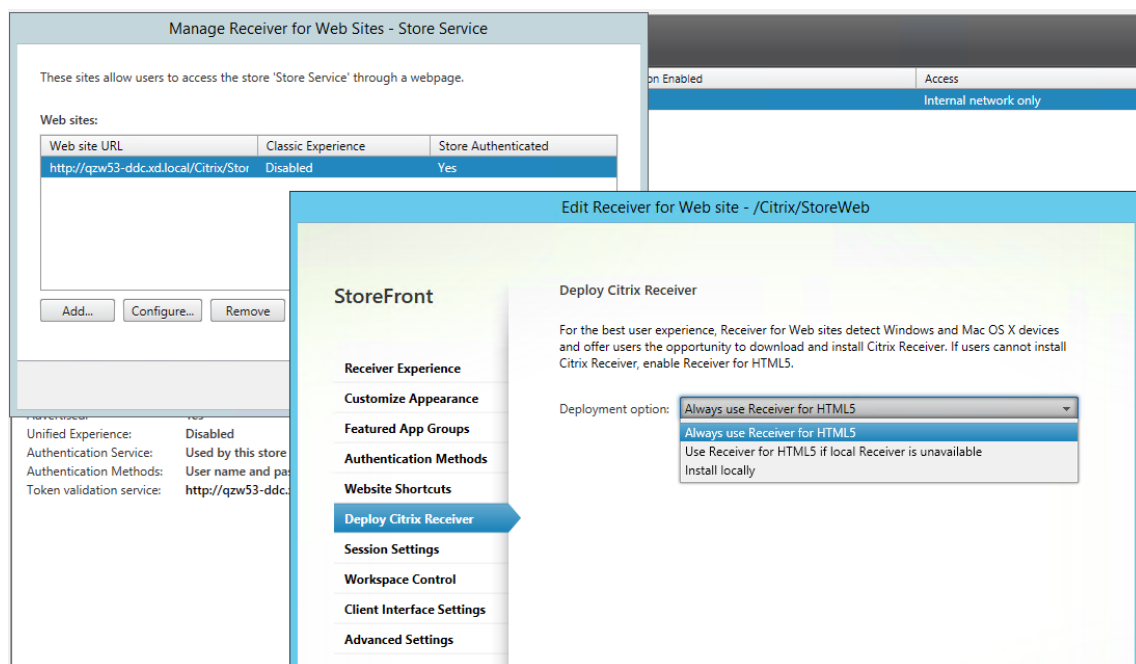
Verwendung

Um das Dateiübertragungsfeature über die Citrix Workspace-App für HTML5 zu verwenden:

1. Legen Sie in Citrix Studio für die Richtlinie **WebSockets-Verbindungen** die Einstellung **Zulassen** fest.



2. Aktivieren Sie in Citrix Studio die Dateiübertragung über die oben beschriebenen Dateiübertragungsrichtlinien.
3. Klicken Sie in der Citrix StoreFront-Verwaltungskonzole auf **Stores**, wählen Sie den Knoten **Receiver für Web-Sites verwalten** und aktivieren Sie Citrix Receiver für HTML5, indem Sie die Option **Immer Receiver für HTML5 verwenden** wählen.



4. Starten Sie eine virtuelle Desktop- oder Webbrowser-App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux VDA und dem Clientgerät durch.

Um das Dateiübertragungsfeature über die Citrix Workspace-App für Chrome zu verwenden:

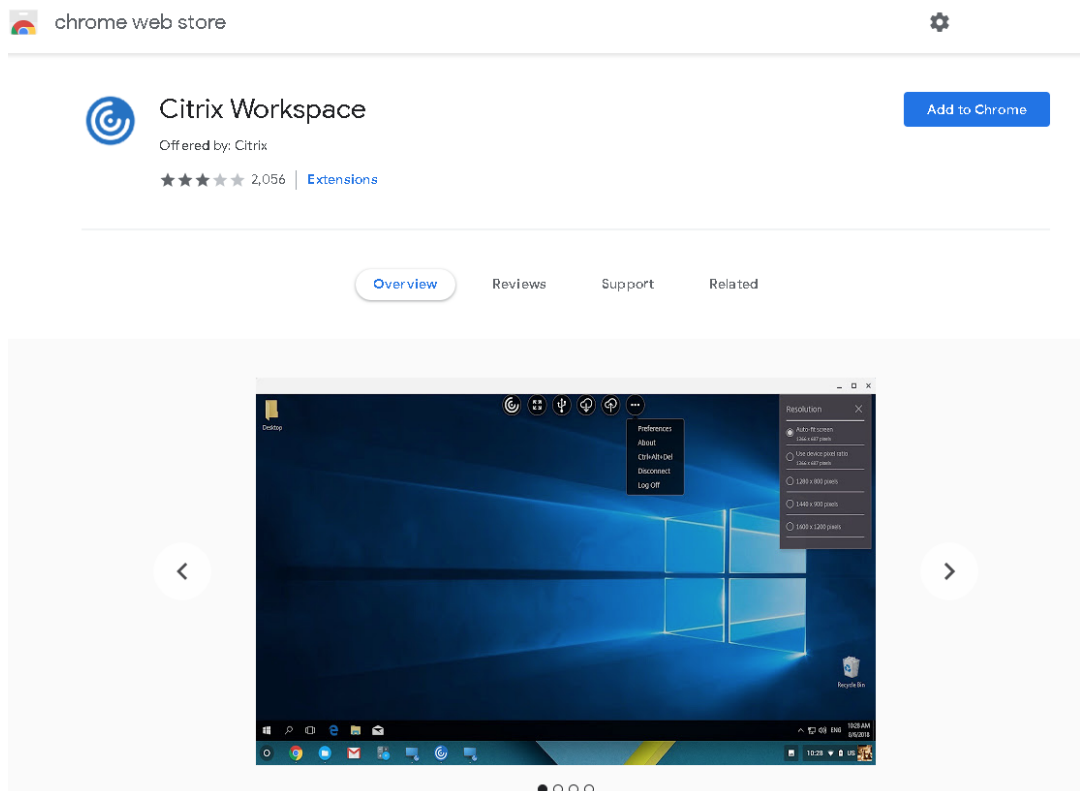
1. Aktivieren Sie die Dateiübertragung über die oben beschriebenen Dateiübertragungsrichtlinien.

ien.

2. Rufen Sie Citrix Workspace-App aus dem Chrome Web Store ab.

Überspringen Sie diesen Schritt, wenn Sie bereits Citrix Workspace-App für Chrome der Seite “Chrome-Apps” hinzugefügt haben.

- a) Geben Sie **Citrix Workspace für Chrome** in das Suchfeld von Google Chrome ein. Klicken Sie auf das Suchsymbol.
- b) Klicken Sie unter den Suchergebnissen auf die URL zum Chrome Web Store, in dem die Citrix Workspace-App verfügbar ist.



- c) Klicken Sie auf **Zu Chrome hinzufügen**, um die Citrix Workspace-App zu Google Chrome hinzuzufügen.
3. Klicken Sie auf der Seite “Chrome Apps” auf “Citrix Workspace-App für Chrome”.
 4. Geben Sie die URL des StoreFront-Stores ein, zu dem eine Verbindung hergestellt werden soll. Überspringen Sie diesen Schritt, wenn Sie die URL bereits vorher eingegeben haben.
 5. Starten Sie eine virtuelle Desktop- oder App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux VDA und dem Clientgerät durch.

Grafik

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Automatische DPI-Skalierung](#)
- [Clientakkustatusanzeige](#)
- [Grafikkonfiguration und -feineinstellung](#)
- [HDX-Bildschirmfreigabe](#)
- [Nicht-GRID 3D-Grafiken](#)
- [Textbasiertes Sitzungswasserzeichen](#)
- [Progressive Anzeige für Thinwire](#)

Automatische DPI-Skalierung

November 22, 2023

Der Linux VDA unterstützt die automatische DPI-Skalierung. Wenn ein Benutzer eine Sitzung mit virtuellem Desktop oder virtueller Anwendung öffnet, wird der DPI-Wert in der Sitzung automatisch an die DPI-Einstellung auf dem Client angepasst.

Beachten Sie folgende Überlegungen zu diesem Feature:

- Für das Feature müssen Sie die DPI-Anpassung für Citrix Workspace aktivieren. Bei Verwendung der Citrix Workspace-App für Windows muss die Option **Nein, native Auflösung verwenden** ausgewählt sein. Weitere Informationen zum Konfigurieren der DPI-Skalierung für die Citrix Workspace-App für Windows finden Sie unter [DPI-Skalierung](#).
- In Szenarien mit mehreren verwendeten Bildschirmen muss auf jedem Bildschirm dieselbe DPI-Einstellung konfiguriert sein. Szenarien mit unterschiedlichen DPI-Einstellungen werden nicht unterstützt. Wenn unterschiedliche DPI-Einstellungen vorliegen, wendet der Linux VDA auf alle Bildschirme den kleinsten DPI-Wert an.
- Das Feature ist für MATE, GNOME, GNOME Classic und KDE aktiviert. Beachten Sie mit KDE oder MATE Folgendes:
 - Für virtuelle Linux-Desktops in einer KDE-Desktopumgebung:
 - * Wir empfehlen die Verwendung von KDE Plasma 5 oder höher.

- ★ Wenn Sie die DPI-Einstellungen auf dem Client ändern, während Sitzungen ausgeführt werden, müssen Benutzer sich ab- und erneut anmelden.
- Für virtuelle Linux-Desktops in einer MATE-Desktopumgebung:
 - ★ Es werden nur die Skalierungsfaktoren 1 und 2 unterstützt.
 - ★ Wenn Sie die DPI-Einstellungen auf dem Client ändern, während Sitzungen ausgeführt werden, müssen Benutzer sich ab- und erneut anmelden.
- Der DPI-Wert in der virtuellen Sitzung wird automatisch an die DPI-Einstellung auf dem Client angepasst. Derzeit unterstützt das Feature nur ganzzahlige Skalierungsfaktoren, z. B. 100 % und 200 %. Wenn auf dem Client ein Skalierungsfaktor vom Typ “Bruchzahl” konfiguriert ist, wird der DPI-Wert der virtuellen Sitzung gemäß der folgenden Tabelle in einen ganzzahligen Skalierungsfaktor geändert. Beispiel: Bei einem Skalierungsfaktor von 125 % ändert sich der DPI-Wert in 100 %.

Skalierungsfaktor auf dem Client	DPI der Remotesitzung
Weniger als oder gleich 174 %	96 (1 x 96)
175–274 %	192 (2 x 96)
275–399 %	288 (3 x 96)
Größer als oder gleich 400 %	384 (4 x 96)

Clientakkustatusanzeige

October 5, 2022

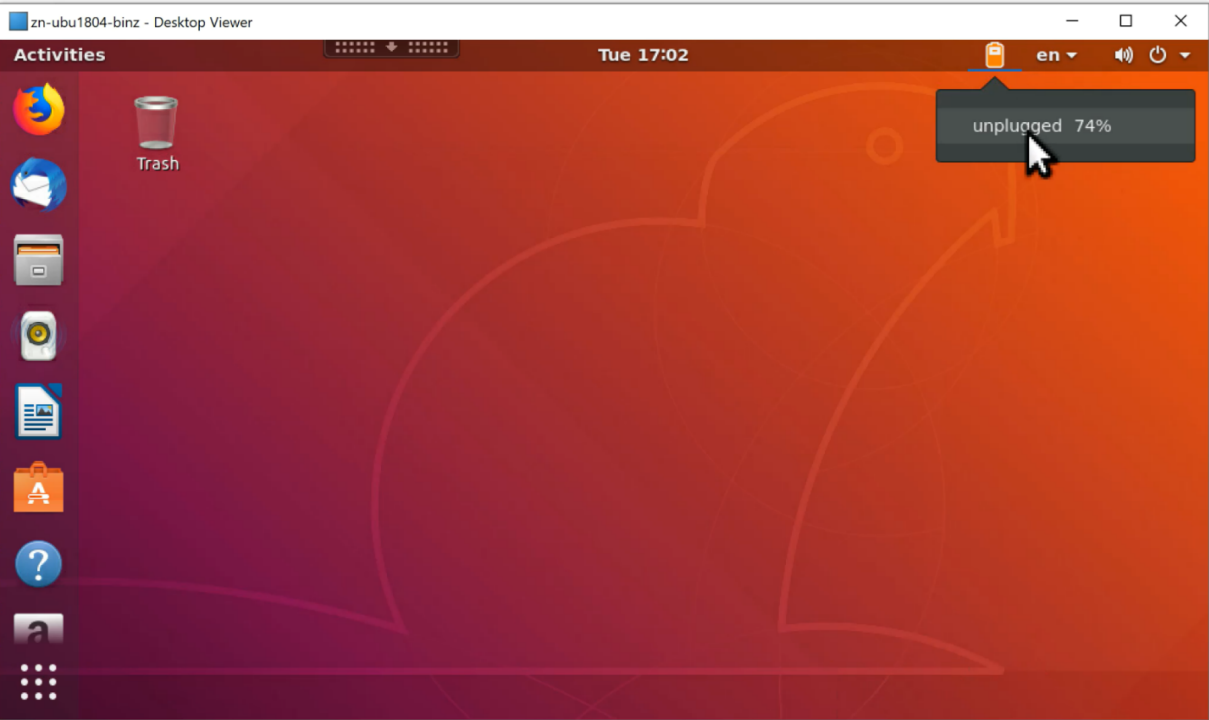
Der Linux VDA kann den Akkustatus von Clientgeräten zu virtuellen Desktops umleiten und dort anzeigen. Dieses Feature ist standardmäßig aktiviert und für folgende Versionen der Citrix Workspace-App verfügbar:

- Citrix Workspace-App für iOS
- Citrix Workspace-App für Linux
- Citrix Workspace-App für Mac (Version 2204.1 wird nicht unterstützt)
- Citrix Workspace-App für Windows (Version 2204.1 wird nicht unterstützt)

Übersicht




Wenn Benutzer einen virtuellen Desktop öffnen, wird im Linux-Infobereich ein Akkusymbol angezeigt. Dieses Symbol zeigt den Akkustatus ihrer Clientgeräte an. Klicken Sie auf das Akkusymbol, um die

verbleibende Akkulaufzeit (in Prozent) zu überprüfen. Ein Beispiel sehen Sie im folgenden Screenshot:



Je nach Akkustatus werden unterschiedliche Symbole angezeigt. Eine Übersicht finden Sie in der folgenden Tabelle:

Akkusymbol	Ladezustand	Akkustand	Verbleibende Akkulaufzeit in Prozent
	Akku wird geladen („+“-Symbol)	Hoch (grüner Akku)	<div><div></div></div> =80 %
	Akku wird geladen („+“-Symbol)	Mittel (orangefarbener Akku)	<div><div></div></div> = 20 % und < 80 %
	Akku wird geladen („+“-Symbol)	Niedrig (roter Akku)	< 20 %
	Akku wird nicht geladen („-“-Symbol)	Hoch (grüner Akku)	<div><div></div></div> =80 %

Akkusymbol	Ladezustand	Akkustand	Verbleibende Akkulaufzeit in Prozent
	Akku wird nicht geladen („--“-Symbol)	Mittel (orangefarbener Akku)	<div><div></div></div> = 20 % und < 80 %
	Akku wird nicht geladen („--“-Symbol)	Niedrig (roter Akku)	< 20 %
	Unbekannt	Unbekannt	Unbekannt

Konfiguration

Die Client-Akkustatusanzeige ist standardmäßig aktiviert.

Führen Sie folgenden Befehl aus, um das Feature zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\  
Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000000"  
2 <!--NeedCopy-->
```

Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

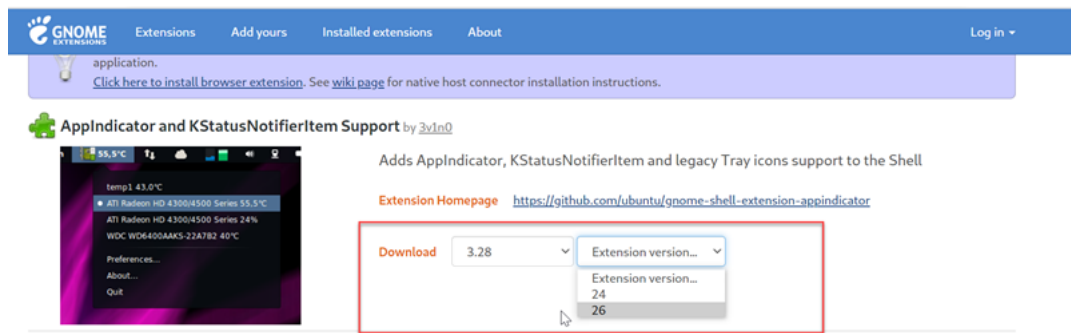
```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\  
Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000001"  
2 <!--NeedCopy-->
```

Hinweis:

Die oben genannten Befehle wirken sich auf das **Bildschirmtastatur**-Feature aus, das Mobile Receiver Virtual Channel (MRVC) mit der Client-Akkustatusanzeige verwendet.

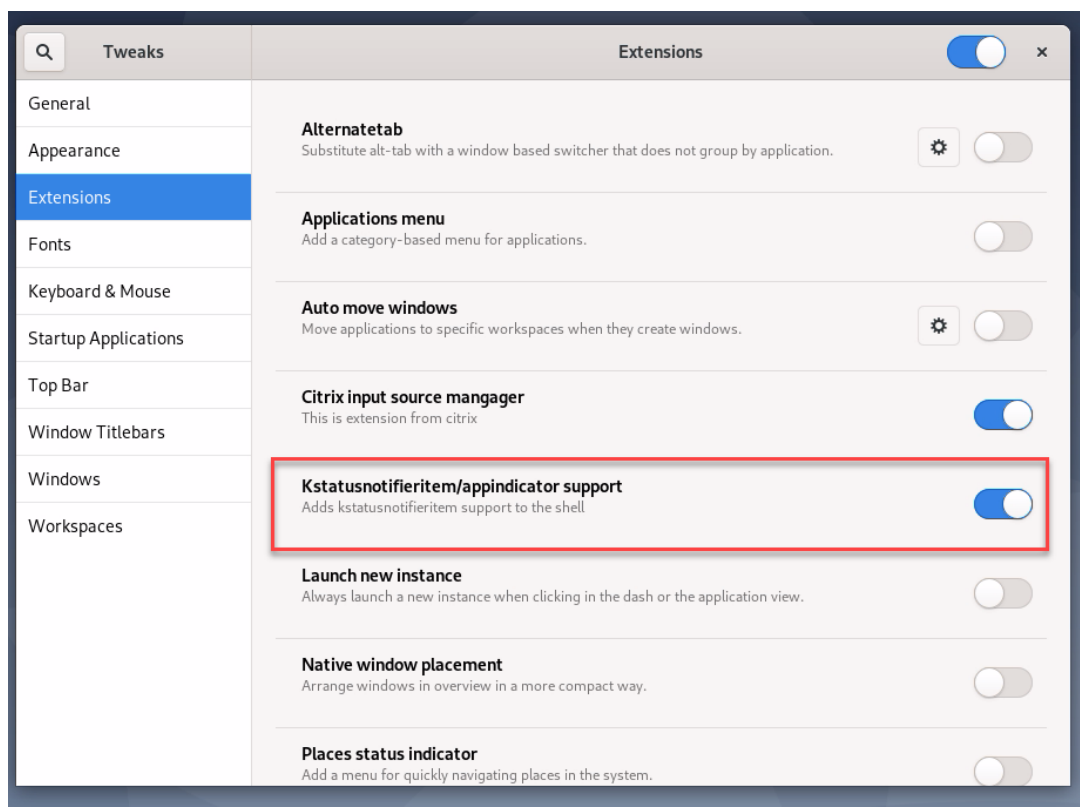
Führen Sie je nach vorliegender Distribution folgende zusätzlichen Schritte aus:

1. Bei Verwendung von mit GNOME installiertem RHEL 8.x oder SUSE 15.x installieren Sie eine kompatible Erweiterung für die GNOME-Shell, um die AppIndicator-Unterstützung zu aktivieren:
 - a) Führen Sie den Befehl `gnome-shell --version` aus, um Ihre GNOME-Shellversion zu überprüfen.
 - b) Laden Sie eine kompatible Erweiterung für die GNOME-Shell von <https://extensions.gnome.org/extension/615/appindicator-support> herunter. Wenn Ihre Shellversion beispielsweise 3.28 ist, können Sie 24 oder 26 als Erweiterungsversion auswählen.



- c) Entpacken Sie das heruntergeladene TAR-Paket. Stellen Sie sicher, dass der Wert “**uuid**” in der Datei **metadata.json** im Paket auf **appindicatorsupport@rgcjonas.gmail.com** gesetzt ist.
 - d) Führen Sie den Befehl `mv` aus, um das Verzeichnis **appindicatorsupport@rgcjonas.gmail.com** unter `/usr/share/gnome-shell/extensions/` zu speichern.
 - e) Führen Sie den Befehl `chmod a+r metadata.json` aus, um die Datei **metadata.json** für andere Benutzer lesbar zu machen.
- Tipp:**

Die Datei **metadata.json** im Verzeichnis **appindicatorsupport@rgcjonas.gmail.com** kann standardmäßig nur vom Root-Benutzer gelesen werden. Um die Bildschirmfreigabe zu unterstützen, machen Sie die Datei **metadata.json** auch für andere Benutzer lesbar.
- f) Installieren Sie GNOME Tweaks.
 - g) Laden Sie in der Desktopumgebung Ihre GNOME-Shell neu, indem Sie nacheinander die Tasten **Alt+F2**, **r** und **Enter** drücken oder aber den Befehl `killall -SIGQUIT gnome-shell` ausführen.
 - h) Führen Sie in der Desktopumgebung GNOME Tweaks aus und aktivieren Sie **KStatusNotifierItem/AppIndicator Support** im Tweaks-Tool.
2. Bei Verwendung von mit GNOME installiertem Debian 11.3 oder Debian 10.9 führen Sie die folgenden Schritte aus, um GNOME-Taskleistensymbole zu installieren und zu aktivieren:
 - a) Führen Sie den Befehl `sudo apt install gnome-shell-extension-appindicator` aus. Sie müssen sich möglicherweise abmelden und erneut anmelden, damit die Erweiterung von GNOME erkannt wird.
 - b) Suchen Sie im Bildschirm **Activities** nach Tweaks.
 - c) Wählen Sie im Tweaks-Tool **Extensions**.
 - d) Aktivieren Sie **Kstatusnotifieritem/appindicator support**.



Grafikkonfiguration und -feineinstellung

November 22, 2023

Dieser Artikel enthält eine Anleitung zur Grafikkonfiguration und -optimierung für den Linux VDA.

Weitere Informationen finden Sie unter [Systemanforderungen](#) und [Installationsübersicht](#).

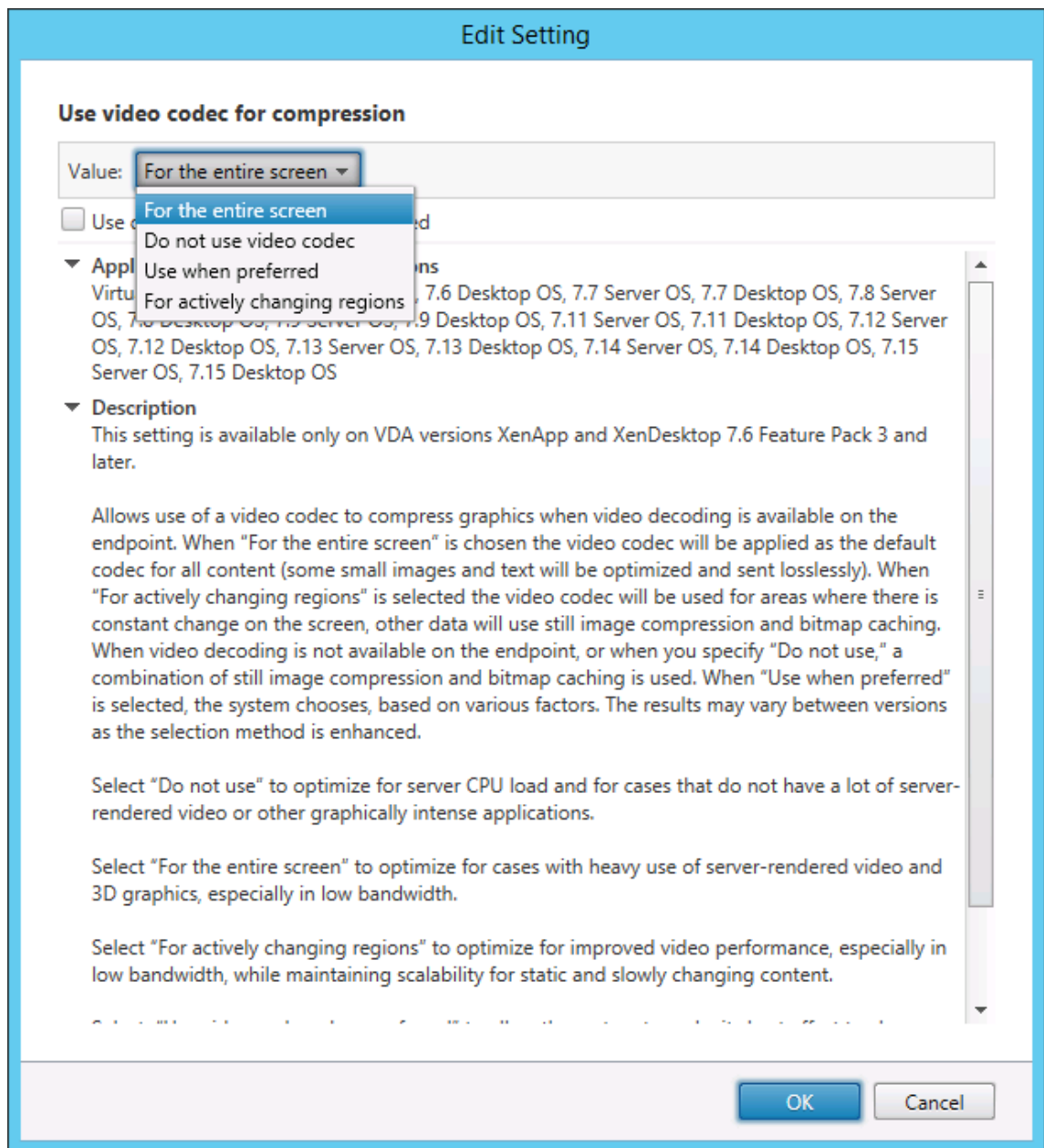
Konfiguration

Videocodec für die Komprimierung

Thinwire ist die bei Linux VDAs verwendete Technologie für das Anzeigeremoting. Durch sie können auf einer Maschine erzeugte Grafiken auf eine andere Maschine für die Anzeige übertragen werden (normalerweise über ein Netzwerk).

Die Richtlinie [Videocodec für Komprimierung verwenden](#) bestimmt den Standardgrafikmodus und bietet folgende Optionen für verschiedene Anwendungsfälle:

- **Verwenden, wenn bevorzugt.** Dies ist die Standardeinstellung. Eine zusätzliche Konfiguration ist nicht erforderlich. Dies stellt sicher, dass Thinwire für alle Citrix Verbindungen ausgewählt und für Skalierbarkeit, Bandbreite und bessere Bildqualität bei typischen Desktoparbeitslasten optimiert wird.
- **Für den gesamten Bildschirm.** Thinwire wird mit Vollbild-H.264 oder -H.265 zur Optimierung der Benutzererfahrung und Bandbreite, insbesondere bei intensiver 3D-Grafiknutzung, verwendet.
- **Für aktive Änderungsbereiche.** Die Technologie für adaptive Anzeige von Thinwire identifiziert Bewegtbilder (Video, 3D In Motion). H.264 wird nur in dem Bildschirmbereich verwendet, in dem das Bild sich bewegt. Mit der selektiven Verwendung des H.264-Videocodecs können Bildschirmsegmente, die häufig mit dem H.264-Videocodec aktualisiert werden, von HDX Thinwire erkannt und codiert werden. Für den übrigen Bildschirm (einschließlich Text und Fotos) werden weiterhin die Standbildkomprimierung (JPEG, RLE) und das Bitmapcaching verwendet. Dies verbraucht weniger Bandbreite und führt zu einer verbesserten Anzeige von Videoinhalten, verbunden mit verlustfreiem Text und hoher Bildqualität. Um dieses Feature zu aktivieren, legen Sie die Richtlinie **Verwenden von Videocodec für die Komprimierung** auf **Verwenden, wenn bevorzugt** (Standardeinstellung) oder **Für aktive Änderungsbereiche** fest. Weitere Informationen finden Sie unter [Einstellungen der Richtlinie “Grafiken”](#). Informationen zum Aktivieren der H.264-Hardwarecodierung für dieses Feature finden Sie unter [H.264-Hardwarecodierung](#).



Einige weitere Richtlinieneinstellungen, einschließlich der nachfolgend aufgeführten Einstellungen der Richtlinie "Visuelle Anzeige", können zur Optimierung der Anzeigeremoting-Leistung verwendet werden:

- **Bevorzugte Farbtiefe für einfache Grafiken**
- **Frameratesollwert**
- **Bildqualität**

H.264-Hardwarekodierung

Die Richtlinie **Hardwarekodierung für Videocodec verwenden** ermöglicht die Verwendung von Grafikhardware (falls verfügbar) zum Komprimieren von Bildelementen mit dem Videocodec. Ist entsprechende Hardware nicht verfügbar, wird die CPU-basierte Codierung mit dem Software-Videocodec verwendet.

Ab Version 2204 unterstützt der Linux VDA die selektive Verwendung des H.264-Hardwarecodecs für aktive Änderungsbereiche. Dieses Feature verlagert den zur Videokomprimierung notwendigen CPU-Verbrauch auf die Hardware und verbessert Bildqualität und FPS-Wert (Frames pro Sekunde). Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Aktivieren Sie die Richtlinie **Hardwarekodierung für Videocodec verwenden**.
2. Aktivieren Sie die Richtlinie **Videocodec zur Komprimierung verwenden** und wählen Sie **Für aktive Änderungsbereiche**.

Visuell verlustfreie Komprimierung zulassen

Mit der Richtlinie **Visuell verlustfreie Komprimierung zulassen** wird für Grafiken visuell verlustfreie Komprimierung statt echter verlustfreier Komprimierung verwendet. Visuell verlustfreie Komprimierung steigert im Vergleich zu echter verlustfreier Komprimierung die Leistung, hat jedoch geringe Verluste, die für das Auge nicht erkennbar sind. Durch diese Einstellung ändert sich, wie die Einstellungswerte für die **Bildqualität** verwendet werden.

Die Richtlinie **Visuell verlustfreie Komprimierung zulassen** ist standardmäßig deaktiviert. Um die visuell verlustfreie Komprimierung zu aktivieren, setzen Sie **Visuell verlustfreie Komprimierung zulassen** auf **Aktiviert** und die Richtlinie für **visuelle Qualität** auf **Zu verlustfrei verbessern**.

Wenn die Richtlinie **Videocodec für Komprimierung verwenden** auf **Videocodec nicht verwenden** festgelegt ist, wird die visuell verlustfreie Komprimierung auf die statische Bildcodierung angewendet. Wenn die Richtlinie **Videocodec für Komprimierung verwenden** auf einen anderen Grafikmodus als **Videocodec nicht verwenden** festgelegt ist, wird die visuell verlustfreie Komprimierung auf die statische H.264-Codierung angewendet.

Die folgenden Clients unterstützen selektives H.264:

- Citrix Receiver für Windows 4.9 bis 4.12
- Citrix Receiver für Linux 13.5 bis 13.10
- Citrix Workspace-App 1808 für Windows und höher
- Citrix Workspace-App 1808 für Linux und höher

Weitere Informationen zu den Richtlinieneinstellungen für **Bildqualität** und **Videocodec zur Komprimierung verwenden** finden Sie unter [Einstellungen der Richtlinie “Visuelle Anzeige”](#) und [Einstellungen der Richtlinie “Grafiken”](#).

Unterstützung für H.265-Videocodec

Ab Version 7.18 unterstützt der Linux VDA die Hardwarebeschleunigung von Remotegrafiken und -videos per H.265-Videocodec.

Das Feature ist kompatibel mit:

- Citrix Receiver für Windows 4.10 bis 4.12
- Citrix Workspace-App 1808 für Windows und höher

Um das Feature zu nutzen, müssen Sie es auf dem Linux VDA und auf dem Client aktivieren. Wenn die GPU auf dem Client eine H.265-Decodierung über die DXVA-Schnittstelle nicht unterstützt, wird die Einstellung der Richtlinie “H.265-Decodierung für Grafiken” ignoriert und Sitzungen greifen auf den H.264-Videocodec zurück. Weitere Informationen finden Sie unter [H.265-Videoencoding](#).

Aktivieren der H.265-Hardwarecodierung auf dem VDA:

1. Aktivieren Sie die Richtlinie **Hardwarecodierung für Videocodec verwenden**.
2. Aktivieren der Richtlinie **Optimierung für 3D-Grafikworkload**
3. Stellen Sie sicher, dass für die Richtlinie **Videocodec zur Komprimierung verwenden** die Standardeinstellung oder **Für den gesamten Bildschirm** verwendet wird.
4. Stellen Sie sicher, dass die Richtlinie **Bildqualität NICHT** auf **Zu verlustfrei verbessern** oder **Immer verlustfrei** festgelegt ist.

Informationen zum Aktivieren der H.265-Hardwarecodierung auf dem Client finden Sie unter [H.265-Videoencoding](#).

Unterstützung für YUV444-Softwarecodierung

Der Linux VDA unterstützt die YUV444-Softwarecodierung. Das YUV-Kodierungsschema weist jedem Pixel sowohl Helligkeits- als auch Farbwerte zu. In YUV steht ‘Y’ für den Helligkeits- bzw. ‘Luma’-Wert und ‘UV’ für die Farb- oder “Chroma”-Werte. Sie können dieses Feature in Citrix Receiver für Windows 4.10 bis 4.12 und in der Citrix Workspace-App 1808 für Windows und höher verwenden.

Jeder eindeutige Y-, U- oder V- Wert hat 8 Bits oder ein Byte an Daten. Das Datenformat YUV444 überträgt 24 Bit pro Pixel. Das Datenformat YUV422 teilt U- und V- Werte zwischen zwei Pixeln, was zu einer durchschnittlichen Übertragungsrate von 16 Bit pro Pixel führt. Folgende Tabelle zeigt einen intuitiven Vergleich zwischen YUV444 und YUV420.

YUV444

	A	B	C
1	Citrix	Citrix	Citrix
2	Citrix	Citrix	Citrix
3	Citrix	Citrix	Citrix
4	Citrix	Citrix	Citrix
5	Citrix	Citrix	Citrix
6	Citrix	Citrix	Citrix

YUV420

	A	B	C
1	Citrix	Citrix	Citrix
2	Citrix	Citrix	Citrix
3	Citrix	Citrix	Citrix
4	Citrix	Citrix	Citrix
5	Citrix	Citrix	Citrix
6	Citrix	Citrix	Citrix

Aktivieren der YUV444-Softwarcodierung auf dem VDA:

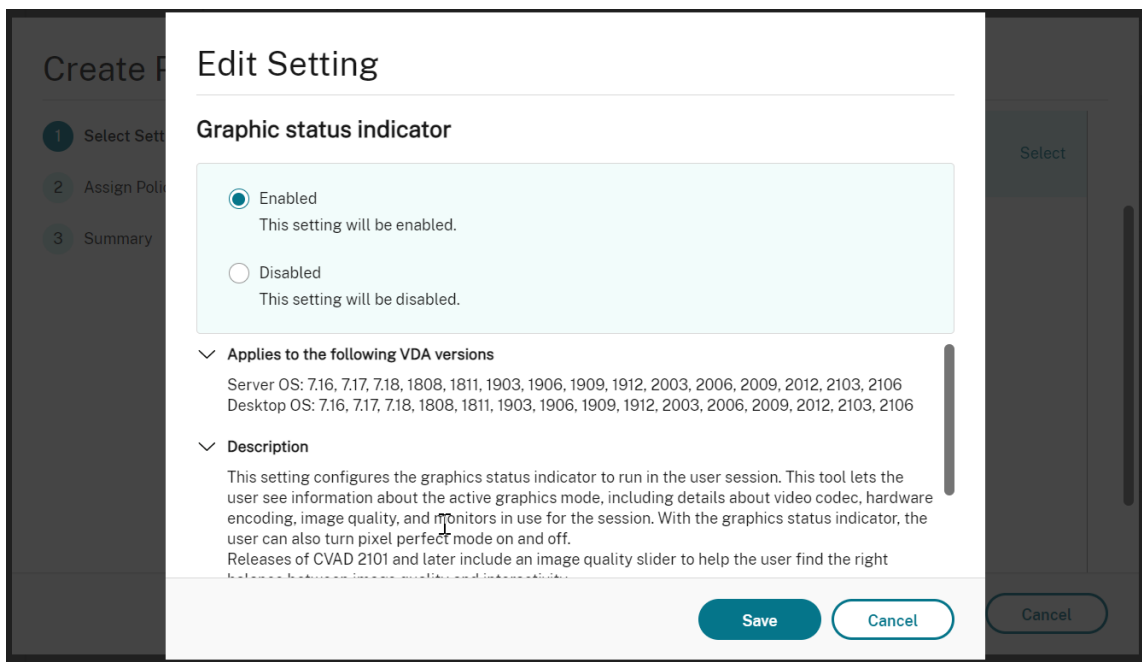
1. Stellen Sie sicher, dass für die Richtlinie **Videocodec zur Komprimierung verwenden** die Einstellung **Für den gesamten Bildschirm** verwendet wird.
2. Stellen Sie sicher, dass die Richtlinie **Bildqualität** auf **Immer verlustfrei** oder **Zu verlustfrei verbessern** festgelegt ist.

Schieberegler für Grafikqualität

In der in virtuellen Linux-Sitzungen ausgeführten Grafikstatusanzeige gibt es jetzt einen Schieberegler für Grafikqualität. Mit dem Schieberegler finden Sie das richtige Gleichgewicht zwischen Bildqualität und Interaktivität.

Führen Sie die folgenden Schritte aus, um den Schieberegler zu verwenden:

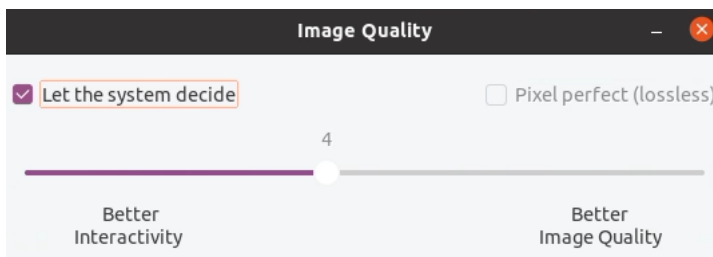
1. Aktivieren Sie die Richtlinie **Grafikstatusanzeige** in Citrix Studio.



- Öffnen Sie das Terminal und führen Sie den Befehl `ctxslider` aus. Der Schieberegler wird angezeigt.

Hinweis:

Wenn Sie die Richtlinie **Bildqualität** auf **Immer verlustfrei** oder **Zu verlustfrei verbessern** festgelegt haben, wird der Schieberegler nicht angezeigt.



Die folgenden Optionen sind jetzt verfügbar:

- Um die Bildqualität zu ändern, verschieben Sie den Schieberegler. Der Schieberegler hat einen Bereich von 0 bis 9.
- Um systemdefinierte Einstellungen zu verwenden, wählen Sie **System entscheiden lassen**.
- Um in den verlustfreien Modus zu wechseln, wählen Sie **Pixelgenau**.

Anpassen der durchschnittlichen Bitraten basierend auf Bandbreitenschätzungen

Citrix verbessert die HDX 3D Pro-Hardwarecodierung durch Anpassung der durchschnittlichen Bitraten basierend auf Bandbreitenschätzungen.

Wenn die HDX 3D Pro-Hardwarecodierung verwendet wird, kann der VDA sporadisch die Bandbreite des Netzwerks schätzen und die Bitraten von codierten Frames entsprechend anpassen. Dieses neue Feature bietet einen Mechanismus, um zwischen Schärfe und Fluss auszugleichen.

Dieses Feature ist standardmäßig aktiviert. Führen Sie folgenden Befehl aus, um es zu deaktivieren:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   DisableReconfigureEncoder" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Zusätzlich zu diesem Feature können Sie auch die folgenden Befehle ausführen, um zwischen Schärfe und Fluss anzupassen. Die Parameter **AverageBitRatePercent** und **MaxBitRatePercent** legen den Prozentsatz der Bandbreitenauslastung fest. Je höhere Werte Sie festlegen, desto schärfer sind Grafiken und weniger glatt fließen sie. Der empfohlene Bereich für diese Einstellung ist 50 bis 100.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   AverageBitRatePercent" -d "90" --force
2
3 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   MaxBitRatePercent" -d "100" --force
4 <!--NeedCopy-->
```

Wenn mit der durchschnittlichen Bitratenanpassung der Bildschirm angehalten wird, erscheint der letzte Frame mit niedriger Qualität, weil keine neuen Frames gesendet werden. Die Schärfungsunterstützung kann dieses Problem beheben, indem neu konfiguriert und sofort der neueste Frame in höchster Qualität sofort gesendet wird.

Eine vollständige Liste der von Linux VDA Thinwire unterstützten Richtlinien finden Sie unter [Liste der unterstützten Richtlinien](#).

Informationen zur Konfiguration der Multi-Monitor-Unterstützung für den Linux VDA finden Sie unter [CTX220128](#).

Parallele Verarbeitung

Thinwire kann die Anzahl der Frames pro Sekunde (FPS) durch Parallelisierung bestimmter Aufgaben verbessern, was einen insgesamt etwas höheren CPU-Verbrauch verursacht. Das Feature ist in der Standardeinstellung deaktiviert. Führen Sie den folgenden Befehl auf Ihrem VDA aus, um das Feature zu aktivieren:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   ParallelProcessing" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Problembehandlung

Verwendeten Grafikmodus ermitteln

Führen Sie folgenden Befehl aus, um den verwendeten Grafikmodus zu ermitteln (**0** ist TW+, **1** ist Vollbildvideocodec):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
2 <!--NeedCopy-->
```

Das Ergebnis sieht in etwa wie folgt aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force
```

Ermitteln, ob H.264 verwendet wird

Führen Sie folgenden Befehl aus, um zu ermitteln, ob H.264 verwendet wird (**0** = nicht verwendet, **1** = verwendet):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
2 <!--NeedCopy-->
```

Das Ergebnis sieht in etwa wie folgt aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000000"--force
```

Ermitteln, ob H.265 verwendet wird

Führen Sie folgenden Befehl aus, um zu ermitteln, ob Vollbild H.265 verwendet wird (**0** = nicht verwendet, **1** = verwendet):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
2 <!--NeedCopy-->
```

Das Ergebnis sieht in etwa wie folgt aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H265"-d "0x00000000"--force
```

Ermitteln des verwendeten YUV-Codierungsschemas

Führen Sie den folgenden Befehl aus, um zu überprüfen, welches YUV-Codierungsschema verwendet wird (**0** bedeutet YUV420. **1** bedeutet YUV422. **2** bedeutet YUV444):

Hinweis: Der Wert von "YUVFormat" ist nur dann sinnvoll, wenn ein Videocodect verwendet wird.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
2 <!--NeedCopy-->
```

Das Ergebnis sieht in etwa wie folgt aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000000"--force
```

Ermitteln, ob die YUV444-Softwarecodierung verwendet wird

Führen Sie den folgenden Befehl aus, um zu prüfen, ob die YUV444-Softwarecodierung verwendet wird:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
2 <!--NeedCopy-->
```

Wenn YUV444 verwendet wird, ähnelt das Ergebnis:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000000"--force
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000002"--force
```

Ermitteln, ob die Hardwarecodierung für 3D Pro verwendet wird

Führen Sie folgenden Befehl aus (**0** = nicht verwendet, **1** = verwendet):

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
2 <!--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:

```
1 Tue Apr 12 10:42:03 2016
2 +-----+
3 | NVIDIA-SMI 361.28      Driver Version: 361.28      |
4 |-----+-----+-----+
5 | GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile
6 |   Uncorr. ECC |
7 | Fan  Temp  Perf  Pwr:Usage/Cap|      Memory-Usage | GPU-Util
8 | Compute M. |
9 |=====+=====+=====+
10 |    0  GRID K1              Off   | 0000:00:05.0     Off   |
11 |          N/A |
12 | N/A   42C    P0      14W / 31W | 207MiB / 4095MiB |      8%
13 |   Default |
14 +-----+-----+-----+
15
16 | Processes:
17 |   Memory |
18 | GPU      PID   Type   Process name
19 |   Usage   |
20 +-----+-----+-----+
21 |    0      2164  C+G    /usr/local/bin/ctxgfx
22 |  106MiB |
23 |    0      2187    G      Xorg
24 |   85MiB |
25 +-----+-----+-----+
26 <!--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:

```
1 +-----+
2 | NVIDIA-SMI 352.70      Driver Version: 352.70      |
3 |-----+-----+-----+
4 | GPU   Name           Persistence-M| Bus-Id        Disp.A | Volatile
5 |   Uncorr. ECC |
6 | Fan  Temp  Perf  Pwr:Usage/Cap|      Memory-Usage | GPU-Util
7 | Compute M. |
8 +-----+-----+-----+
```

```
6 | =====+=====+=====+=====+
7 | 0 Tesla M60 Off | 0000:00:05.0 Off |
8 | N/A 20C P0 Off | 37W / 150W | 19MiB / 8191MiB | 0%
9 | Default |
10 |
11 | -----+-----+-----+-----+
12 | Processes: GPU
13 | Memory |
14 | GPU PID Type Process name
15 | Usage |
16 | =====+=====+=====+=====+
17 | No running processes found
18 |
19 | -----+-----+-----+-----+
20 | <!--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 Citrix Hypervisor-Konsole der Bildschirm der ICA-Desktopsitzung angezeigt

Workaround: Deaktivieren Sie die lokale VGA-Konsole der VM, indem Sie folgende Befehle ausführen:

Citrix Hypervisor 8.1 und höher:

```
1 [root@xenserver ~]# xe vgpu-param-set uuid=vgpu-uuid extra_args=
  disable_vnc=1
2 <!--NeedCopy-->
```

Citrix Hypervisor vor Version 8.1:

```
1 xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
2 <!--NeedCopy-->
```

NVIDIA K2-Grafikkarten unterstützen nicht die YUV444-Hardwarecodierung im Passthroughmodus

Bei aktivierter Richtlinieneinstellung **Zu verlustfrei verbessern** wird ein schwarzer oder grauer Bildschirm angezeigt, wenn Benutzer eine App- oder Desktop-Sitzung mit einer NVIDIA K2-Grafikkarte starten. Dieses Problem tritt auf, da NVIDIA K2-Grafikkarten die YUV444-Hardwarecodierung im Passthroughmodus nicht unterstützen. Weitere Informationen finden Sie unter [Video Encode and Decode GPU Support Matrix](#).

Gnome 3-Desktoppopups bei Anmeldung langsam

Dies ist eine Einschränkung im Gnome 3-Desktopsitzungsstart.

Einige OpenGL/WebGL-Anwendungen werden nach dem Ändern der Fenstergröße der Citrix Workspace-App nicht einwandfrei gerendert

Beim Ändern der Fenstergröße für die Citrix Workspace-App 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)’.

HDX-Bildschirmfreigabe

November 4, 2022

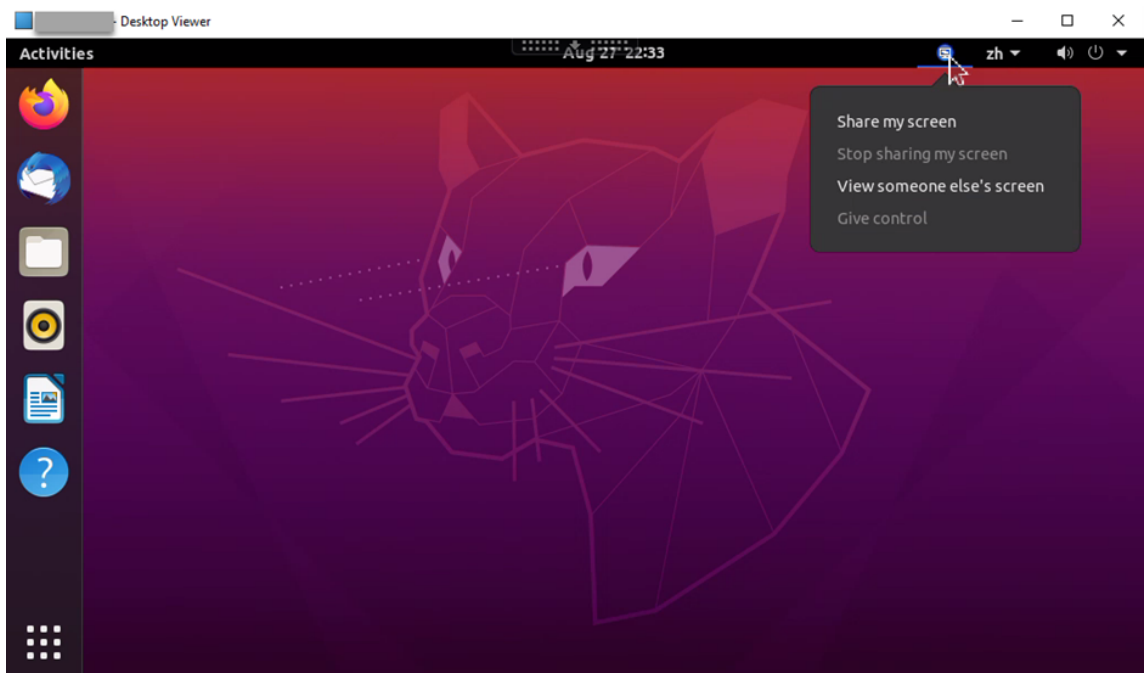
Übersicht

Mit dem Linux VDA können Sie den Bildschirm Ihres virtuellen Desktops für Sitzungsbenutzer auf anderen virtuellen Desktops freigeben.

Das folgende Beispiel erläutert die Schritte zur Freigabe eines Bildschirms und zur Anzeige des Bildschirms anderer Benutzer.

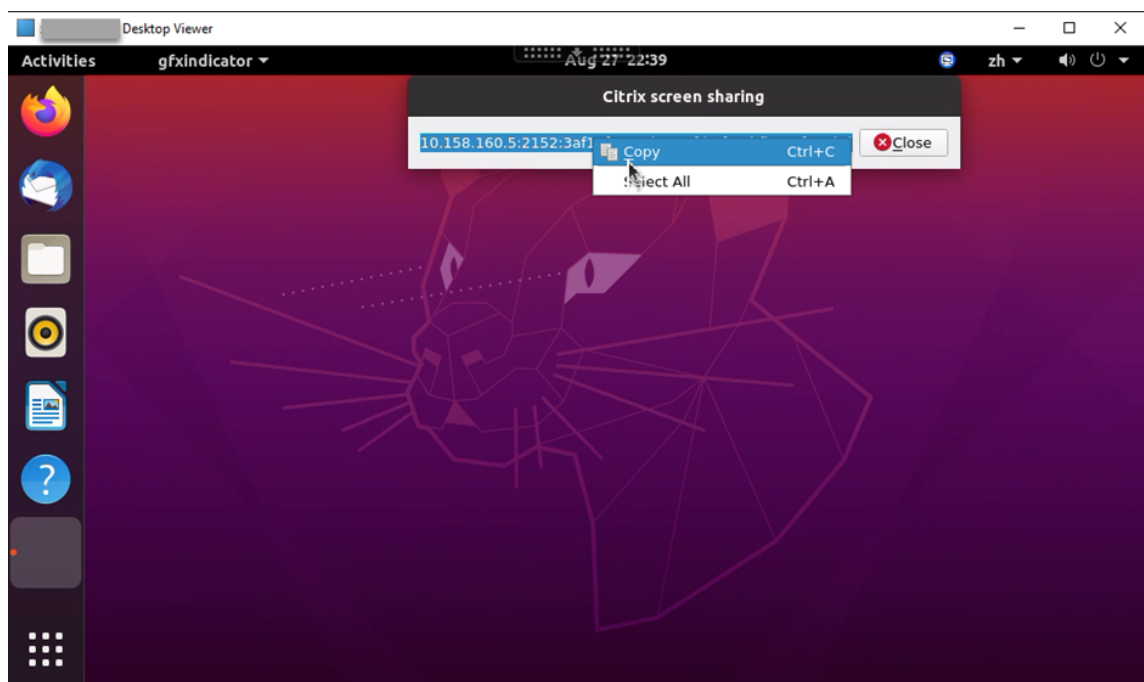
Freigeben des eigenen Bildschirms:

1. Klicken Sie im Infobereich Ihres virtuellen Desktops auf das Symbol für die **Bildschirmfreigabe** und wählen Sie **Meinen Bildschirm freigeben**.



2. Klicken Sie auf **Kopieren und schließen**.

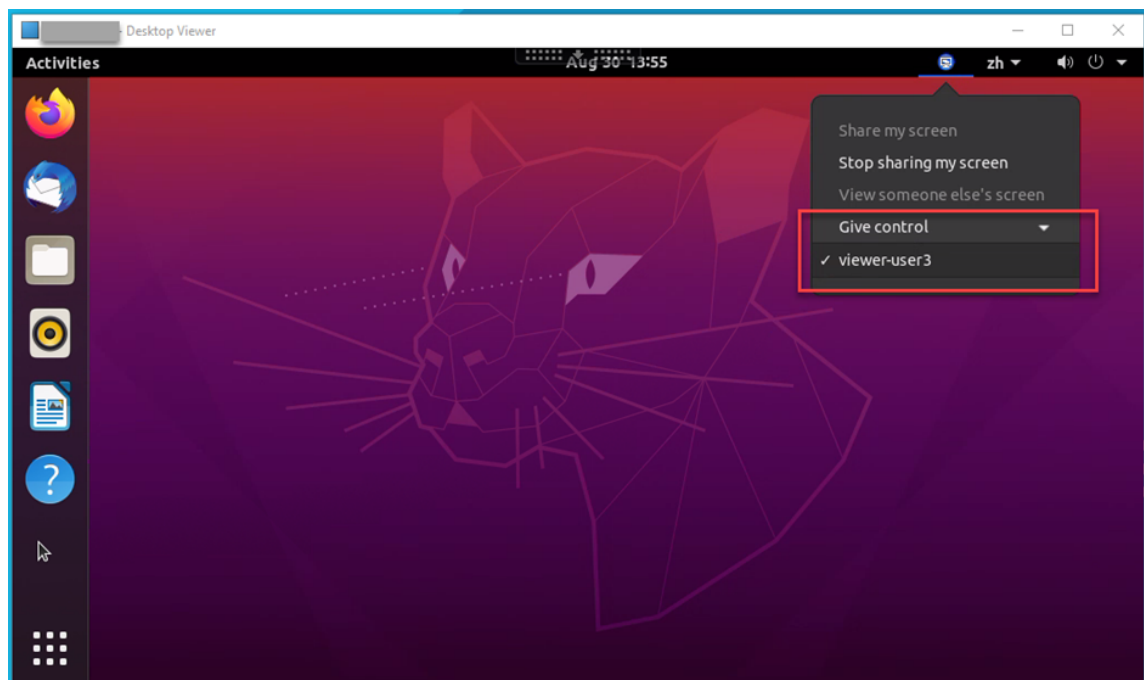
Der aktuelle Code für die Bildschirmfreigabe bleibt bestehen, bis Sie die Bildschirmfreigabe beenden und erneut starten.



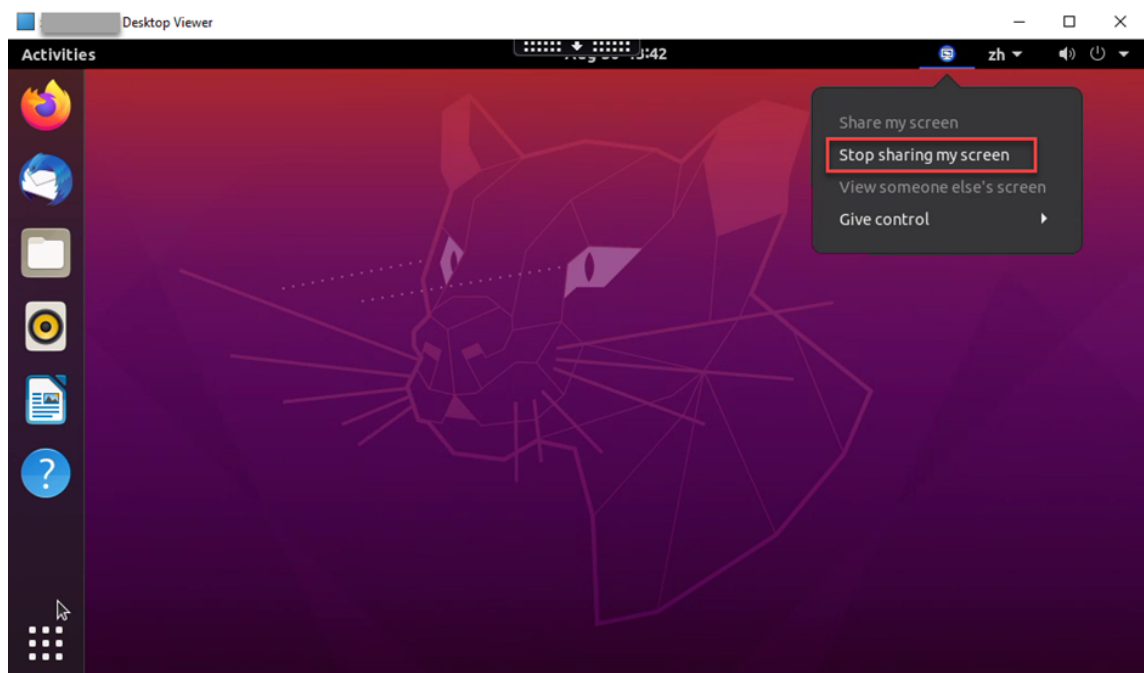
Tipp:

Während der Bildschirmfreigabe ist Ihr Bildschirm rot umrandet.

3. Teilen Sie den kopierten Code mit Sitzungsbenutzern auf anderen virtuellen Desktops, für die Sie Ihren Bildschirm freigeben möchten.
4. Damit ein anderer Benutzer Ihren Bildschirm steuern kann, wählen Sie **Steuerung übergeben** und dann den Namen des Benutzers. Um die Steuerungsübergabe zu beenden, löschen Sie den Namen des Benutzers.

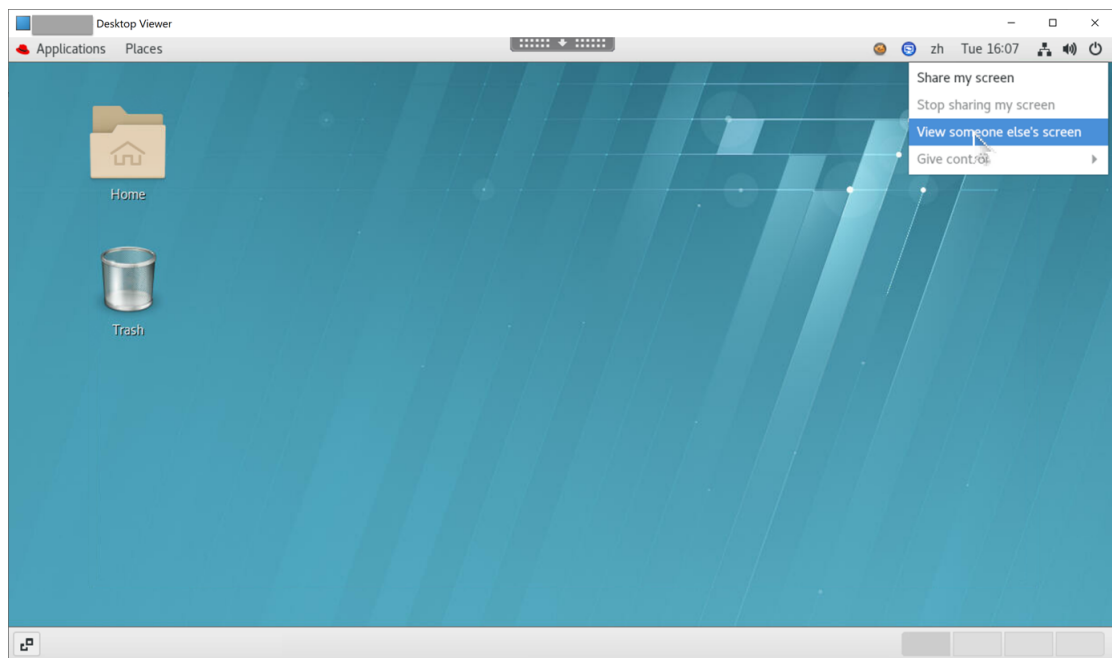


5. Um die Bildschirmfreigabe zu beenden, wählen Sie **Bildschirmfreigabe stoppen**.

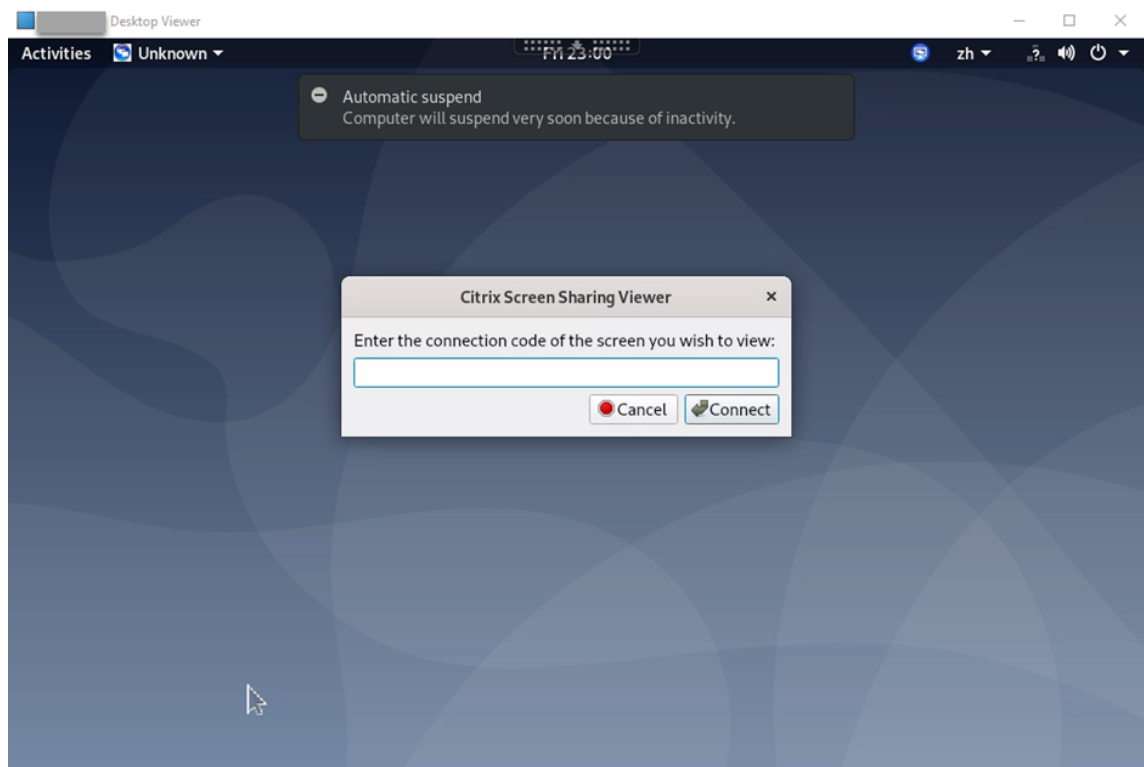


Bildschirm einer anderen Person anzeigen:

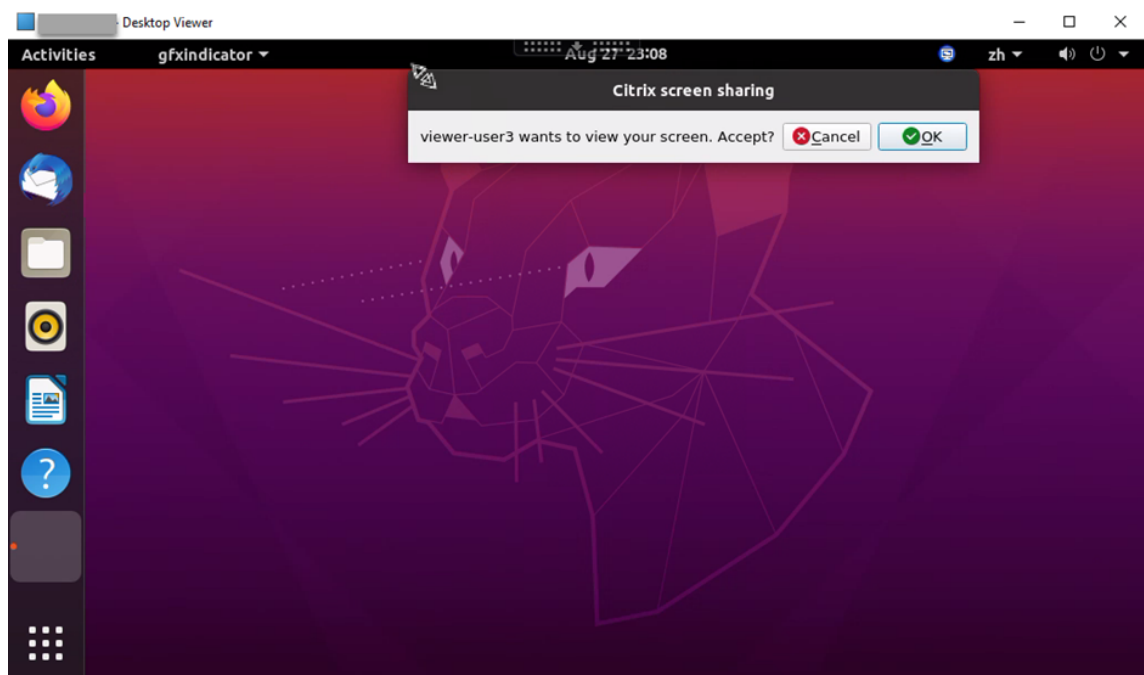
1. Klicken Sie im Infobereich Ihres virtuellen Desktops auf das Symbol für die **Bildschirmfreigabe** und wählen Sie **Bildschirm einer anderen Person anzeigen**.



2. Geben Sie den Verbindungscode des anzuzeigenden Bildschirms ein und klicken Sie auf **Verbinden**.

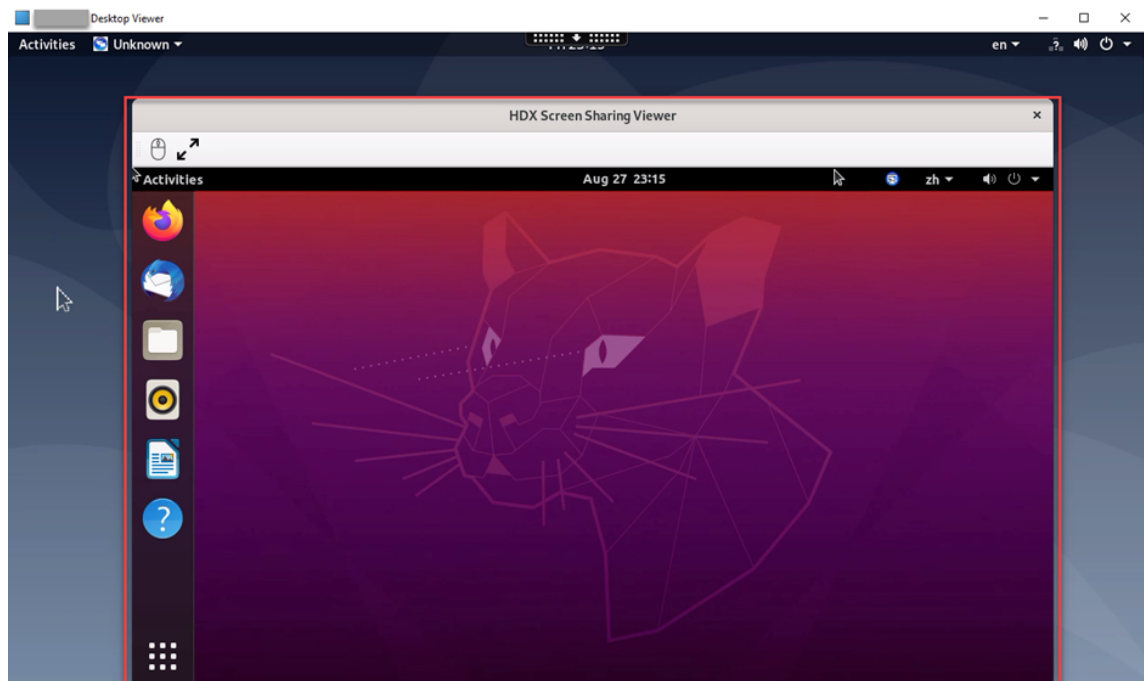


3. Warten Sie, bis der andere Benutzer Ihre Anforderung akzeptiert. Beispiel:



Tipp:

- Der Besitzer des freizugebenden Bildschirms erhält vom Linux-System eine Benachrichtigung zu Ihrer Anforderung.
 - Wenn der andere Benutzer Ihre Anforderung nicht innerhalb von 30 Sekunden akzeptiert, läuft sie ab und es wird eine Eingabeaufforderung angezeigt.
4. Wenn der Benutzer Ihre Anforderung durch Klicken auf **OK** akzeptiert, wird der freigegebene Bildschirm in Ihrem Desktop Viewer angezeigt. Sie sind als Leseberechtigter mit automatisch zugewiesenem Benutzernamen verbunden.

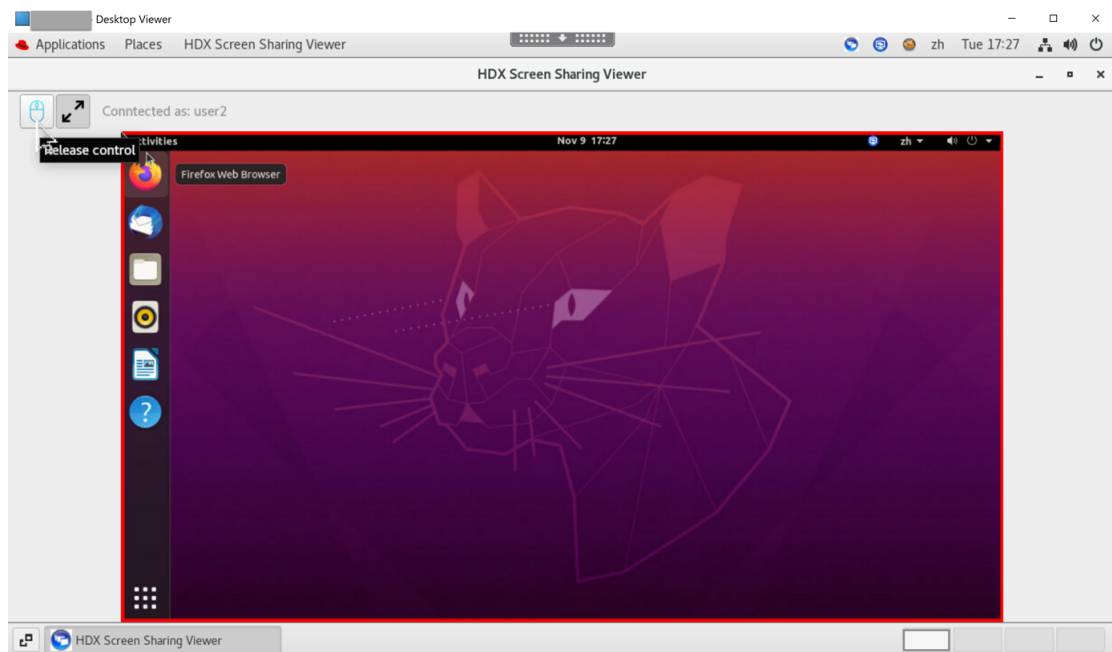


5. Um die Steuerung des freigegebenen Bildschirms anzufordern, klicken Sie links oben auf das Maussymbol.

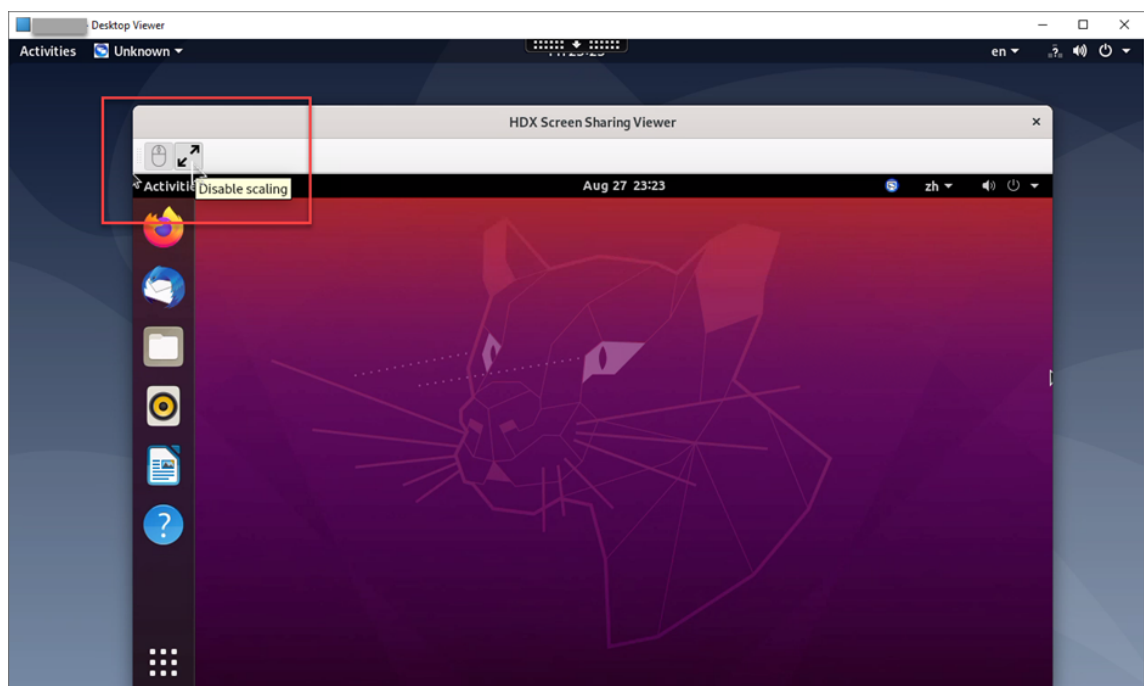
Tipp:

- Wenn der Besitzer des freizugebenden Bildschirms Ihre Anforderung nicht innerhalb von 30 Sekunden akzeptiert, läuft sie ab.
- Ein freigegebener Bildschirm kann nur von jeweils einem Leseberechtigten gesteuert werden.

Klicken Sie erneut auf das Maussymbol, um die Steuerung einer Bildschirmfreigabe abzugeben.



6. Um die Anzeigeskalierung zu deaktivieren oder auf die Fenstergröße zu skalieren, klicken Sie auf das Symbol neben dem Maussymbol.



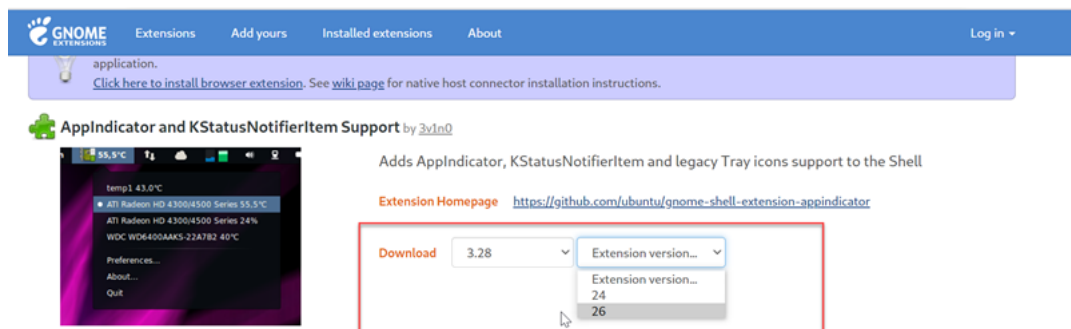
Konfiguration

Die Bildschirmfreigabe ist standardmäßig deaktiviert. Um sie zu aktivieren, legen Sie die folgenden Einstellungen fest:

1. Aktivieren Sie die Richtlinie zur Grafikstatusanzeige in Citrix Studio.
2. Für Citrix Virtual Apps and Desktops 2112 und höher aktivieren Sie die Richtlinie **Bildschirmfreigabe** in Citrix Studio.
3. (Optional) Für Citrix Virtual Apps and Desktops 2109 und früher aktivieren Sie die Bildschirmfreigabe auf dem Linux VDA, indem Sie folgenden Befehl ausführen:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -v "
   EnableScreenSharing" -d "0x00000001"
2 <!--NeedCopy-->
```

4. Erlauben Sie den Zugriff auf die Ports 52525—52625 in Ihrer Firewall.
5. (Optional) Bei Verwendung von mit GNOME installiertem RHEL 8.x, Debian 11 oder SUSE 15.x installieren Sie eine kompatible Erweiterung für die GNOME-Shell, um die AppIndicator-Unterstützung zu aktivieren:
 - a) Führen Sie den Befehl `gnome-shell --version` aus, um Ihre GNOME-Shellversion zu überprüfen.
 - b) Laden Sie eine kompatible Erweiterung für die GNOME-Shell von <https://extensions.gnome.org/extension/615/appindicator-support> herunter. Wenn Ihre Shellversion beispielsweise 3.28 ist, können Sie 24 oder 26 als Erweiterungsversion auswählen.



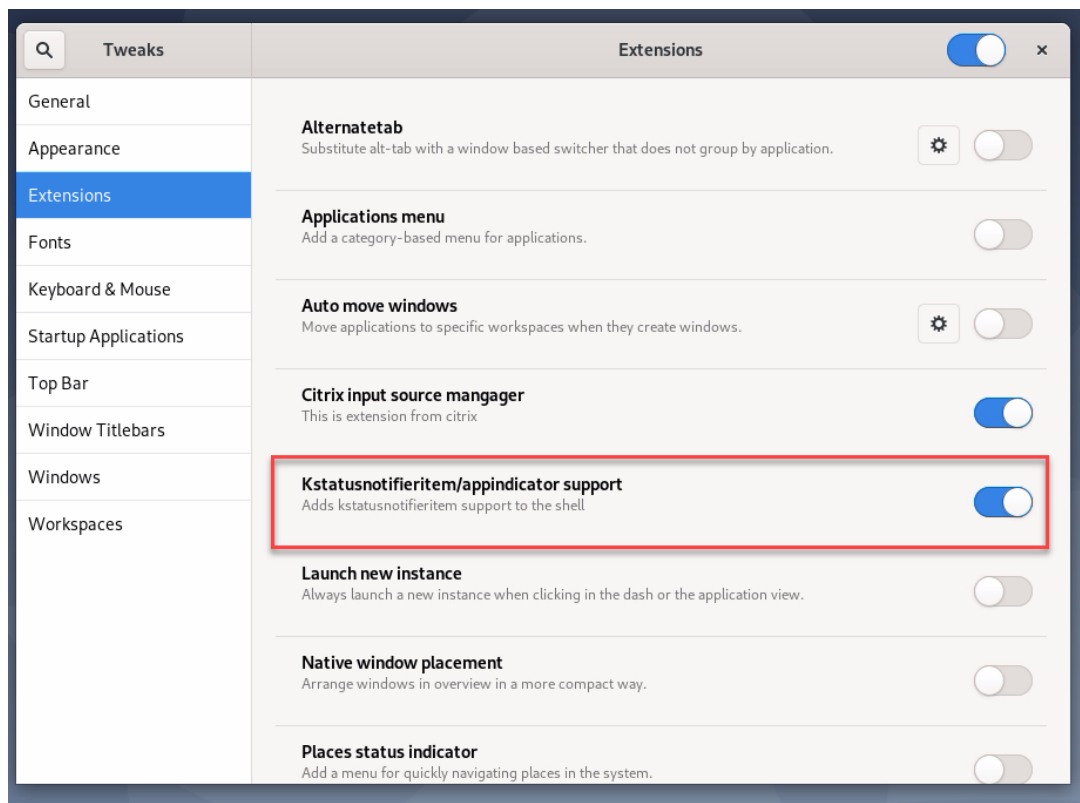
- c) Entpacken Sie das heruntergeladene TAR-Paket. Stellen Sie sicher, dass der Wert “**uuid**” in der Datei **metadata.json** im Paket auf **appindicatorsupport@rgcjonas.gmail.com** gesetzt ist.
- d) Führen Sie den Befehl `mv` aus, um das Verzeichnis **appindicatorsupport@rgcjonas.gmail.com** unter `/usr/share/gnome-shell/extensions/` zu speichern.
- e) Führen Sie den Befehl `chmod a+r metadata.json` aus, um die Datei **metadata.json** für andere Benutzer lesbar zu machen.

Tipp:

Die Datei **metadata.json** im Verzeichnis **appindicatorsupport@rgcjonas.gmail.com**

kann standardmäßig nur vom Root-Benutzer gelesen werden. Um die Bildschirmfreigabe zu unterstützen, machen Sie die Datei **metadata.json** auch für andere Benutzer lesbar.

- f) Installieren Sie GNOME Tweaks.
 - g) Laden Sie in der Desktopumgebung Ihre GNOME-Shell neu, indem Sie nacheinander die Tasten **Alt+F2**, **r** und **Enter** drücken oder aber den Befehl `killall -SIGQUIT gnome-shell` ausführen.
 - h) Führen Sie in der Desktopumgebung GNOME Tweaks aus und aktivieren Sie **KStatusNotifierItem/AppIndicator Support** im Tweaks-Tool.
6. (Optional) Bei Verwendung von mit GNOME installiertem Debian 10 führen Sie die folgenden Schritte aus, um GNOME-Taskleistensymbole zu installieren und zu aktivieren:
- a) Führen Sie den Befehl `sudo apt install gnome-shell-extension-appindicator` aus. Sie müssen sich möglicherweise abmelden und erneut anmelden, damit die Erweiterung von GNOME erkannt wird.
 - b) Suchen Sie im Bildschirm **Activities** nach Tweaks.
 - c) Wählen Sie im Tweaks-Tool **Extensions**.
 - d) Aktivieren Sie **Kstatusnotifieritem/appindicator support**.



Überlegungen

- Der H.265-Videocodec wird von der Bildschirmfreigabe nicht unterstützt.
- Die Bildschirmfreigabe ist für App-Sitzungen nicht verfügbar.
- Benutzer von Desktopsitzungen können ihre Sitzungsbildschirme standardmäßig für bis zu 10 Leseberechtigte freigeben. Die maximale Anzahl von Leseberechtigten ist über `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -v "ScreenSharingViewerMaxNum" -d <hex_value>` konfigurierbar. Wenn die maximale Anzahl erreicht ist, wird eine Meldung angezeigt, wenn Benutzer versuchen, zusätzliche Verbindungsanforderungen anzunehmen.

Nicht-vGPU-Grafikkarten

March 13, 2024

Nicht-vGPU-Grafikkarten bezieht sich auf Grafikkarten, die die virtuelle NVIDIA GPU (vGPU)-Lösung nicht unterstützen. Dieser Artikel enthält Informationen zum Verwenden von Nicht-vGPU-Grafikkarten.

Voraussetzungen

Zum Verwenden von Nicht-vGPU-Grafikkarten:

- 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 7: Einrichten der Laufzeitumgebung für die Installation](#).

Konfiguration

Anpassen von Xorg-Konfigurationsdateien

Für NVIDIA-Grafikkarten Wenn Sie einen NVIDIA-Treiber verwenden, werden die Konfigurationsdateien automatisch installiert und festgelegt.

Für andere Grafikkarten Sie müssen die vier Vorlagenkonfigurationsdateien ändern, die unter `/etc/X11/` installiert sind :

- `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 Kartenherstellers. Es wird eine native Konfigurationsdatei erstellt. Stellen Sie sicher, dass Ihre Karte in einer lokalen Umgebung mit der nativen Konfigurationsdatei funktioniert, wenn Sie keine Linux VDA-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 von Nicht-vGPU-Grafiken

Das Feature für Nicht-vGPU-Grafiken ist standardmäßig deaktiviert. Führen Sie zum Aktivieren folgenden Befehl aus, mit dem `XDamageEnabled` auf den Wert 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-->
```

Ausblenden des Bildschirms für VDAs mit Remote-PC-Zugriff

Der Linux VDA unterstützt das Ausblenden physischer Monitore für VDAs mit Remote-PC-Zugriff, die Nicht-vGPU-Karten verwenden. Durch diese Verbesserung wird die Grafikanzeige auf virtuelle Monitore mit Extensible Virtual Display Interface (EVDI) ausgelagert.

Hinweis:

Die Höchstanzahl virtueller EVDI-Monitore variiert je nach Distribution.

Das Ausblenden des Bildschirms funktioniert für VDAs mit Ubuntu 20.04, Debian 11.3 und Debian 10.9. Führen Sie die folgenden Schritte aus, um den Bildschirm auszublenden:

1. Installieren Sie das `evdi-dkms`-Paket gemäß Ihrer Linux-Distribution:

```
1 sudo apt install evdi-dkms
2 <!--NeedCopy-->
```

2. Aktivieren Sie das Auslagern der Grafikanzeige auf EVDI:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
  CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
  Evdi" -d "0x00000001" --force
2 <!--NeedCopy-->
```

3. Deaktivieren Sie bei Verwendung einer Intel-Grafikkarte den Anzeigemanager. Andernfalls ist die Intel-Karte vom Anzeigemanager belegt und für Citrix Remotesitzungen nicht verfügbar.

```
1 sudo systemctl disable --now gdm
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.

Sitzungswasserzeichen

October 5, 2022

Sitzungswasserzeichen helfen bei der Verhinderung und Verfolgung von Datendiebstahl. Verfolgbare Informationen erscheinen auf den Sitzungsdesktops als Abschreckung für Benutzer, die Daten per Foto oder Screenshot stehlen möchten. Sie können ein Wasserzeichen als Textebene oder als PNG-Bild mit Alphakanal angeben. Das Wasserzeichen wird über dem gesamten Sitzungsbildschirm angezeigt, ohne das Originaldokument zu ändern.

Wichtig:

Sitzungswasserzeichen sind kein Sicherheitsfeature. Sie verhindern einen Datendiebstahl nicht vollständig, bieten jedoch ein gewisses Maß an Abschreckung und Rückverfolgbarkeit. Bei Verwendung des Features kann keine vollständige Rückverfolgbarkeit von Informationen garantiert werden. Es wird jedoch empfohlen, dieses Feature nach Bedarf mit anderen Sicherheitslösungen zu kombinieren.

Sitzungswasserzeichen enthalten Informationen zur Rückverfolgung von Datendiebstahl. Die wichtigste Angabe ist die Identität des angemeldeten Benutzers, in dessen Sitzung das Bildschirmbild erstellt wurde. Zur besseren Rückverfolgung von Datenlecks sollten Sie weitere Informationen wie die IP-Adresse des Servers oder des Clients und die Verbindungszeit einschließen.

Um die Benutzererfahrung anzupassen, verwenden Sie die folgenden Einstellungen der Richtlinie "Sitzungswasserzeichen", um die Platzierung und Erscheinung von Wasserzeichen auf dem Bildschirm zu konfigurieren.

Sitzungswasserzeichen - Richtlinieneinstellungen

Aktivieren von Sitzungswasserzeichen

Wenn Sie diese Einstellung aktivieren, werden Sitzungen mit einem undurchsichtigen Wasserzeichen angezeigt, das sitzungsspezifische Informationen enthält. Die anderen Wasserzeicheneinstellungen hängen davon ab, dass dieses aktiviert ist.

Standardmäßig ist das Sitzungswasserzeichen deaktiviert.

Client-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die aktuelle Client-IP-Adresse als Wasserzeichen angezeigt.

Standardmäßig ist die Option **Client-IP-Adresse einschließen** deaktiviert.

Verbindungszeit einschließen

Wenn Sie diese Einstellung aktivieren, wird im Sitzungswasserzeichen eine Verbindungszeit angezeigt. Das Format ist JJJJ/MM/TT hh:mm. Die angezeigte Zeit basiert auf der Systemuhr und der Zeitzone.

Standardmäßig ist die Option **Verbindungszeit einschließen** deaktiviert.

Anmeldennamen einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der aktuelle Anmeldename als Wasserzeichen angezeigt. Das Anzeigeformat ist BENUTZERNAME@DOMÄNENNAME. Es wird empfohlen, Benutzernamen auf maximal 20 Zeichen zu beschränken. Wenn ein Benutzernamen mehr als 20 Zeichen hat, werden die Zeichen evtl. kleiner angezeigt oder abgeschnitten und die Wirksamkeit des Wasserzeichens verringert.

Standardmäßig ist **Anmeldebenutzernamen einschließen** aktiviert.

VDA-Hostnamen einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der VDA-Hostname der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Standardmäßig ist **VDA-Hostnamen einschließen** aktiviert.

VDA-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die VDA-IP-Adresse der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Standardmäßig ist die Option **Client-IP-Adresse einschließen** deaktiviert.

Sitzungswasserzeichenstil

Diese Einstellung steuert, ob eine einzelne oder mehrere Wasserzeichenbeschriftungen angezeigt werden sollen. Wählen Sie in dem Dropdownmenü "Wert" die Option **Einzeln** oder **Mehrere**. Informationen zu weiteren Stiloptionen finden Sie im Abschnitt **Benutzerdefinierter Wasserzeichentext** in diesem Artikel.

Bei Auswahl von **Mehrere** werden fünf Wasserzeichenbeschriftungen in der Sitzung angezeigt: eine in der Mitte und vier in den Ecken.

Bei Auswahl von **Einzeln** wird nur eine Wasserzeichenbeschriftung in der Mitte angezeigt.

Standardmäßig ist für **Sitzungswasserzeichenstil** die Option **Mehrere** ausgewählt.

Wasserzeichentransparenz

Sie können eine Wasserzeichendeckkraft von 0–100 angeben. Je größer der Wert, desto deckender ist das Wasserzeichen.

Der Standardwert ist 17.

Benutzerdefinierter Wasserzeichentext

Der Wert ist standardmäßig leer. Sie können eine nicht leere Zeichenfolge eingeben, eine Syntax festlegen, um eine Zeichenfolge zu bilden, oder die Kombination zur Anzeige im Sitzungswasserzeichen verwenden. Nicht leere Zeichenfolgen unterstützen bis zu 25 Unicode-Zeichen pro Zeile. Längere Zeichenfolgen werden auf 25 Zeichen gekürzt.

Sie können die Richtlinie beispielsweise auf den folgenden Wert festlegen:

```
<date> <time><newline><username><style=single><fontsize=40><font=
Ubuntu><position=center><rotation=0><newline><serverip><newline><
clientip><newline>Citrix Linux VDA<newline>Version 2207
```

Eine Beschreibung aller Syntaxoptionen finden Sie in der folgenden Tabelle:

Syntaxoption	Beschreibung	Gültige Einstellung (Groß- /Kleinschreibung beachten)	Standardwert	Bemerkungen
<style>	Layoutstil für Wasserzeichen	xstyle, single, tile, horizontal	xstyle	-
<position>	Wasserzeichenposition	center, topleft, topright, bottomleft, bottomright	center	Nur gültig, wenn der Layoutstil auf Einzeln festgelegt ist.
<rotation>	Drehung des Wasserzeichens um einen bestimmten Winkel	-180–180	0	-

Syntaxoption	Beschreibung	Gültige Einstellung (Groß- /Kleinschreibung beachten)	Standardwert	Bemerkungen
< transparency >	Wasserzeichendeckkraft	0–100	17	-
	-	Eine vom System unterstützte Schriftart	Sans	-
<fontsize>	-	20–50	0 (automatisch berechnet)	-
<fontzoom>	Prozentsatz der von Ihnen über <fontsize> und <image> eingestellten Schrift- und Bildgrößen	0 –	100	-
<image>	PNG- Wasserzeichen	Pfad zu einem PNG-Bild auf dem VDA	Nicht zutreffend	Diese Syntax konfiguriert ein PNG- Wasserzeichen. Nur PNG mit Alphakanal wird unterstützt. Bei Verwendung eines PNG- Wasserzeichens können nur die Syntaxoptionen <style>, <position>, <rotation>,< transparency > und <fontzoom> wirksam sein.

Syntaxoption	Beschreibung	Gültige Einstellung (Groß- /Kleinschreibung beachten)	Standardwert	Bemerkungen
<date>	Platzhalter für das Datum der Sitzungsverbindung (JJJJ/MM/TT)	Nicht zutreffend	Nicht zutreffend	-
<time>	Platzhalter für die Uhrzeit der Sitzungsverbindung (HH:MM)	Nicht zutreffend	Nicht zutreffend	-
<domain>	Platzhalter für die Domäne des Benutzerkontos	Nicht zutreffend	Nicht zutreffend	-
<username>	Platzhalter für den aktuellen Anmeldenamen (ohne die Domäne des Benutzerkontos)	Nicht zutreffend	Nicht zutreffend	-
<hostname>	Platzhalter für den Hostnamen des VDAs	Nicht zutreffend	Nicht zutreffend	-
<clientip>	Platzhalter für die Client-IP-Adresse	Nicht zutreffend	Nicht zutreffend	-
<serverip>	Platzhalter für die VDA-IP-Adresse	Nicht zutreffend	Nicht zutreffend	-

Hinweis:

Wenn **Benutzerdefinierter Wasserzeichentext** mit einer gültigen Syntaxeinstellung festgelegt ist, werden alle anderen Richtlinien für Sitzungswasserzeichen außer **Sitzungswasserzeichen aktivieren** ignoriert.

Wenn Sie eine Syntaxoption nicht festlegen oder auf einen nicht unterstützten Wert festlegen, wird ihr Standardwert verwendet.

Einschränkungen

- Sitzungswasserzeichen werden in Sitzungen, in denen die Browserinhaltsumleitung verwendet wird, nicht unterstützt. Wenn Sie Sitzungswasserzeichen verwenden möchten, deaktivieren Sie bitte die Browserinhaltsumleitung.
- Sitzungswasserzeichen werden nicht unterstützt und nicht angezeigt, wenn eine Sitzung im Vollbildmodus mit Hardwarebeschleunigung (H.264- oder H.265-Codierung) mit Legacy-NVIDIA-Treibern ausgeführt wird. (In diesem Fall ist `NvCaptureType` in der Registrierung auf 2 festgelegt).
- Wasserzeichen sind für die Sitzungsspiegelung nicht sichtbar.
- Wenn Sie die Taste Druck/S-Abf drücken, um eine Bildschirmaufnahme zu erstellen, enthält diese VDA-seitig kein Wasserzeichen. Es wird empfohlen, Maßnahmen zu ergreifen, damit Bildschirmaufnahmen nicht kopiert werden.

Progressive Anzeige für Thinwire

October 5, 2022

Die Sitzungsinteraktivität kann sich bei Verbindungen mit niedriger Bandbreite oder hoher Latenz verschlechtern. Das Scrollen auf einer Webseite kann dann beispielsweise langsam oder abgehakt sein oder nicht funktionieren. Tastatur- und Mausoperationen können hinter Grafikaktualisierungen zurückbleiben.

Bis Version 7.17 konnten Sie den Bandbreitenverbrauch über Richtlinieneinstellungen verringern, indem Sie für Sitzungen eine **niedrige** Bildqualität oder geringere Farbtiefe (16- oder 8-Bit-Grafik) festlegten. Sie mussten jedoch wissen, dass ein Benutzer eine schwache Verbindung nutzte. HDX Thinwire hat die Qualität statischer Bilder nicht je nach Netzwerkbedingungen dynamisch angepasst.

Ab Version 7.18 wechselt HDX Thinwire standardmäßig in einen progressiven Aktualisierungsmodus, wenn eine der folgenden Situationen vorliegt:

- Die verfügbare Bandbreite fällt unter 2 MBit/s.
- Die Netzwerklatenz überschreitet 200 ms.

In diesem Modus gilt:

In der folgenden Beispielgrafik mit aktivierter progressiver Aktualisierung sieht man blaue Artefakte an den Buchstaben **F** und **e** und das Bild ist stark komprimiert. Durch dieses Verfahren wird der Bandbreitenverbrauch erheblich reduziert, sodass Bilder und Text schneller empfangen werden und die Interaktivität der Sitzung sich verbessert.

Features



Sobald Sie die Interaktion mit der Sitzung beenden, werden die unscharf angezeigten Bilder und Textsegmente kontinuierlich optimiert, bis sie verlustfrei sind. In der folgenden Beispielgrafik zeigen die Buchstaben keine blauen Artefakte mehr und das Bild erscheint in Originalqualität.

Features



Für Bilder wird beim Scharfzeichnen eine zufällige blockartige Methode verwendet. Für Text werden einzelne Buchstaben oder Wortteile geschärft. Das Scharfzeichnen erfolgt über mehrere Frames hinweg. Dies vermeidet Bildverzögerungen, die durch das Scharfzeichnen eines einzelnen großen Frames auftreten würden.

Bewegliche Bilder (Video) werden weiterhin per adaptive Anzeige oder selektives H.264 verarbeitet.

Verwendung des progressiven Modus

Standardmäßig ist der progressive Modus auf Standby für die Einstellungen der Richtlinie für **Bildqualität** auf **Hoch**, **Mittel** (Standard) und **Niedrig** festgelegt.

Der progressive Modus ist in folgenden Situationen deaktiviert:

- **Bildqualität = Immer verlustfrei** oder **Zu verlustfrei verbessern**
- **Bevorzugte Farbtiefe für einfache Grafiken** = 8-Bit
- **Videocodec zur Komprimierung verwenden** = **Für den gesamten Bildschirm** (wenn Vollbild-H.264 gewünscht wird)

Wenn der progressive Modus auf Standby ist, wird er standardmäßig aktiviert, wenn eine der folgenden Bedingungen eintritt:

- Die verfügbare Bandbreite fällt unter 2 MBit/s.
- Die Netzwerklatenz steigt über 200 ms.

Nach einem Moduswechsel bleibt der neue Modus mindestens 10 Sekunden aktiv, selbst wenn die ungünstigen Netzwerkbedingungen nur vorübergehend sind.

Ändern des progressiven Modusverhaltens

Sie können das progressive Modusverhalten ändern, indem Sie den folgenden Befehl ausführen:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\  
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "  
    ProgressiveDisplay" -d "<value>" --force  
2 <!--NeedCopy-->
```

Wobei <value> Folgendes angibt:

0 = Immer deaktiviert (niemals verwenden)

1 = Automatisch (Umschalten je nach Netzwerkbedingungen, Standardwert)

2 = Immer aktiviert

Im automatischen Modus (1) können Sie über einen der folgenden Befehle die Schwellenwerte ändern, bei denen ein Moduswechsel erfolgt:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\  
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "  
    ProgressiveDisplayBandwidthThreshold" -d "<value>" --force  
2 <!--NeedCopy-->
```

<value> ist der <Schwellenwert in KBit/s> (Standardwert = 2.048)

Beispiel: 4096 = progressiven Modus einschalten, wenn die Bandbreite unter 4 MBit/s fällt

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\  
    \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "  
    ProgressiveDisplayLatencyThreshold" -d "<value>" --force  
2 <!--NeedCopy-->
```

<value> ist der <Schwellenwert in ms> (Standardwert = 200)

Beispiel: 100 = progressiven Modus einschalten, wenn die Netzwerklatenz unter 100 ms fällt.

Tastatur

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Client-IME](#)
- [Synchronisierung der Client-IME-Benutzeroberfläche](#)
- [Dynamische Tastaturlayoutsynchronisierung](#)
- [Bildschirmtastatur](#)
- [Unterstützung der Eingabe in mehreren Sprachen](#)

Client-Eingabemethoden-Editor (IME)

October 5, 2022

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 Citrix Virtual Apps- oder Citrix Virtual Desktops-Sitzung.

Ändern Sie die Eingabemethode nach Bedarf auf der Clientseite, um das IME-Feature zu verwenden.

Bekannte Probleme

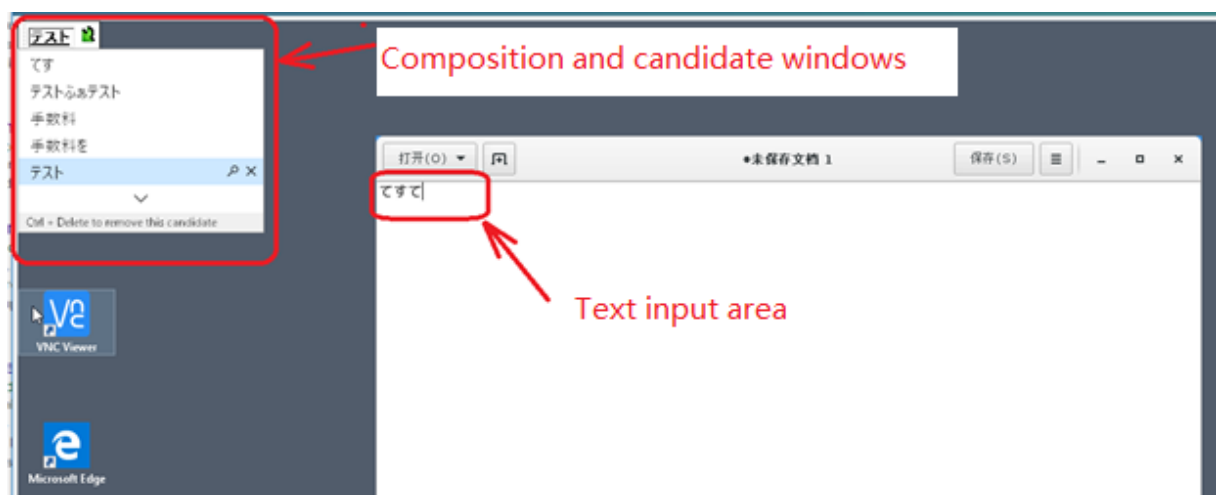
- Sie müssen auf eine Zelle in einer Google-Kalkulationstabelle doppelklicken, damit Sie mit dem Client-IME-Feature Zeichen in die Zelle eingeben können.
- Das Client-IME-Feature wird in Kennwortfeldern nicht automatisch deaktiviert.
- Die IME-Benutzerschnittstelle folgt nicht dem Cursor im Eingabebereich.

Synchronisierung der Client-IME-Benutzeroberfläche

October 5, 2022

Übersicht

Bislang befand sich die Client-IME-Benutzeroberfläche (einschließlich Kompositionsfenster und Kandidatenfenster) in der linken oberen Ecke des Bildschirms. Sie folgte dem Cursor nicht und war unter Umständen weit von ihm entfernt im Texteingabebereich.



Citrix bietet für die Client-IME mehr Benutzerfreundlichkeit und eine optimierte Anwendung:



Voraussetzungen für die Verwendung des Features

1. Aktivieren Sie Intelligent Input Bus (IBus) auf dem Linux VDA. Informationen zum Aktivieren von IBus auf einem Linux-Betriebssystem finden Sie in der Betriebssystemdokumentation des Herstellers. Beispiel:
 - Ubuntu: <https://help.ubuntu.com/community/ibus>
 - CentOS, RHEL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods
 - Debian: <https://wiki.debian.org/I18n/ibus>
 - SUSE: <https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang>
2. Das Feature wird automatisch installiert, Sie müssen es jedoch vor der Verwendung aktivieren.

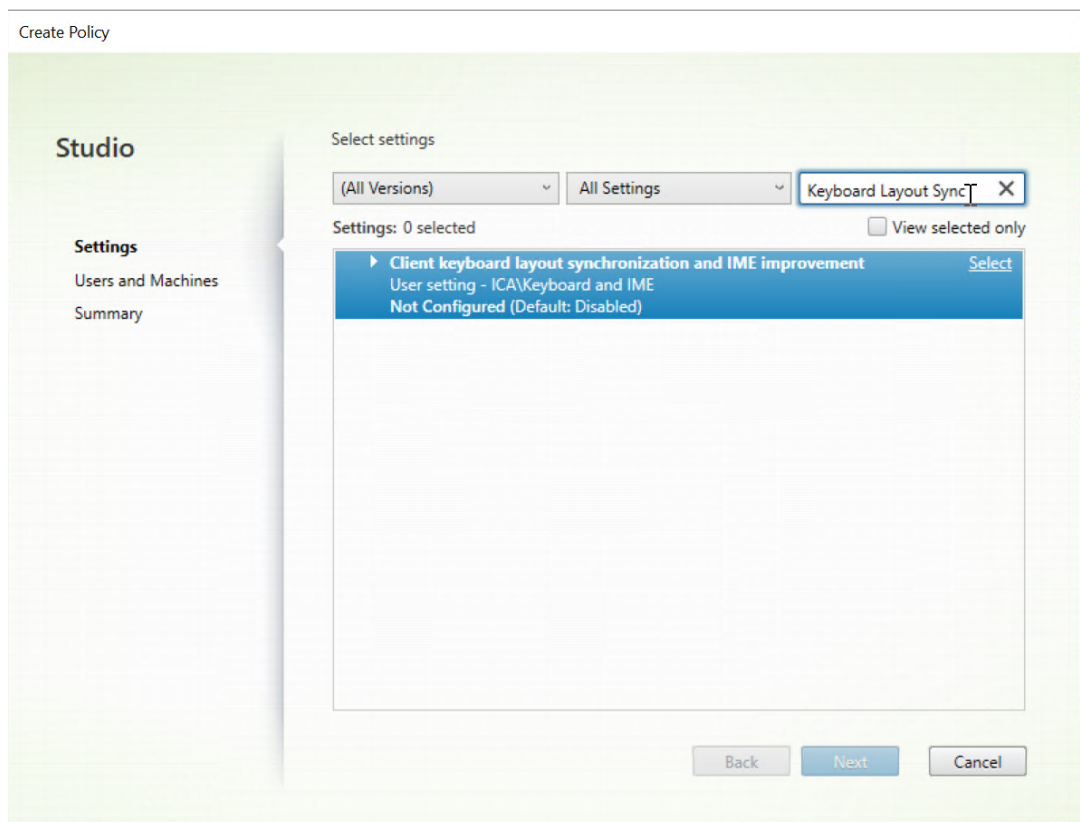
Aktivieren und Deaktivieren des Features

Die Synchronisierung der Client-IME-Benutzeroberfläche ist standardmäßig deaktiviert. Um das Feature zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, oder bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg`.

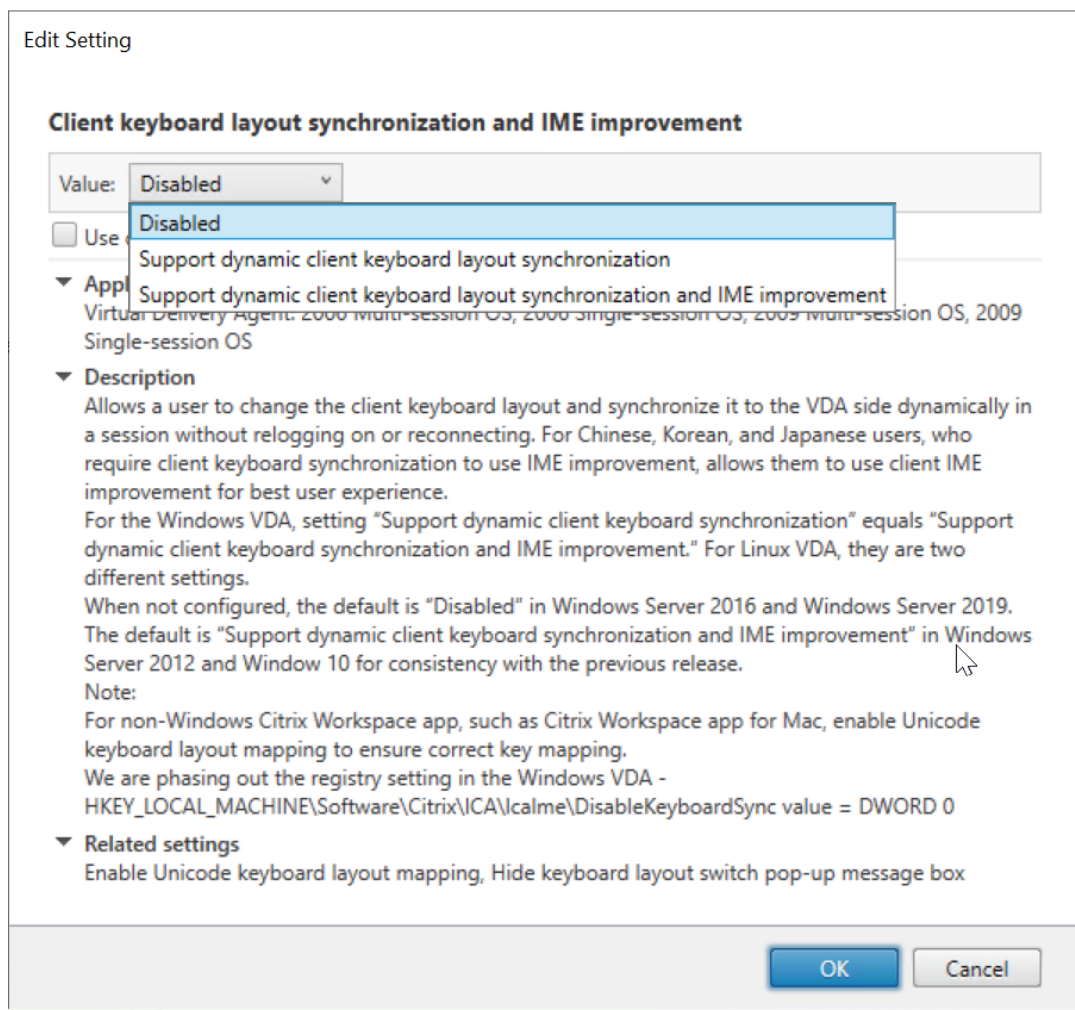
Hinweis:

Die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Maschinenobjekte oder auf alle Objekte in Ihrer Site angewendet werden. Registrierungseinstellungen auf einem bestimmten Linux VDA gelten für alle Sitzungen auf diesem VDA.

- Legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, um die Synchronisierung der Client-IME-Benutzeroberfläche zu aktivieren oder zu deaktivieren:
 1. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.
 2. Suchen Sie nach der Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME**.



3. Klicken Sie neben dem Richtliniennamen auf **Auswählen**.
4. Legen Sie die Richtlinie fest.



Es stehen drei Optionen zur Verfügung:

- **Deaktiviert:** Deaktiviert die dynamische Tastaturlayoutsynchronisierung und die Synchronisierung der Client-IME-Benutzeroberfläche
 - **Dynamische Client-Tastaturlayoutsynchronisierung unterstützen:** Aktiviert die dynamische Tastaturlayoutsynchronisierung unabhängig vom DWORD-Wert des Registrierungsschlüssels **SyncKeyboardLayout** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
 - **Dynamische Client-Tastaturlayoutsynchronisierung und Verbesserung des IME unterstützen:** Aktiviert sowohl die dynamische Tastaturlayoutsynchronisierung als auch die Synchronisierung der Client-IME-Benutzeroberfläche unabhängig von den DWORD-Werten der Registrierungsschlüssel **SyncKeyboardLayout** und **SyncClientIME** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
- Bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg`, um die Synchronisierung der Client-IME-Benutzeroberfläche zu aktivieren oder zu deaktivieren:

Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncClientIME" -d "0x00000001"
2 <!--NeedCopy-->
```

Führen Sie folgenden Befehl aus, um das Feature zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncClientIME" -d "0x00000000"
2 <!--NeedCopy-->
```

Dynamische Tastaturlayoutsynchronisierung

October 5, 2022

Bisher musste das Tastaturlayout auf dem Linux VDA mit dem auf dem Clientgerät identisch sein. Probleme bei der Tastenzuordnung konnten beispielsweise auftreten, wenn das Tastaturlayout auf dem Clientgerät von Englisch auf Deutsch geändert wurde, nicht jedoch auf dem VDA.

Das Problem wurde von Citrix behoben. Das Tastaturlayout des VDA wird automatisch mit dem des Clientgeräts synchronisiert. Jedes Mal, wenn sich das Tastaturlayout auf dem Clientgerät ändert, ändert sich das Layout auf dem VDA entsprechend mit.

Hinweis:

Die Citrix Workspace-App für HTML5 bietet keine Unterstützung für die dynamische Tastaturlayoutsynchronisierung.

Konfiguration

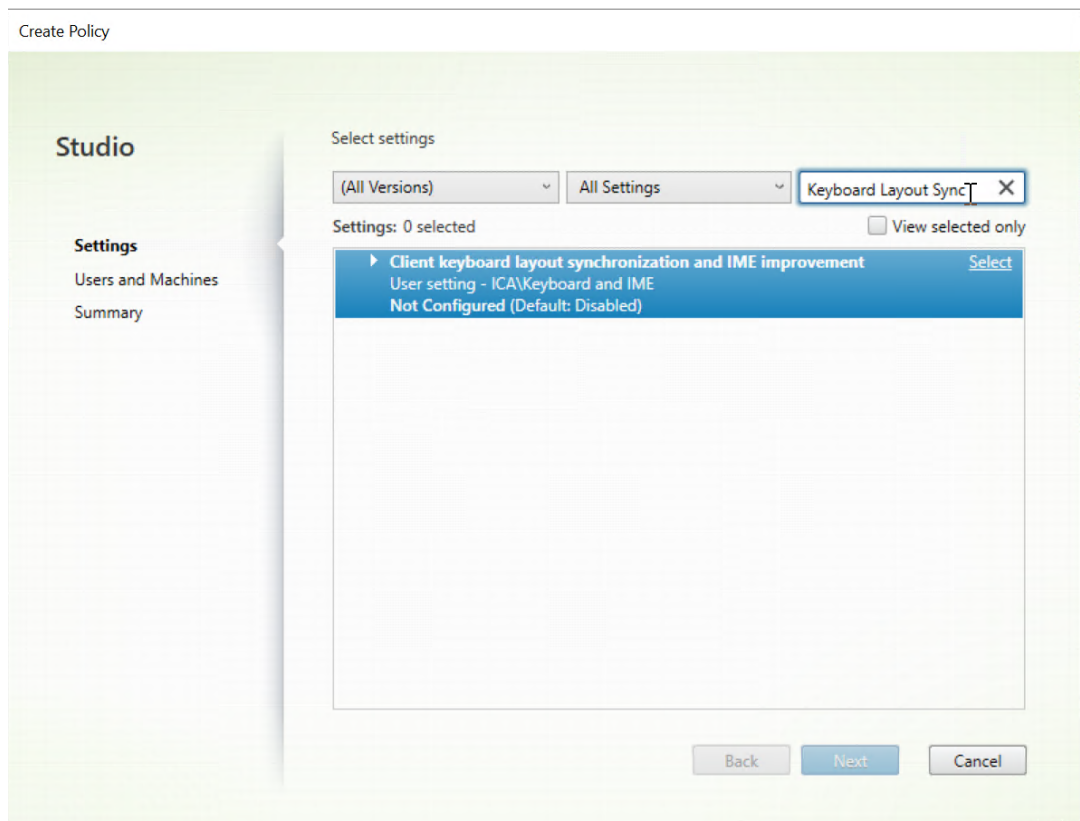
Die dynamische Tastaturlayoutsynchronisierung ist standardmäßig deaktiviert. Um das Feature zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, oder bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg`.

Hinweis:

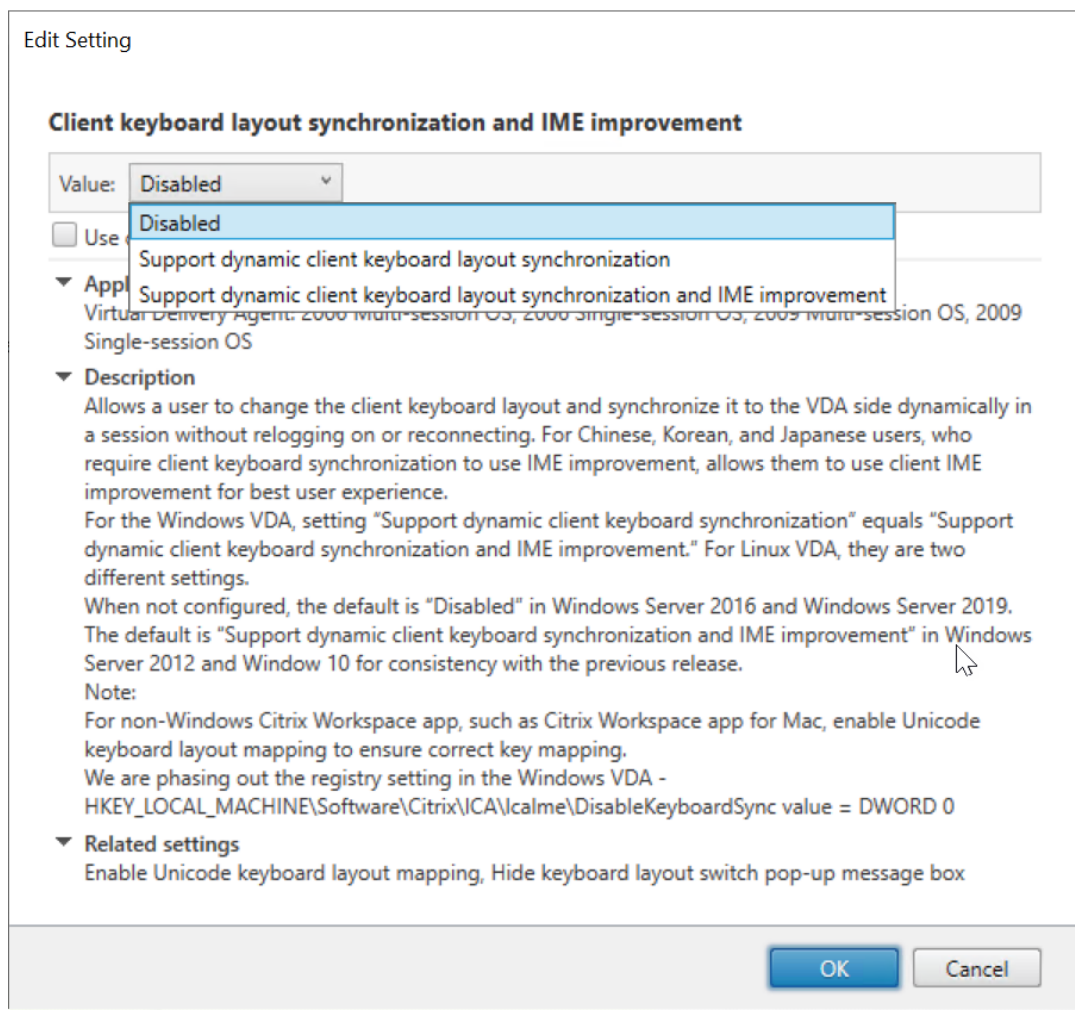
Die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Maschinenobjekte oder auf alle Objekte in Ihrer Site angewendet werden. Registrierungseinstellungen

auf einem bestimmten Linux VDA gelten für alle Sitzungen auf diesem VDA.

- Legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, um die dynamische Tastaturlayoutsynchronisierung zu aktivieren oder zu deaktivieren.
1. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.
 2. Suchen Sie nach der Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME**.



3. Klicken Sie neben dem Richtliniennamen auf **Auswählen**.
4. Legen Sie die Richtlinie fest.



Es stehen drei Optionen zur Verfügung:

- **Deaktiviert:** Deaktiviert die dynamische Tastaturlayoutsynchronisierung und die Synchronisierung der Client-IME-Benutzeroberfläche
 - **Dynamische Client-Tastaturlayoutsynchronisierung unterstützen:** Aktiviert die dynamische Tastaturlayoutsynchronisierung unabhängig vom DWORD-Wert des Registrierungsschlüssels **SyncKeyboardLayout** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
 - **Dynamische Client-Tastaturlayoutsynchronisierung und Verbesserung des IME unterstützen:** Aktiviert sowohl die dynamische Tastaturlayoutsynchronisierung als auch die Synchronisierung der Client-IME-Benutzeroberfläche unabhängig von den DWORD-Werten der Registrierungsschlüssel **SyncKeyboardLayout** und **SyncClientIME** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
- Bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg`, um die dynamische Tastaturlayoutsynchronisierung zu aktivieren oder zu deaktivieren:

Führen Sie folgenden Befehl aus, um dieses Feature zu aktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncKeyboardLayout" -d "0x00000001"
2 <!--NeedCopy-->
```

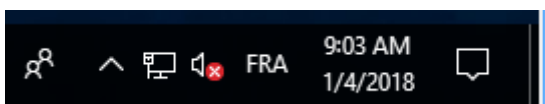
Führen Sie folgenden Befehl aus, um dieses Feature zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncKeyboardLayout" -d "0x00000000"
2 <!--NeedCopy-->
```

Verwendung

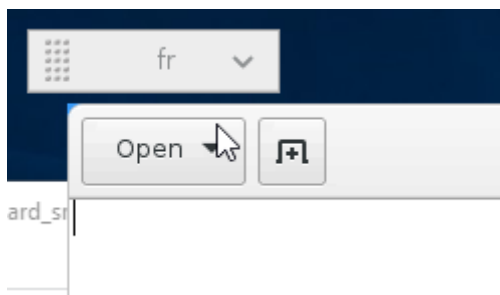
Wenn das Feature aktiviert ist, ändert sich das Tastaturlayout auf dem VDA automatisch zusammen mit dem auf dem Clientgerät.

Wenn Sie beispielsweise das Tastaturlayout auf einem Clientgerät auf Französisch ändern:



Ändert sich das Tastaturlayout der Linux VDA-Sitzung ebenfalls in “fr”.

In Anwendungssitzungen können Sie diese automatische Änderung sehen, wenn Sie die Sprachenleiste aktiviert haben:



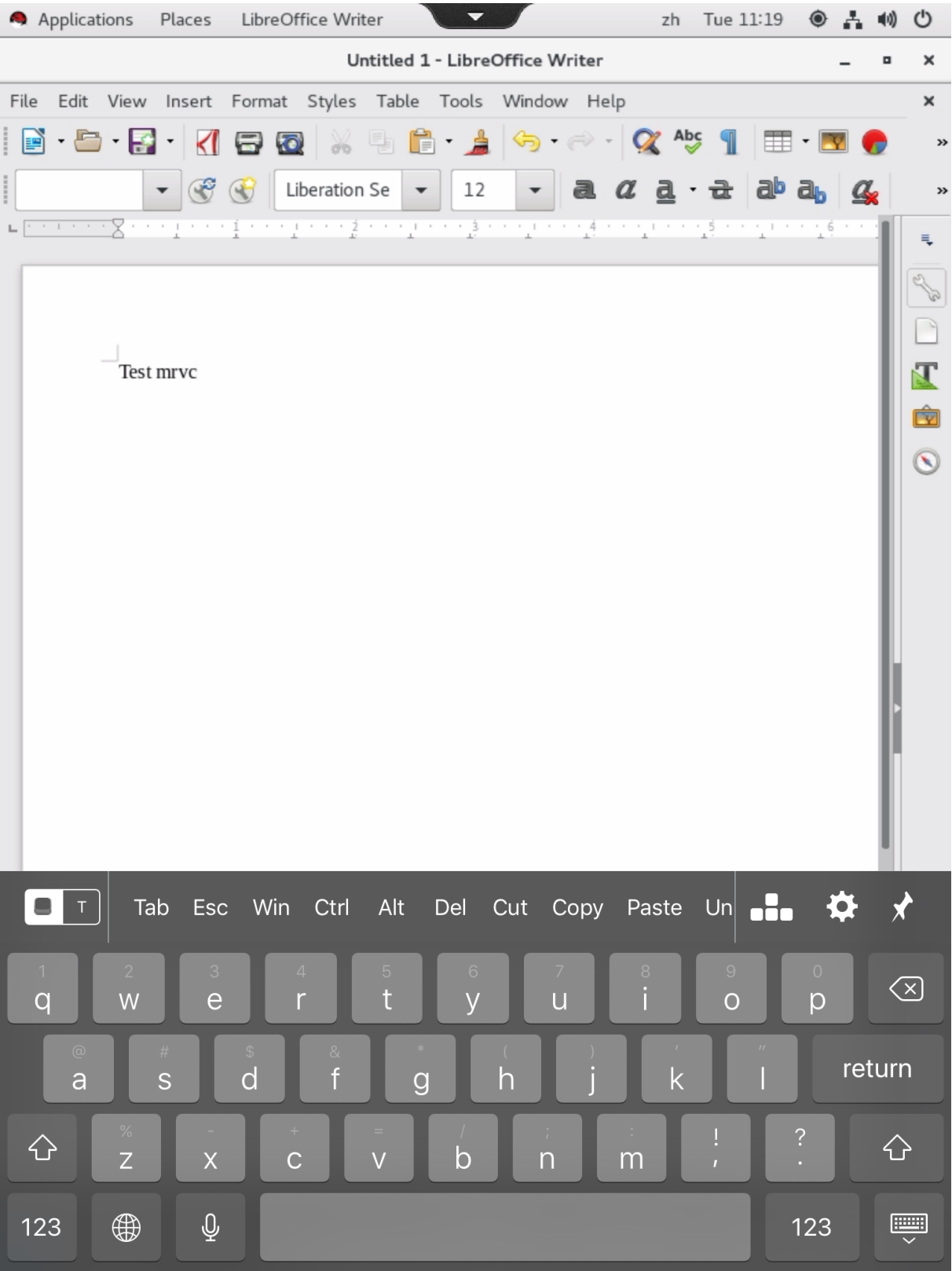
In einer Desktop-Sitzung sehen Sie diese automatische Änderung in der Taskleiste:



Bildschirmtastatur

October 5, 2022

Die Funktion der Bildschirmtastatur ist in einem virtuellen Linux-Desktop oder in einer Anwendungssitzung verfügbar. Die Bildschirmtastatur wird automatisch ein- oder ausgeblendet, wenn Sie auf ein Eingabefeld gehen oder es verlassen.



Hinweis:

Das Feature ist für RHEL 7.9, RHEL 8.2, SUSE 15.3, SUSE 15.2, Ubuntu 18.04 und Ubuntu 20.04 verfügbar. Es wird für die Citrix Workspace-App für iOS und Android unterstützt.

Aktivieren und Deaktivieren des Features

Dieses Feature ist standardmäßig deaktiviert. Sie können es mit dem Hilfsprogramm **ctxreg** aktivieren oder deaktivieren. Die Konfiguration des Features auf einem Linux VDA gilt für alle Sitzungen auf diesem VDA.

Aktivieren des Features:

1. Befehl:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
  CurrentControlSet\Control\Citrix\VirtualChannels\MrVc" -v "
  Enabled" -d "0x00000001"
2 <!--NeedCopy-->
```

2. Legen Sie in Citrix Studio die Richtlinie **Automatische Anzeige der Tastatur** auf **Zulässig** fest.
3. (Optional) Führen Sie für RHEL 7 und CentOS 7 den folgenden Befehl aus, um Intelligent Input Bus (IBus) als den Standard-IM-Dienst zu konfigurieren:

```
1 echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
2 <!--NeedCopy-->
```

Führen Sie folgenden Befehl aus, um das Feature zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
  Control\Citrix\VirtualChannels\MrVc" -v "Enabled" -d "0x00000000"
2 <!--NeedCopy-->
```

Hinweis:

Die vorherigen Einstellungen werden wirksam, wenn Sie sich an einer neuen Sitzung anmelden oder sich bei der aktuellen Sitzung abmelden und wieder anmelden.

Einschränkungen

- Das Feature funktioniert möglicherweise nicht wie erwartet mit Google Chrome, LibreOffice und anderen Apps.
- Um die Bildschirmtastatur wieder anzuzeigen, nachdem sie manuell ausgeblendet wurde, klicken Sie auf ein Nicht-Eingabefeld und dann wieder auf das aktuelle Eingabefeld.

- Die Bildschirmtastatur wird möglicherweise nicht angezeigt, wenn Sie in einem Webbrowser von einem Eingabefeld zu einem anderen klicken. Als Workaround klicken Sie auf ein Nicht-Eingabefeld und dann wieder auf das Zieleingabefeld.
- Das Feature unterstützt keine Unicode-Zeichen und Doppelbyte-Zeichen (z. B. chinesische, japanische und koreanische Zeichen).
- Die Bildschirmtastatur ist für Kennworteingabefelder nicht verfügbar.
- Die Bildschirmtastatur kann das aktuelle Eingabefeld überlappen. Verschieben Sie in diesem Fall das App-Fenster oder scrollen Sie auf dem Bildschirm nach oben, um das Eingabefeld an eine zugängliche Position zu verschieben.
- Aufgrund von Kompatibilitätsproblemen zwischen der Citrix Workspace-App und Huawei-Tablets erscheint die Bildschirmtastatur auf Huawei-Tablets sogar dann, wenn eine physische Tastatur angeschlossen ist.

Unterstützung der Eingabe in mehreren Sprachen

October 5, 2022

Citrix unterstützt ab Linux VDA Version 1.4 auch veröffentlichte Anwendungen. Benutzer können damit auch ohne Linux-Desktopumgebung auf eine gewünschte Linux-Anwendung zugreifen.

Die systemeigene Sprachleiste auf dem Linux VDA war jedoch für veröffentlichte Anwendungen nicht verfügbar, da sie eng in die Linux-Desktopumgebung integriert ist. Daher konnten Benutzer keinen Text in einer Sprache eingeben, für die IME erforderlich ist, z. B. Chinesisch, Japanisch oder Koreanisch. Außerdem war während einer Anwendungssitzung kein Wechsel des Tastaturlayouts möglich.

Dieses Feature bietet nun eine Sprachleiste für veröffentlichte Anwendungen, bei denen eine Texteingabe möglich ist. Über die Sprachleiste können Benutzer einen serverseitigen Eingabemethoden-Editor auswählen und während Anwendungssitzungen das Tastaturlayout wechseln.

Konfiguration

Sie können das Feature mit dem Hilfsprogramm **ctxreg** aktivieren oder deaktivieren (standardmäßig ist es deaktiviert). Die Konfiguration des Features auf einem Linux VDA-Server gilt für alle Anwendungen, die auf diesem VDA veröffentlicht werden.

Der Schlüssel zur Konfiguration ist "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Language", der Typ ist "DWORD".

Führen Sie folgenden Befehl aus, um dieses Feature zu aktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
   x00000001"
2 <!--NeedCopy-->
```

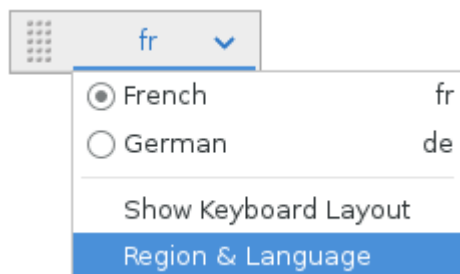
Führen Sie folgenden Befehl aus, um dieses Feature zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
   x00000000"
2 <!--NeedCopy-->
```

Verwendung

Die Verwendung ist einfach.

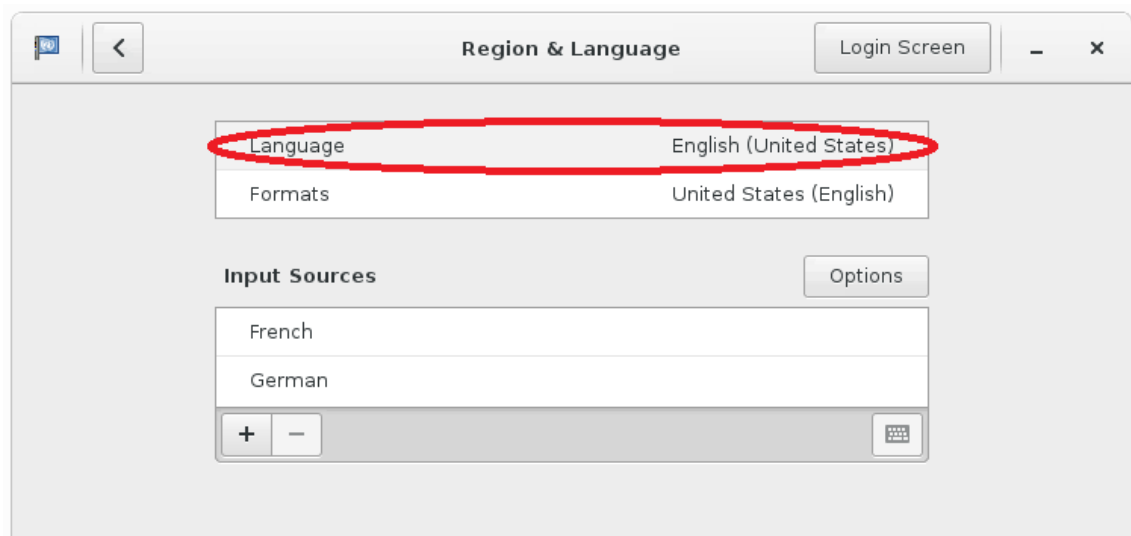
1. Aktivieren Sie das Feature.
2. Rufen Sie eine veröffentlichte Anwendung auf, die Texteingabe ermöglicht. Eine Sprachleiste wird in der Sitzung zusätzlich zur Anwendung angezeigt.
3. Wählen Sie im Dropdownmenü **Region und Sprache**, um die gewünschte Sprache (Eingabequelle) hinzuzufügen.



4. Wählen Sie den IME oder das Tastaturlayout aus dem Dropdownmenü.
5. Geben Sie Text mit dem ausgewählten IME- oder Tastaturlayout ein.

Hinweis:

- Wenn Sie ein Tastaturlayout in der VDA-seitigen Sprachleiste ändern, stellen Sie sicher, dass das gleiche Tastaturlayout auf dem Client (mit Citrix Workspace-App) verwendet wird.
- Das Paket **accountsservice** muss auf Version 0.6.37 oder höher aktualisiert werden, damit Sie Einstellungen im Dialogfeld **Region und Sprache** vornehmen können.



Multimedia

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Audiofeatures](#)
- [Browserinhaltsumleitung](#)
- [HDX-Webcamvideokomprimierung](#)

Audiofeatures

October 5, 2022

Adaptives Audio

Adaptives Audio ist standardmäßig aktiviert. Folgende Citrix Workspace-App-Clients werden unterstützt:

- Citrix Workspace-App für Windows –2109 und höher
- Citrix Workspace-App für Linux –2109 und höher
- Citrix Workspace-App für Mac –2109 und höher

Wenn Sie einen Client verwenden, der nicht auf der Liste steht, greift adaptives Audio auf Legacy-Audio zurück.

Bei adaptivem Audio müssen Sie die [Audioqualitätsrichtlinien](#) auf dem VDA nicht manuell konfigurieren. Adaptives Audio passt die Audio-Abtastrate dynamisch an die Netzwerkbedingungen an, um ein erstklassiges Audioerlebnis zu bieten.

Die folgende Tabelle vergleicht adaptives Audio mit Legacy-Audio:

Adaptives Audio	Legacy-Audio
Max. Audio-Abtastrate: 48 kHz	Max. Audio-Abtastrate: 8 kHz
Stereo-Kanal	Mono-Kanal

Tipp:

Verwenden Sie PulseAudio 13.99 oder höher für RHEL 8.x.

Verwenden Sie PulseAudio 14.2 oder höher unter SUSE 15.3 und PulseAudio 13.0 oder höher unter SUSE 15.2.

Browserinhaltsumleitung

October 5, 2022

Übersicht

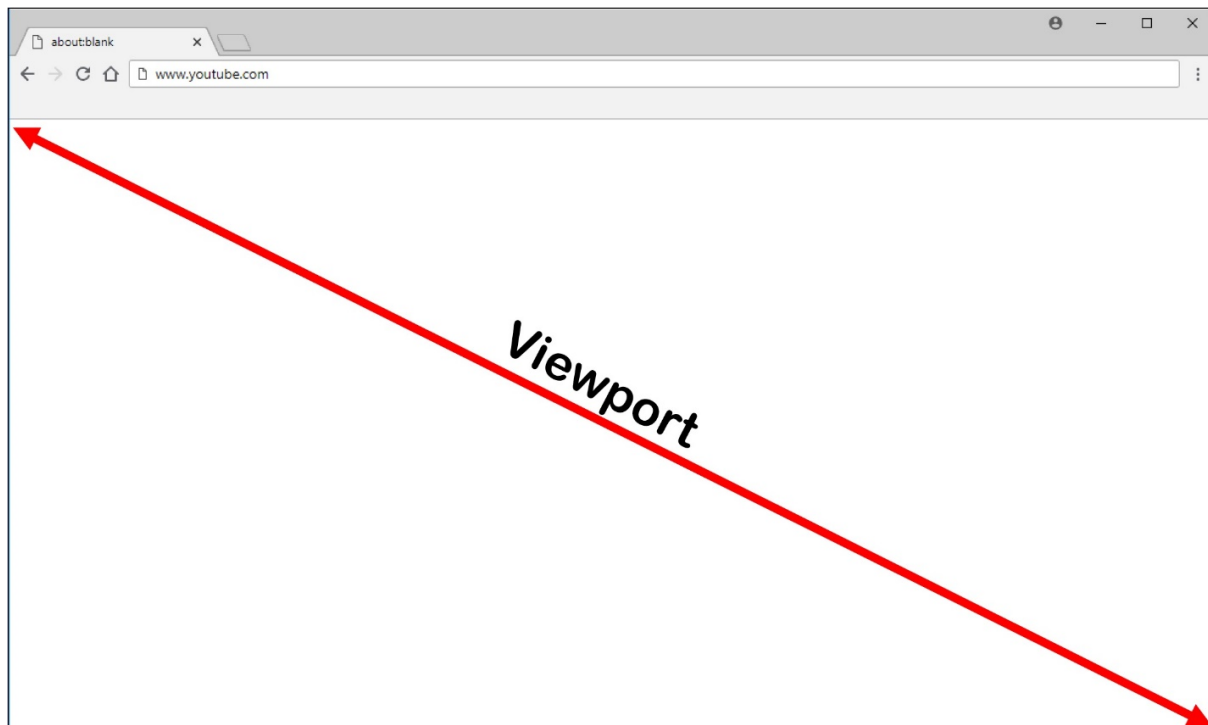
Der Linux VDA unterstützt die Browserinhaltsumleitung in Google Chrome. Die Browserinhaltsumleitung bietet die Möglichkeit der Wiedergabe von Webseiten in der Positivliste auf Clientseite. Dabei wird von der Citrix Workspace-App clientseitig die Instanz einer entsprechenden Renderingengine erzeugt, die den HTTP- und HTTPS-Inhalt von der URL abruft.

Hinweis:

Mit einer Positivliste können Sie festlegen, welche Webseiten an die Clientseite umgeleitet werden. Umgekehrt können Sie mit einer Sperrliste festlegen, welche Webseiten nicht an die Clientseite umgeleitet werden.

Diese Overlay-Weblayoutengine wird statt auf dem VDA auf dem Client ausgeführt und verwendet dessen CPU, GPU, Arbeitsspeicher und Netzwerk.

Es wird nur der Browserviewport umgeleitet. Der Viewport ist der rechteckige Browserbereich, in dem der Inhalt angezeigt wird. Der Viewport enthält keine Elemente wie Adressleiste, Favoritenleiste und Statusleiste. Diese Elemente werden weiterhin im Browser auf dem VDA ausgeführt.



Systemanforderungen

Windows-Client:

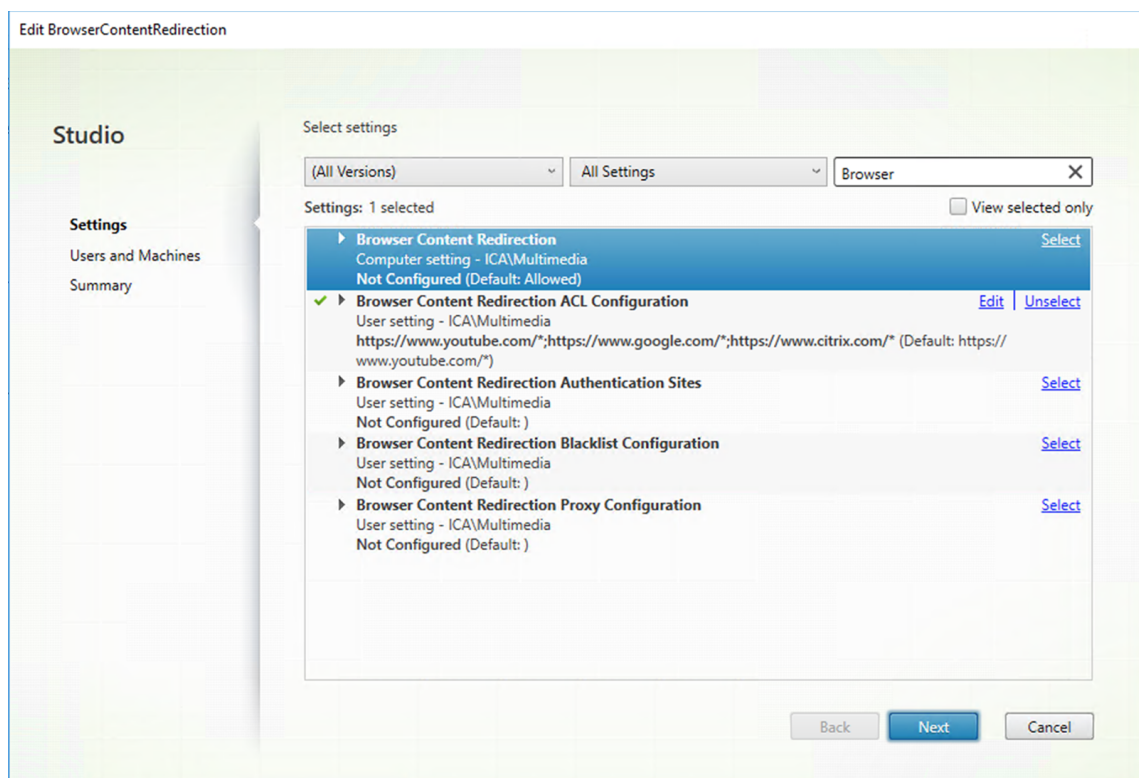
- Citrix Workspace-App 1809 für Windows oder höher

Linux VDA:

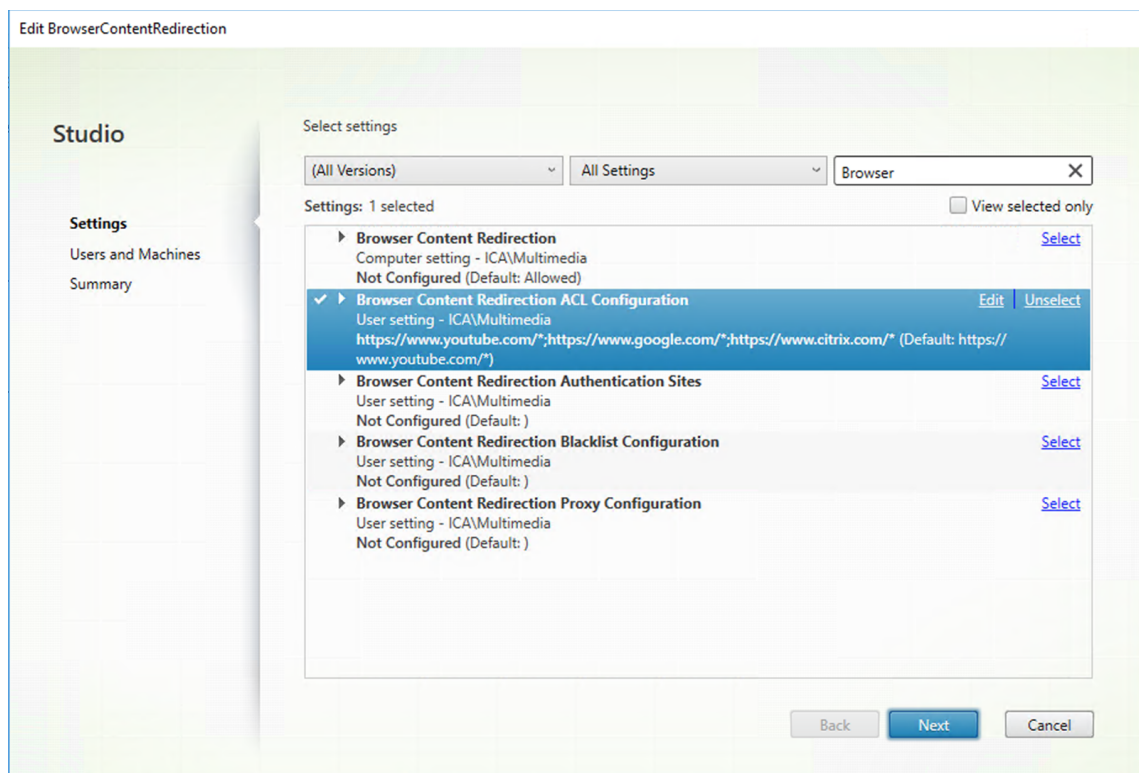
- VDA-Betriebssystem: Ubuntu 20.04, Ubuntu 18.04, RHEL 8.2, RHEL 8.1
- Browser auf dem VDA: Google Chrome v66 oder höher mit der hinzugefügten Citrix-Browserinhaltsumleitungs-Erweiterung

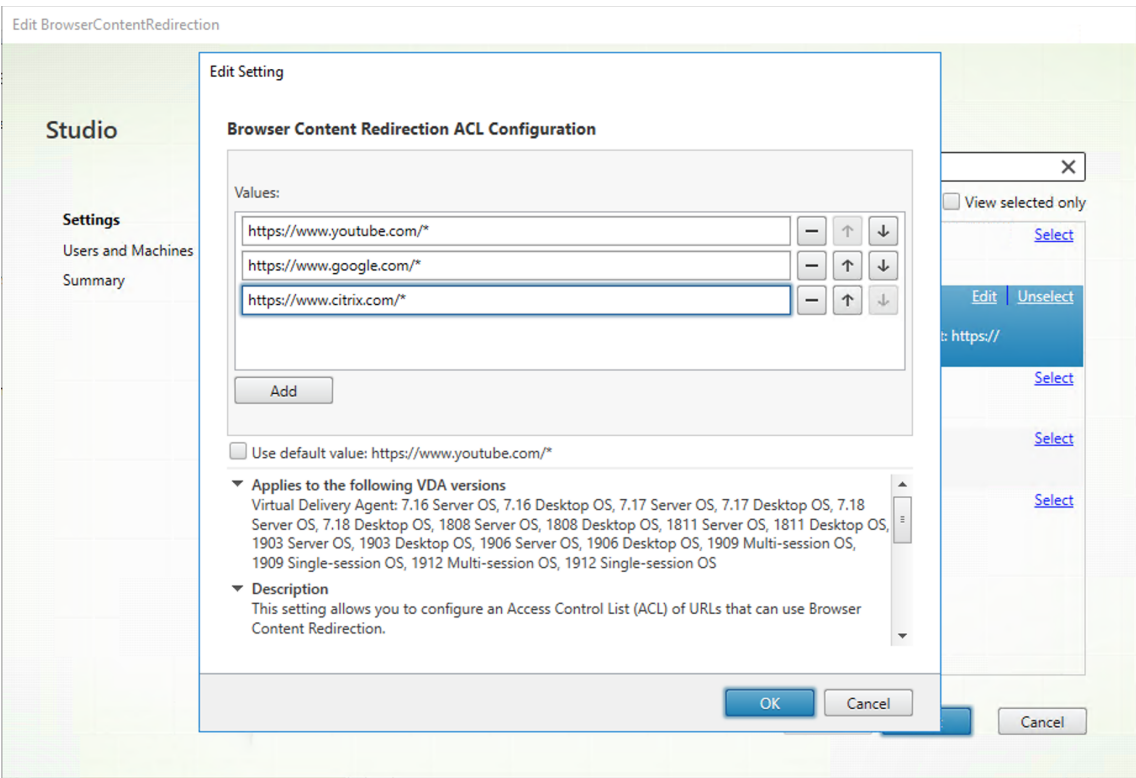
Konfigurieren der Browserinhaltsumleitung

1. Konfigurieren Sie in Citrix Studio Richtlinien, mit denen eine Positivliste und eine Sperrliste von URLs für die Browserinhaltsumleitung angegeben wird. Für die Browserinhaltsumleitung ist standardmäßig **Zulässig** festgelegt.

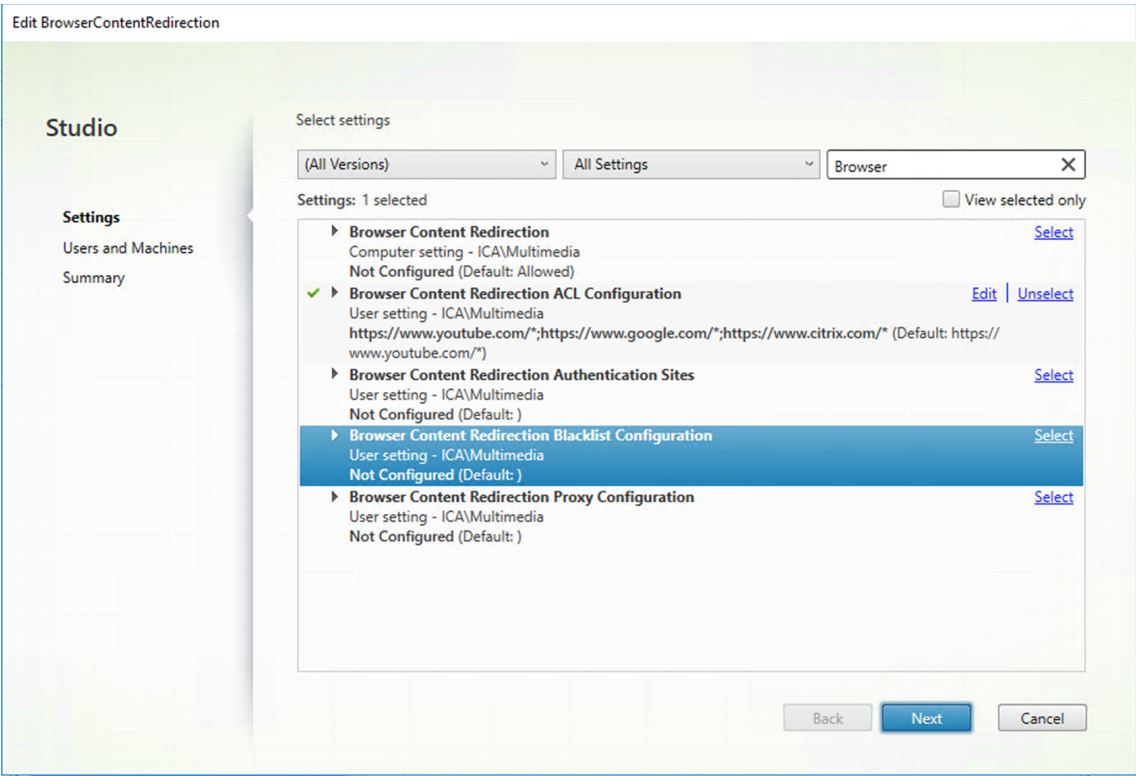


Die Einstellung **ACL-Konfiguration für die Browserinhaltsumleitung** gibt eine Positivliste von URLs an, die die Browserinhaltsumleitung verwenden können.





Die Einstellung **Sperrlistenkonfiguration für die Browserinhaltsumleitung** gibt eine Sperre von URLs an, die keine Browserinhaltsumleitung verwenden können.



Hinweis:

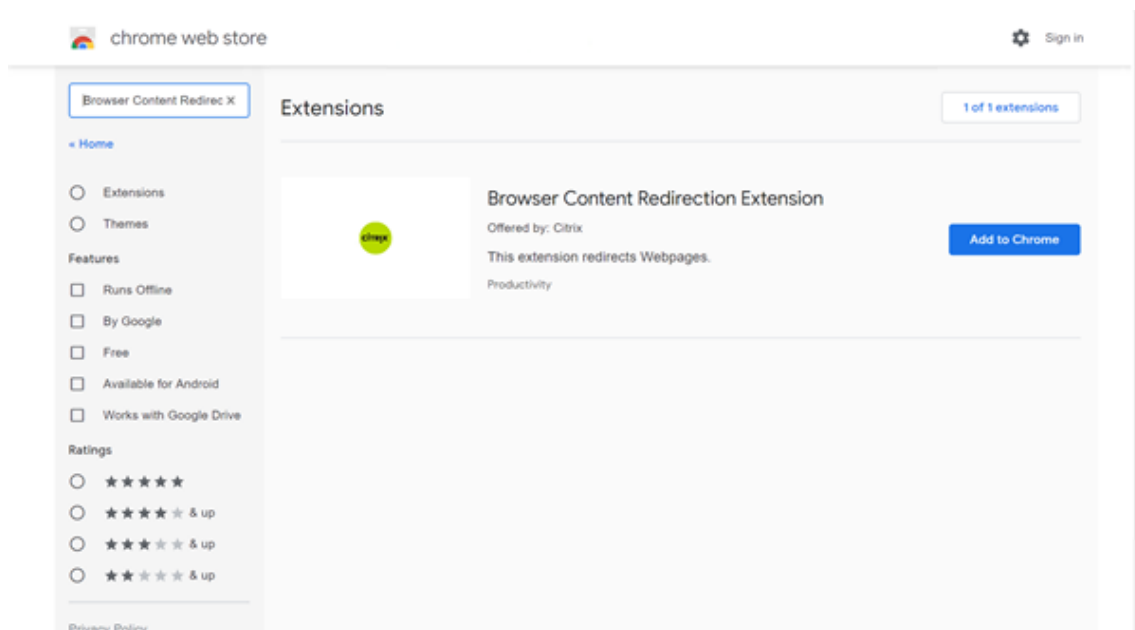
Vom Linux VDA wird die Einstellung **Proxykonfiguration für die Browserinhaltsumleitung** zurzeit nicht unterstützt.

2. Klicken Sie auf dem VDA auf **Zu Chrome hinzufügen**, um die Citrix-Erweiterung zur Browserinhaltsumleitung aus dem Chrome Web Store hinzuzufügen. Auf diese Weise kann der Browser auf dem VDA erkennen, ob eine aufgerufene URL mit einer Positiv- oder Sperrliste übereinstimmt.

Wichtig:

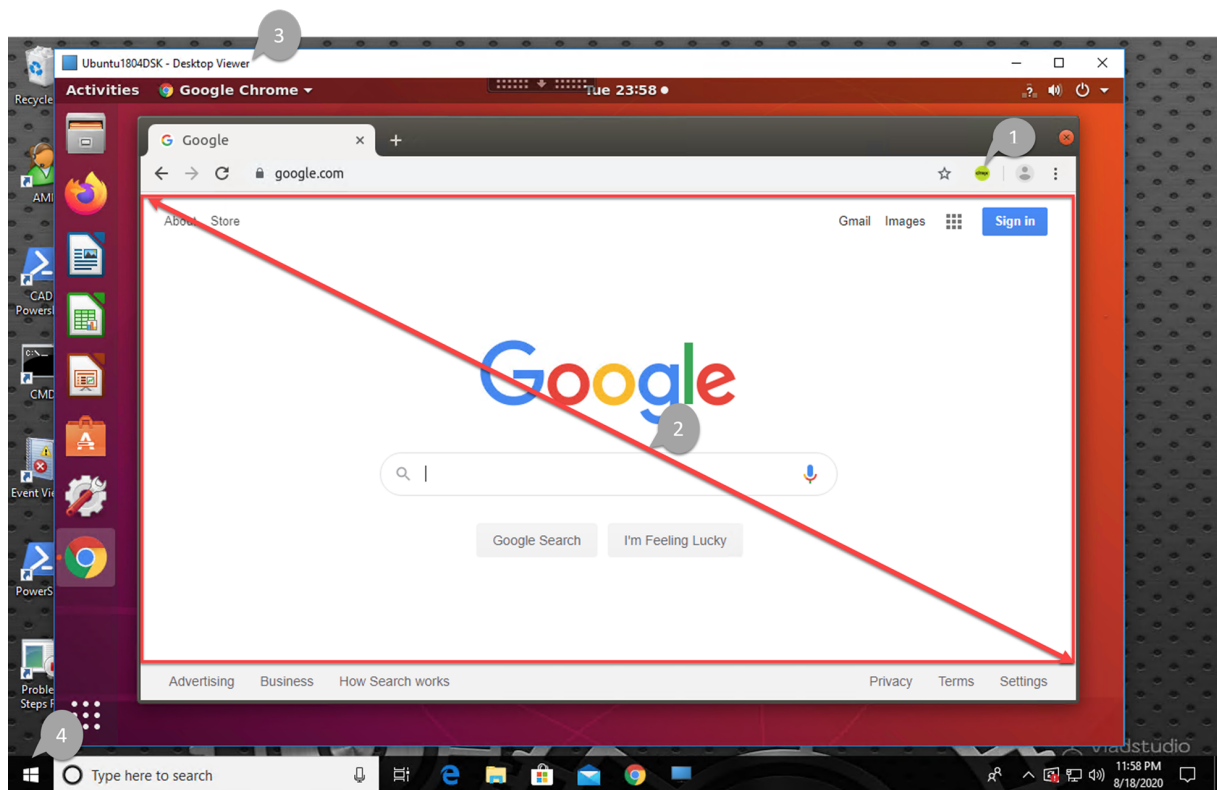
Die Erweiterung ist auf dem Client nicht erforderlich. Fügen Sie sie nur auf dem VDA hinzu.

Chrome-Erweiterungen werden für einzelne Benutzer installiert. Das Update eines Gold-Masterimages zum Hinzufügen oder Entfernen einer Erweiterung ist nicht erforderlich.



Wird eine Übereinstimmung mit einer URL in einer Positivliste (z. B. <https://www.mycompany.com/>) gefunden, jedoch nicht in einer Sperrliste, weist ein virtueller Kanal (CTXCSB) die Citrix Workspace-App an, dass eine Umleitung erforderlich ist, und leitet die URL weiter. Die Citrix Workspace-App erzeugt dann eine lokale Renderingengine-Instanz und zeigt die Website an.

Anschließend fügt die Citrix Workspace-App die Website nahtlos in den Inhaltsbereich des virtuellen Desktopbrowsers ein.



1. Symbol der Citrix-Browserinhaltsumleitungs-Erweiterung

Die Farbe des Erweiterungssymbols gibt den Status der Chrome-Erweiterung an. Folgende drei Farben sind möglich:

- Grün: Aktiv und verbunden
- Grau: Nicht aktiv/Leerlauf auf der aktuellen Registerkarte
- Rot: Defekt/außer Betrieb

2. Wiedergabe von Viewport auf dem Client oder nahtloses Einfügen in den virtuellen Desktop

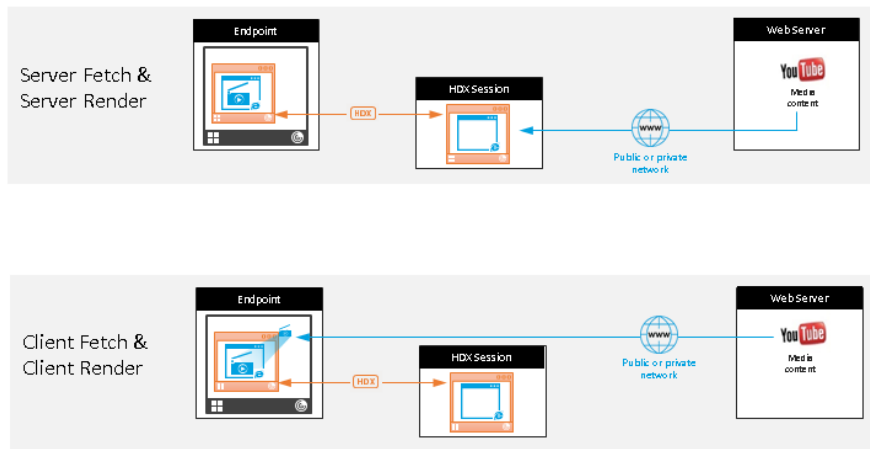
3. Linux VDA

4. Windows-Client

Umleitungsszenarios

Szenarien für den Inhaltsabruf durch die Citrix Workspace-App:

Redirection scenarios



Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

- **Abruf und Wiedergabe auf dem Server:** Es findet keine Umleitung statt, weil die Site nicht auf der Positivliste steht oder ein Fehler aufgetreten ist. Die Wiedergabe findet dann auf dem VDA statt und das Grafikremoting mithilfe von Thinwire. Verwenden Sie Richtlinien, um dieses Fallbackverhalten zu steuern. Dieses Szenario führt zu einem hohen CPU-, RAM- und Bandbreitenverbrauch auf dem VDA.
- **Abruf und Wiedergabe auf dem Client:** Da die Citrix Workspace-App direkt auf den Webserver zugreift, ist Internetzugang erforderlich. In diesem Szenario wird die gesamte Netzwerk-, CPU- und RAM-Last von der Citrix Virtual Apps and Desktops-Site abgeladen.

Fallbackmechanismus

Es kann vorkommen, dass die Clientumleitung fehlschlägt. Wenn der Client beispielsweise keinen direkten Internetzugriff hat, kann eine Fehlerantwort an den VDA zurückgegeben werden. In einem solchen Fall kann der Browser auf dem VDA die Seite auf dem Server neu laden und wiedergeben.

HDX-Webcamvideokomprimierung

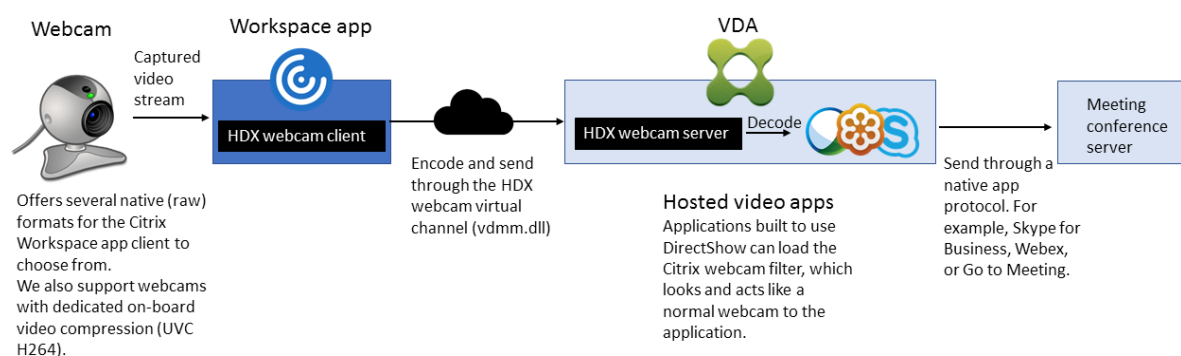
April 3, 2023

Übersicht

Benutzer von Videokonferenzanwendungen, die in Linux VDA-Sitzungen ausgeführt werden, können für ihre Webcams jetzt die HDX-Webcamvideokomprimierung verwenden. Das Feature ist in der Standardeinstellung aktiviert. Wir empfehlen, nach Möglichkeit die HDX-Webcamvideokomprimierung zu verwenden.

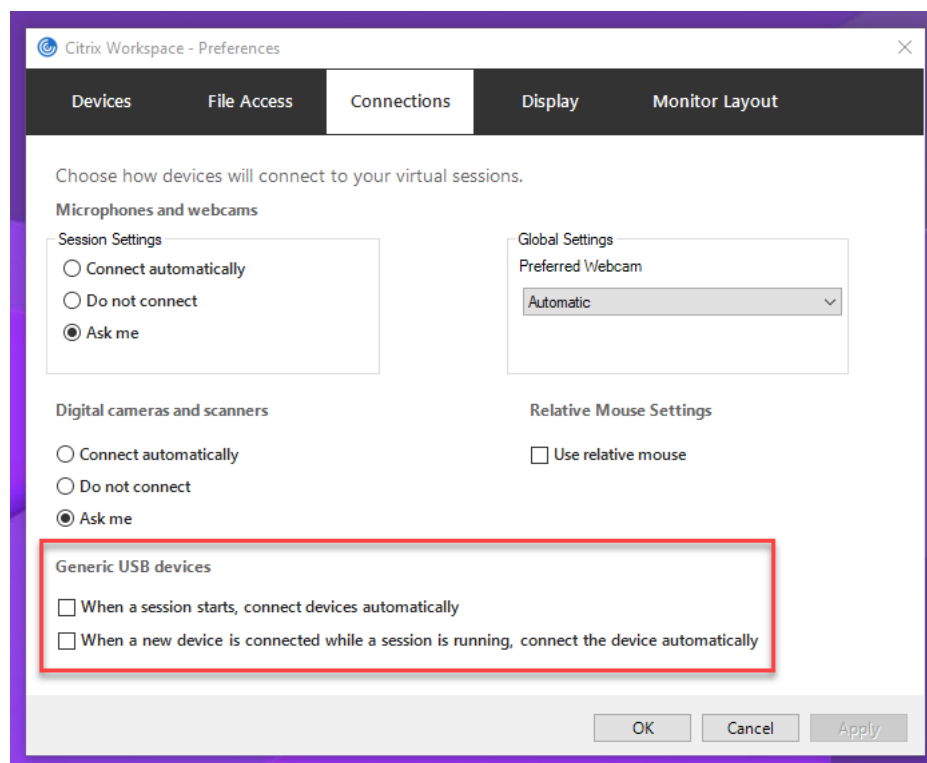
Die HDX-Webcamvideokomprimierung wird auch als **optimierter** Webcammodus bezeichnet. Bei dieser Art der Webcamvideokomprimierung wird das H.264-Video direkt an die Videokonferenzanwendung gesendet, die in der virtuellen Sitzung ausgeführt wird. Bei der HDX-Webcamvideokomprimierung wird die Multimediaframework-Technologie des Clientbetriebssystems verwendet, um Videos von Aufnahmeegeräten zu erfassen, zu transcodieren und zu komprimieren. Hersteller von Aufnahmeegeräten liefern die Treiber, die sich in die Betriebssystem-Kernelstreaming-Architektur einfügen.

Der Client übernimmt die Kommunikation mit der Webcam. Der Client sendet Videos nur an Server, die es ordnungsgemäß anzeigen können. Der Server ist nicht direkt mit der Webcam verbunden, seine Integration sorgt jedoch dafür, dass die gleiche Erfahrung auf dem Desktop geliefert wird. Die Workspace-App komprimiert Videos zum Einsparen von Bandbreite und zur Gewährleistung einer besseren Ausfallsicherheit in WANs.



Hinweis:

- Dieses Feature unterstützt nur H.264-Videos vom Citrix Workspace-App-Client.
- Es unterstützt eine Webcamauflösung von 48 x 32 bis 1920 x 1080.
- Wählen Sie bei Verwendung einer Webcam nicht **Generische USB-Geräte** auf der Citrix Workspace-App-Symboleiste aus. Andernfalls können unerwartete Probleme auftreten.



Unterstützte Linux-Distributionen

- RHEL 8.4
- RHEL 7.9/CentOS 7.9
- Ubuntu 20.04
- Ubuntu 18.04
- Debian 11.3
- Debian 10.9
- SUSE 15.3
- SUSE 15.2

Unterstützte Citrix Workspace-App

Die HDX-Webcam-Videokomprimierung unterstützt die folgenden Versionen der Citrix Workspace-App:

Plattform	Prozessor
Citrix Workspace-App für Windows	Die Citrix Workspace-App für Windows unterstützt die Webcam-Videokomprimierung für 32-Bit- und 64-Bit-Apps unter XenApp und XenDesktop 7.17 und höher. Unter früheren Versionen unterstützt die Citrix Workspace-App für Windows nur 32-Bit-Apps.
Citrix Workspace-App für Chrome	Da manche ARM-Chromebooks die H.264-Codierung nicht unterstützen, können nur 32-Bit-Apps die optimierte HDX-Webcam-Videokomprimierung verwenden.

Vollständig getestete Webcams

Die Bildfrequenz sowie Helligkeits- und Kontraststufen sind bei den einzelnen Webcams unterschiedlich. Citrix verwendet die folgenden Webcams für die Feature-Erstvalidierung:

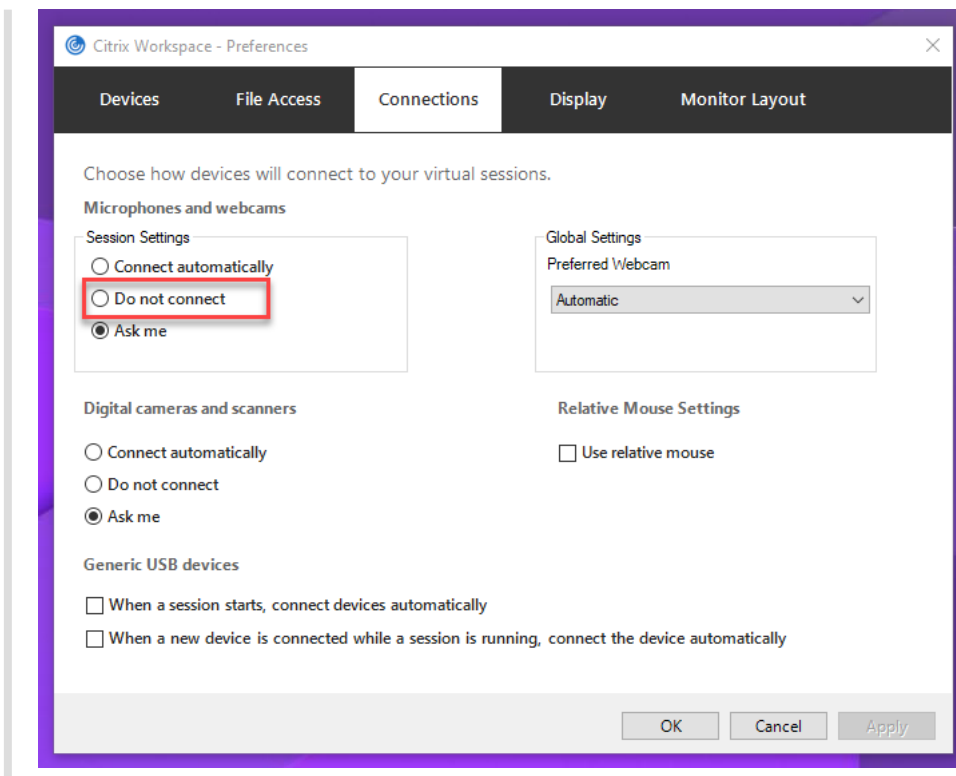
- Logitech HD C270
- Logitech C930e
- Microsoft-LifeCam-HD3000

Konfiguration

Das Feature ist in der Standardeinstellung aktiviert. Zur Verwendung führen Sie die folgende Überprüfung und Konfiguration aus:

Tipp:

Benutzer der Citrix Workspace-App können die Standardeinstellung außer Kraft setzen, indem sie in Desktop Viewer unter **Mikrofon & Webcam** die Einstellung **Nicht verbinden** auswählen.



1. Stellen Sie nach Abschluss der VDA-Installation sicher, dass sich der VDA beim Delivery Controller registrieren kann und dass die veröffentlichten Linux-Desktopsitzungen mit der Windows-Anmeldeinformationen gestartet werden können.
2. Stellen Sie sicher, dass der VDA Internetzugang hat, und führen Sie dann den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um die Webcamkonfiguration abzuschließen. Wenn der VDA keinen Internetzugang hat, gehen Sie zu Schritt 3.

Hinweis:

Es kann vorkommen, dass `uname -r` und Kernel-Header nicht übereinstimmen. Dies führt dazu, dass das Skript `ctxwcamcfg.sh` nicht ausgeführt werden kann. Zur ordnungsgemäßen Verwendung der HDX-Webcam-Videokomprimierung führen Sie zunächst **sudo apt-get dist-upgrade** aus, starten dann den VDA neu und führen anschließend das Skript `ctxwcamcfg.sh` erneut aus.

Wenn Ihr VDA unter Debian bereitgestellt ist, stellen Sie sicher, dass er unter der neuesten Kernelversion ausgeführt wird. Führen Sie andernfalls die folgenden Befehle aus, um ein Update auf die neueste Kernelversion durchzuführen:

```
1 sudo apt-get update
2 sudo apt-get dist-upgrade
3 sudo reboot
4 <!--NeedCopy-->
```

Wenn Ihr VDA auf SUSE 15.3, SUSE 15.2 oder SUSE 12.5 bereitgestellt ist, führen Sie die folgenden Befehle aus, um den VDA auf die neueste Kernelversion zu aktualisieren und neu zu starten:

```
1 zypper up kernel-default
2 reboot
3 <!--NeedCopy-->
```

Das Skript `ctxwcamcfg.sh` hat folgende Funktionen:

- a) Installation der Programme für `kernel-devel` und DKMS (Dynamic Kernel Module Support) auf dem VDA.
 - `kernel-devel` wird verwendet, um ein Kernelmodul der virtuellen Webcam in der benötigten Version zu erstellen.
 - DKMS wird zur dynamischen Verwaltung des Kernelmoduls der virtuellen Webcam verwendet.
- Hinweis:**

Bei Installation der o. g. Programme unter RHEL und CentOS installiert und aktiviert das Skript `ctxwcamcfg.sh` die folgenden Repositories auf dem VDA:

 - Extra Pakete für Enterprise Linux (EPEL)
 - RPM Fusion
- b) Laden Sie den Open-Source-Code `v4l2loopback` von <https://github.com/umlaeute/v4l2loopback> herunter und verwenden Sie DKMS zur Verwaltung von `v4l2loopback`. `v4l2loopback` ist ein Kernelmodul, mit dem Sie V4L2-Loopback-Geräte erstellen können.
 - c) Führen Sie den Befehl `sudo service ctxwcamsd restart` aus. Der Webcamdienst `ctxwcamsd` des Linux VDAs startet neu und lädt das `v4l2loopback`-Kernelmodul für die HDX-Webcamvideokomprimierung.
3. Wenn der VDA keinen Internetzugang hat, erstellen Sie das Kernelmodul `v4l2loopback` auf einer anderen Maschine und kopieren es dann auf den VDA.
- a) Bereiten Sie eine Buildmaschine mit Internetzugriff vor und verwenden Sie dieselbe Kernelversion wie beim VDA. Mit dem Befehl `uname -r` werden Kernelversionen gefunden.
 - b) Führen Sie auf der Buildmaschine den Befehl `sudo mkdir -p /var/xdl` aus.
 - c) Kopieren Sie `/var/xdl/configure_*` vom VDA auf die Buildmaschine unter `/var/xdl/`.
 - d) Führen Sie auf der Buildmaschine den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um das Kernelmodul zu erstellen. Beim erfolgreichen Ausführen des Befehls wird unter dem Pfad `/var/lib/dkms/v4l2loopback/1.81`

`b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/` die Datei `v4l2loopback.ko` erstellt. Ignorieren Sie Fehler, die auftreten können, wenn Sie das Skript `ctxwcamcfg.sh` ausführen.

- e) Kopieren Sie `v4l2loopback.ko` von der Buildmaschine auf den VDA und speichern Sie die Datei unter `/opt/Citrix/VDA/lib64/`.
- f) Führen Sie auf dem VDA den Befehl `sudo service ctxwcamsd restart` aus, um den Webcamdienst neu zu starten und das Kernelmodul `v4l2loopback` zu laden.

Nicht in Domänen eingebundene VDAs

October 10, 2022

Übersicht über die Einrichtung

Nicht in Domänen eingebundene VDAs werden nur in Citrix DaaS unterstützt. Um nicht in Domänen eingebundene VDAs in Citrix DaaS zu erstellen, müssen Sie Maschinenerstellungsdienste (MCS) verwenden. Hier die kurzen Schritte:

1. Erstellen Sie ein Masterimage auf einer Vorlagen-VM, auf der Sie auch das VDA-Paket installieren. Sie können ein einzelnes Image zum Erstellen von VDAs sowohl mit als auch ohne Domäneneinbindung verwenden.
2. Verwenden Sie das Masterimage, um einen Maschinenkatalog zu erstellen. Wählen Sie MCS als Methode zur Bereitstellung der Maschinen und wählen Sie **Gehört keiner Domäne an** als Identität für die im Katalog zu erstellenden Maschinen aus.

Weitere Informationen finden Sie unter [Erstellen von Linux-VMs mit Maschinenerstellungsdiensten \(MCS\)](#) und [Maschinenidentitäten](#).

Für nicht in Domänen eingebundene VDAs verfügbare Features

Erstellen lokaler Benutzer mit angegebenen Attributen auf VDAs ohne Domäne

Wenn Sie eine Sitzung öffnen, die auf einem nicht in eine Domäne eingebundenen VDA gehostet wird, erstellt der VDA automatisch einen lokalen Benutzer mit Standardattributen. Der VDA erstellt den lokalen Benutzer basierend auf dem Benutzernamen, mit dem Sie sich bei der Citrix Workspace-App angemeldet haben. Sie können auch Benutzerattribute angeben, darunter die Benutzer-ID (UID), die Gruppen-ID (GID), das Homeverzeichnis und die Login-Shell des Benutzers. Führen Sie die folgenden Schritte aus, um die Funktion zu nutzen:

1. Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent\LocalMappedAccount" -t "REG_DWORD" -v "
  CreateWithUidGid" -d "0x00000001" --force
2 <!--NeedCopy-->
```

2. Geben Sie im Skript `/var/xdm/getuidgid.sh` unter dem Installationspfad des VDA die folgenden Attribute an:

Attribut	Erforderlich oder optional	Beschreibung
uid	Erforderlich	Ein Benutzer-ID (UID) ist eine Nummer, die Linux jedem Benutzer im System zuweist. Sie bestimmt, auf welche Systemressourcen der Benutzer zugreifen kann.
gid	Erforderlich	Eine Gruppen-ID (GID) ist eine Zahl, die für eine bestimmte Gruppe steht.
homedir	Optional	Das Linux-Homeverzeichnis ist ein Verzeichnis für einen bestimmten Benutzer.
shell	Optional	Eine Login-Shell ist eine Shell, die einem Benutzer bei der Anmeldung bei seinem Benutzerkonto zugewiesen wird.

Im Folgenden finden Sie ein Beispiel für das Skript `getuidgid.sh`:

Hinweis:

Stellen Sie sicher, dass die im Skript angegebenen Attribute gültig sind.

```
1 #!/bin/bash
2
3 #####
4 #
5 # Citrix Virtual Apps and Desktops für Linux-Skript: Abrufen von
  UID und GID für den Benutzer
6 #
7 # Copyright (c) Citrix Systems, Inc. Alle Rechte vorbehalten.
```

```
8 #
9
10 export LC_ALL="en_US.UTF-8"
11
12 function get_uid_gid_for_user()
13 {
14
15     echo "uid:12345"
16     echo "gid:1003"
17     echo "homedir:/home/$1"
18     echo "shell:/bin/sh"
19 }
20
21
22 get_uid_gid_for_user $1<!--NeedCopy-->
```

Liste der unterstützten Richtlinien

October 5, 2022

Liste der für Linux VDA unterstützten Richtlinien

Studio-				
Richtlinie	Schlüssel	Type	Modul	Standardwert
Lokale Zeit des Clients	UseLocalTimeOfClient	Boolean	ICA	Serverzeit
ICA-Roundtripintervall für ICA-Überwachung	IcaRoundTripCheckPeriod	Integer	ICA	15
ICA-Roundtripberechnung	IcaRoundTripCalculation	Boolean	ICA	aktiviert
ICA-Roundtripberechnung	IcaRoundTripCalculation	Boolean	ICA	aktiviert

Studio-				
Richtlinie	Schlüssel	Type	Modul	Standardwert
ICA- Roundtrip für Verbindun- gen im Leer- lauf berech- nen	IcaRoundTripCheck	Boolean	ClientHealthMonitoring	
				(0)
Bandbreitenlimit für Sitzung insge- samt	IdentifiableUserBandwidth	Integer	ICA\Bandwidth	
Bandbreitenlimit für die Au- dioum- leitung	IdentifiableUserBandwidth	Integer	ICA\Bandwidth	
Bandbreitenlimit für die Au- dioum- leitung (Prozent)	IdentifiableUserBandwidth	Integer	ICA\Bandwidth	
Bandbreitenlimit für Client- USB- Geräteumleitung	IdentifiableUserBandwidth	Integer	ICA\Bandwidth	

Studio-				
Richtlinie	Schlüssel	Type	Modul	Standardwert
Bandbreite mit USB-Peripherie für Client-USB-Geräteumleitung (Prozent)				
ItemID	Path	Benutzer	ICA	Bandbreite
Bandbreite mit USB-Peripherie für Zwischenablageumleitung				
ItemID	Path	Benutzer	ICA	Bandbreite
Bandbreite mit USB-Peripherie für Zwischenablageumleitung (Prozent)				
ItemID	Path	Benutzer	ICA	Bandbreite
Bandbreite mit USB-Peripherie für Dateiumleitung				
ItemID	Path	Benutzer	ICA	Bandbreite
Bandbreite mit USB-Peripherie für Dateiumleitung (Prozent)				
ItemID	Path	Benutzer	ICA	Bandbreite
Bandbreite mit USB-Peripherie für Druckerumleitung				
ItemID	Path	Benutzer	ICA	Bandbreite

Studio-				
Richtlinie	Schlüssel	Typ	Modul	Standardwert
Bandbreitenlimit für Druckerumleitung (Prozent)				
Bandbreitenlimit für Druckerumleitung (Prozent)	PrinterBandwidth	Integer	ICA\Bandwidth	0
WebSockets-Verbindungen				
WebSockets-Verbindungen	WebSocketsConnections	Boolean	ICA\WebSockets	True
WebSockets-Portnummer				
WebSockets-Portnummer	WebSocketsPort	Integer	ICA\WebSockets	8008
Vertrauenswürdiges Ursprungsserververzeichnis				
Vertrauenswürdiges Ursprungsserververzeichnis	WebSocketsTrustedOrigins	String	ICA\WebSockets	
ICA-Keep-Alive				
ICA-Keep-Alive	ICAKeepAlive	Boolean	ICA-Keep-Alive	True
ICA-Keep-Alive - Time-out				
ICA-Keep-Alive - Time-out	ICAKeepAliveTimeout	Integer	ICA-Keep-Alive	60
ICA-Listenerportnummer				
ICA-Listenerportnummer	IcaListenerPort	Integer	ICA-Listener	1494
Adaptiver HDX-Transport				
Adaptiver HDX-Transport	HDXoverUDP	Boolean	ICA	True
Sitzungszuverlässigkeit				
Sitzungszuverlässigkeit	SessionReliability	Integer	ICA\Reliability	1
Verbindungen				
Verbindungen	SessionReliability	Integer	ICA\Reliability	1

Studio-				
Richtlinie	Schlüssel	Type	Modul	Standardwert
UI-Transparenzstufe während Wiederverbindung	ReconnectionTimeout	Computer	Client	30 s
	ReconnectionPort	Client	Reconnection	2598
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
Sitzungszuverlässigkeit - Time-out	ReconnectionTimeout	Computer	Client	30 s
	ReconnectionPort	Client	Reconnection	2598
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
Automatische Wiederverbindung von Clients	ReconnectionTimeout	Computer	Client	30 s
	ReconnectionPort	Client	Reconnection	2598
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
Clientaudioumleitung	ReconnectionTimeout	Computer	Client	30 s
	ReconnectionPort	Client	Reconnection	2598
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
Clientdruckerumleitung	ReconnectionTimeout	Computer	Client	30 s
	ReconnectionPort	Client	Reconnection	2598
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
Universeller PDF-Drucker erstellen	ReconnectionTimeout	Computer	Client	30 s
	ReconnectionPort	Client	Reconnection	2598
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s
	ReconnectionPort	Client	Sitzungszuverlässigkeit	180 s

Studio-				
Richtlinie	Schlüssel	Type	Modul	Standardwert
Druckertreiber-Mapping und -kompatibilität	PrinterMapping	Drucken	"	
			Microsoft	
			XPS	
			Document	
			Writer	
			*	
			Deny	
			;	
			Send	
			to	
			Microsoft	
			OneNote	
			*	
			Deny	
			"	
Client-USB-Geräteumleitung	AllowUSBRedirector	USB	Nicht zuge-	
			lassen	
			(1)	
Regeln für die Client-USB-Geräteumleitung	USBDeviceRedirector	USB	“	
			“\0”	
			”	
Bewegbilddrucker-Treiber-Mapping	PrinterMapping	Drucken	(1)	

Studio-				
Richtlinie	Schlüssel	Type	Modul	Standardwert
Zusätzliche Far- bkom- prim- ierung	ExtraColorCompression	Boolean	Thinwire	Deaktiviert
	Far- bkom- prim- ierung			(0)
Mindestframerate	MinFrameRate	Integer	Thinwire	15 f/s
Frameratesollwert	FrameRateSollwert	Integer	Thinwire	30 f/s
Bildqualität	ImageQuality	Integer	Thinwire	Mittel
				(3)
Verwenden von Videocodec für die Kom- prim- ierung	UseVideoCodec	Boolean	Thinwire	Bevorzugt
				ver-
				wen-
				den
				(3)
Verwenden der Hard- ware- codierung für Videocodec	UseHardwareEncoding	Boolean	Thinwire	Vorwiegend
				(1)
Visuell ver- lust- freie Kom- prim- ierung zu- lassen	AllowVisualLosslessCompression	Boolean	Thinwire	Deaktiviert
				(0)

Studio-				
Richtlinie	Schlüssel	Type	Modul	Standardwert
Optimierung für 3D-Grafikworkload	OptimizePerUserThinwire	Boolean	Thinwire	Deaktiviert
				(0)
Bevorzugte Farbtiefe für ein-fache Grafiken	PreferredColorDepth	Integer	Thinwire	24 Bit
				pro
				Pixel
Audioqualität	AudioQuality	Enum	UserAudio	Hoch - High Definition Audio
				(2)
Clientmikrofon-Einstellung	ClientMicrophone	Boolean	Radio	Zugelassen
				(1)
Sitzungsdauer-Toleranzwert für gleichzeitige Anmeldungen	SessionTimeout	Integer	Session	250
Automatische Controllerupdates aktivieren	AutoUpdateController	Boolean	Control	Zugelassen
			Delivery	(1)
			Agent-Einstellungen	

Studio-				
Richtlinie	Schlüssel	Typ	Modul	Standardwert
Aktualisierungsmethode für die Zwischenablage	Clipboard	Boolean	Clipboard	True
	Clipboard	Boolean	Clipboard	True
	Clipboard	Boolean	Clipboard	True
Aktualisierungsmethode für die Primärauswahl	Clipboard	Boolean	Clipboard	True
	Clipboard	Boolean	Clipboard	True
	Clipboard	Boolean	Clipboard	True
Maximale Speex-Qualität	MaxSpeechQuality	Integer	Audio	5
	MaxSpeechQuality	Integer	Audio	5
	MaxSpeechQuality	Integer	Audio	5
Clientlaufwerke verbinden	ClientDrive	Boolean	ClientDrive	True
	ClientDrive	Boolean	ClientDrive	True
	ClientDrive	Boolean	ClientDrive	True
Optische Clientlaufwerke	AllowCdrom	Boolean	ClientDrive	True
	AllowCdrom	Boolean	ClientDrive	True
	AllowCdrom	Boolean	ClientDrive	True
Lokale Clientfestplattenlaufwerke	AllowFixedDrive	Boolean	ClientDrive	True
	AllowFixedDrive	Boolean	ClientDrive	True
	AllowFixedDrive	Boolean	ClientDrive	True
Clientdiskettenlaufwerke	AllowFloppyDrive	Boolean	ClientDrive	True
	AllowFloppyDrive	Boolean	ClientDrive	True
	AllowFloppyDrive	Boolean	ClientDrive	True
Clientnetzlaufwerke	AllowNetworkDrive	Boolean	ClientDrive	True
	AllowNetworkDrive	Boolean	ClientDrive	True
	AllowNetworkDrive	Boolean	ClientDrive	True
Clientlaufwerke	AllowDrive	Boolean	ClientDrive	True
	AllowDrive	Boolean	ClientDrive	True
	AllowDrive	Boolean	ClientDrive	True

Studio-				
Richtlinie	Schlüssel	Typ	Modul	Standardwert
Schreibgeschütztes Zugriff auf Client- laufwerke	Recht über Remote-Datei	Deaktiviert	COM	
	Zugriff auf Client- laufwerke	(0)		
Automatische Anzeige der Tastatur	Automatische Anzeige der Tastatur	Deaktiviert	VRM	
	Anzeige der Tastatur	(0)		
Dateiübertragungs- zwischen Desktop und Client zulassen	Übertragungsfenster Dateiübertragungen	Zugang		
Dateien von Desktop herunterladen	AllowFileBrowser	Benutzer	Dateiübertragungen	
Dateien auf Desktop hochladen	AllowFileBrowser	Benutzer	Dateiübertragungen	
Sitzungserhaltungs- Timer	Session Timers	Aktiviert		
		(1)		

Studio-Richtlinie	Schlüssel	Typ	Modul	Standardwert
Sitzungsleerlauf-Timerintervall	Sitzungsleerlauf-Timer	Timer	Session	1440
	-		Timers	Minuten
Timer für getrennte Sitzungen - Timerintervall	Sitzungsleerlauf-Timer	Timer	Session	Deaktiviert
	-		Timers	(0)
Getrennte Sitzungen - Timerintervall	Getrennte Sitzungen - Timer	Timer	Session	1440
	-		Timers	Minuten

Hinweis:

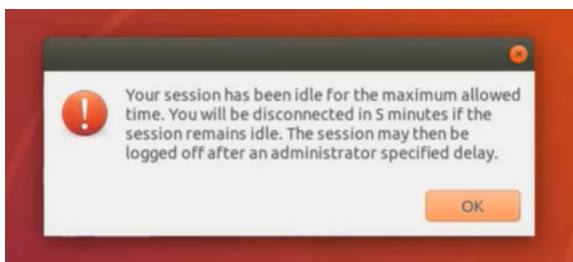
Nur der Windows Virtual Delivery Agent (VDA) unterstützt Audio über UDP (User Datagram Protocol). Der Linux VDA unterstützt dies nicht. Weitere Informationen finden Sie unter [Audio über User Datagram Protocol \(UDP\) –Echtzeitübertragung](#).

Sie können mit den folgenden Citrix Richtlinieneinstellungen Sitzungsverbindungstimer in Citrix Studio konfigurieren:

- **Sitzungsleerlauf-Timer:** Bestimmt, ob ein Zeitlimit für Sitzungen im Leerlauf erzwungen werden soll.
- **Sitzungsleerlauf - Timerintervall:** Legt ein Zeitlimit für Sitzungen im Leerlauf fest. Wenn der **Sitzungsleerlauf-Timer Aktiviert** ist und in einer aktiven Sitzung während der festgelegten Zeit keine Benutzereingabe erfolgt, wird die Sitzung getrennt.
- **Timer für getrennte Sitzung:** Bestimmt, ob ein Zeitlimit für getrennte Sitzungen erzwungen werden soll.
- **Getrennte Sitzungen - Timerintervall:** Legt ein Intervall fest, bevor eine getrennte Sitzung abgemeldet wird.

Wenn Sie eine der Richtlinieneinstellungen aktualisieren, achten Sie darauf, dass sie in der ganzen Bereitstellung konsistent sind.

A warning message appears when your time limit for idle sessions expires. Ein Beispiel sehen Sie im folgenden Screenshot. Pressing **OK** closes the warning message but cannot keep your session active. To keep your session active, provide user input to reset the idle timer.



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 Sprachencodern 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:

Primary selection update mode

Value: **Selection changes are not updated on neither client nor host**

☐ Use

▼ Apply

Virtual Desktop OS, 7.1 Desktop OS, 7.5 Server OS, 7.2 Desktop OS, 7.6 Server OS, 7.3 Desktop OS, 7.7 Server OS, 7.4 Desktop OS, 7.8 Server OS, 7.9 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Server OS, 7.17 Desktop OS, 7.18 Server OS, 7.18 Desktop OS, 7.19 Server OS, 7.19 Desktop OS

▼ Description

This setting is supported only by Linux VDA version 1.4 onwards.

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

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

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

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

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

▼ Related settings

Clipboard selection update mode

- **Auswähländerungen 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.
- **Auswähländerungen 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.
- **Auswähländerungen 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.

– **Auswähländerungen 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

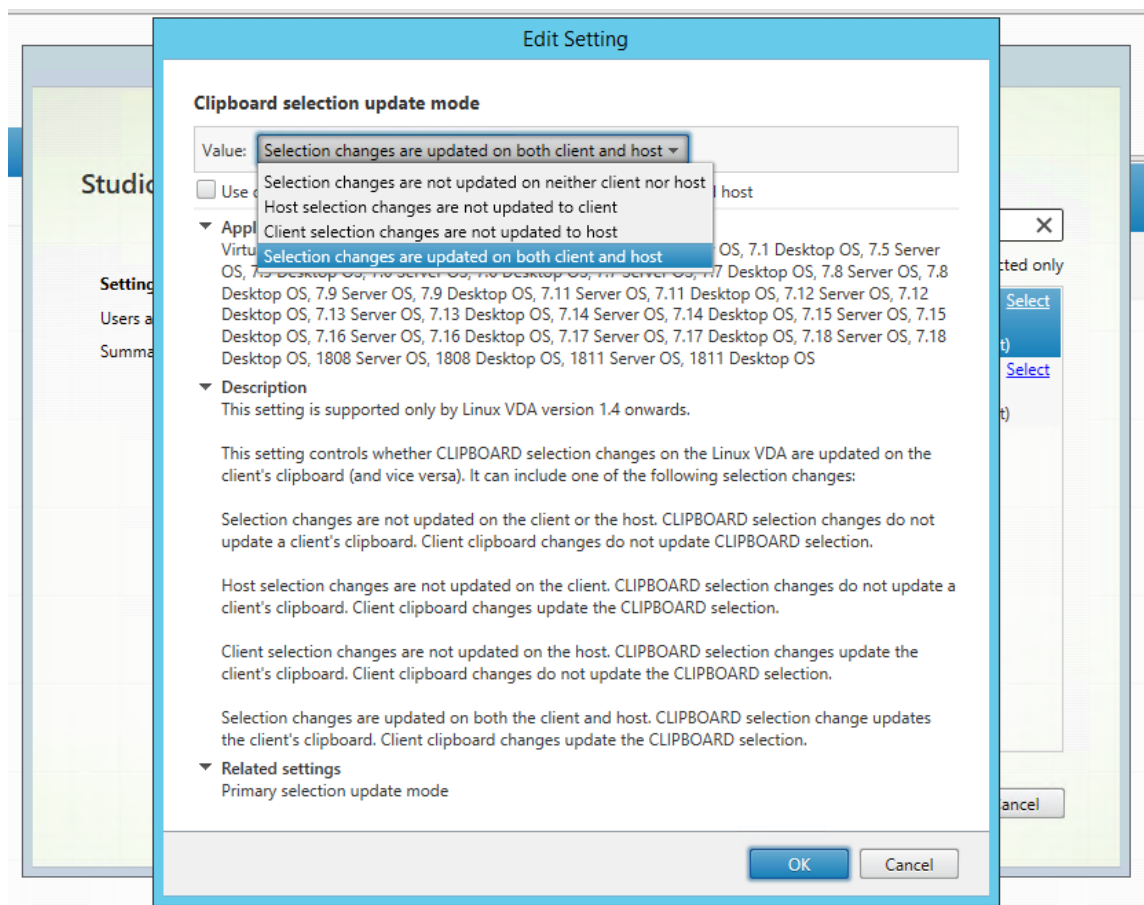
Wert (Aufzählung): [0, 1, 2, 3]

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.

Drucken

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Bewährte Methoden beim Drucken](#)
- [PDF-Druck](#)

Bewährte Methoden beim Drucken

October 5, 2022

Dieser Artikel enthält Informationen zu bewährten Druckmethoden.

Installation

Der Linux VDA benötigt die Filter **cups** und **foomatic**. Die Filter werden im Rahmen der VDA-Installation installiert. Sie können die Filter gemäß Ihrer Distribution auch manuell installieren. Beispiel:

Auf RHEL 7:

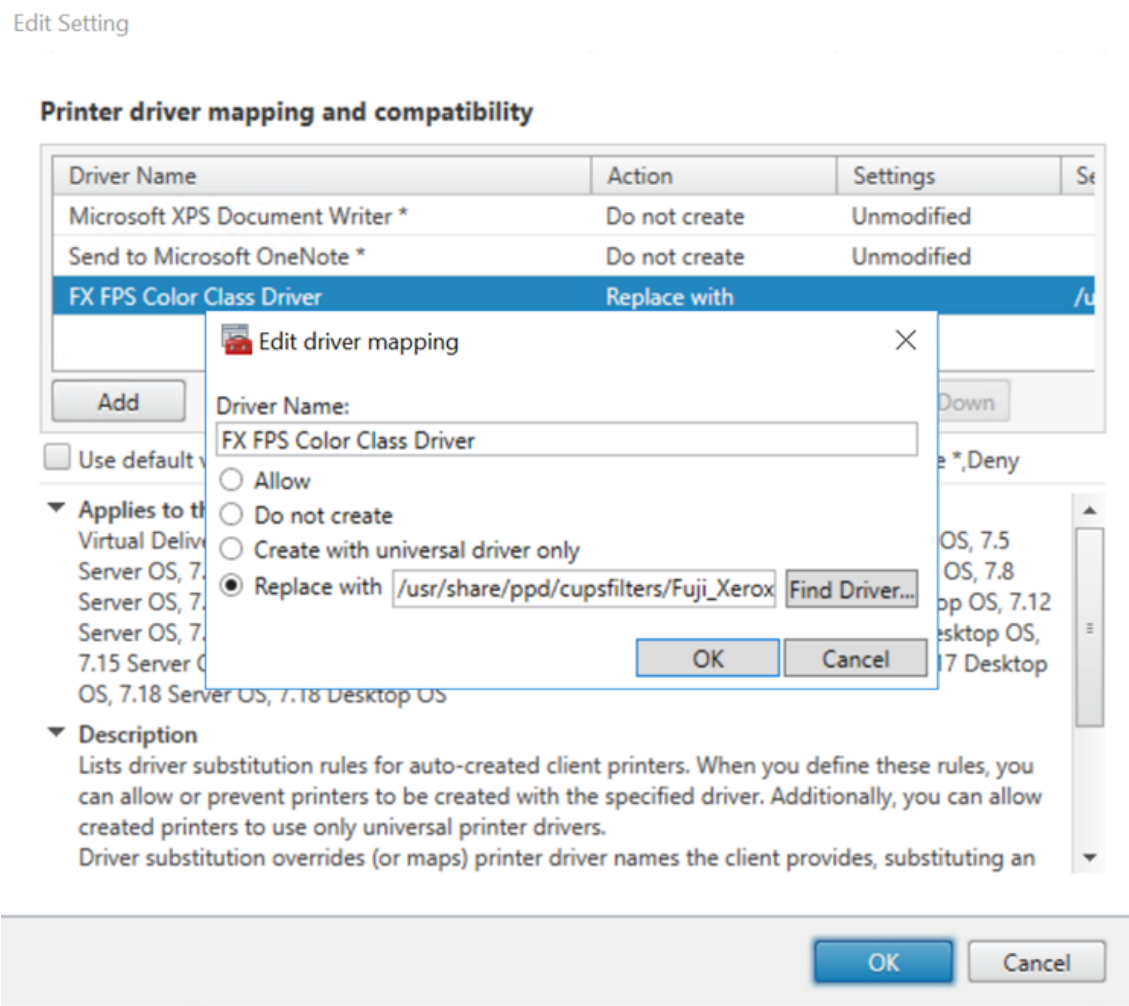
```
1 sudo yum -y install cups
2
3 sudo yum -y install foomatic-filters
4 <!--NeedCopy-->
```

Konfiguration

Citrix bietet drei universelle Druckertreibertypen: postscript, pcl5 und pcl6. Der universelle Druckertreiber ist unter Umständen nicht mit dem Clientdrucker kompatibel. In diesem Fall bestand in früheren Versionen die einzige Option darin, die Konfigurationsdatei ~/.CitrlpProfile\$CLIENT_NAME zu bearbeiten. Ab Version 1906 können Sie stattdessen auch die Richtlinie **Druckertreiberzuordnung und -kompatibilität** in Citrix Studio konfigurieren.

Konfigurieren der Richtlinie **Druckertreiberzuordnung und -kompatibilität** in Citrix Studio:

- 1. Wählen Sie die Richtlinie **Druckertreiberzuordnung und -kompatibilität** aus.
- 2. Klicken Sie auf **Hinzufügen**.
- 3. Geben Sie unter **Treibername** den Treibernamen des Clientdruckers ein. Bei Verwendung der Citrix Workspace-App für Linux geben Sie stattdessen den Druckernamen ein.
- 4. Wählen Sie **Ersetzen durch** und geben Sie den absoluten Pfad der Treiberdatei auf dem VDA ein.



Hinweis:

- Es werden nur PPD-Treiberdateien unterstützt.
- Andere Optionen der Richtlinie **Druckertreiberzuordnung und -kompatibilität** werden nicht unterstützt. Es wird nur **Ersetzen durch** wirksam.

Verwendung

Sie können aus veröffentlichten Desktops und veröffentlichten Anwendungen drucken. Nur der client-seitige Standarddrucker wird in einer Linux VDA-Sitzung zugeordnet. Die Druckernamen müssen für Desktops und Anwendungen unterschiedlich sein.

- 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 oder auf einem Anwendungsdrucker über einen veröffentlichten Desktop schlägt fehl.

Problembehandlung**Fehler beim Drucken**

Wenn das Drucken nicht ordnungsgemäß funktioniert, sollten Sie den Druckdaemon **ctxlpmngt** und das CUPS-Framework überprüfen.

Der Druckdaemon **ctxlpmngt** ist ein pro Sitzung ausgeführter Vorgang, der für die gesamte Sitzungsdauer ausgeführt werden muss. Mit dem folgenden Befehl prüfen Sie, ob der Druckdaemon ausgeführt wird. Wenn der Prozess **ctxlpmngt** nicht ausgeführt wird, starten Sie **ctxlpmngt** manuell über eine Befehlszeile.

```
1 ps -ef | grep ctxlpmngt
2 <!--NeedCopy-->
```

Wenn der Druck immer noch nicht funktioniert, überprüfen Sie das CUPS-Framework. Der Dienst **ctx-cups** dient zur Druckerverwaltung und kommuniziert mit dem Linux CUPS-Framework. Es gibt jeweils einen Prozess pro Maschine, der mit folgendem Befehl überprüft werden kann:

```
1 service ctx cups status
2 <!--NeedCopy-->
```

Zusätzliche Schritte zum Sammeln von CUPS-Protokollen

Führen Sie die folgenden Befehle aus, um die CUPS-Dienstdatei für das Sammeln von CUPS-Protokollen zu konfigurieren. Andernfalls können CUPS-Protokolle nicht in **hdx.log** aufgezeichnet werden:

```
1 sudo service cups stop
2
3 sudo vi /etc/systemd/system/printer.target.wants/cups.service
4
5 PrivateTmp=false
6
7 sudo service cups start
8
9 sudo systemctl daemon-reload
10 <!--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 **~/.CtclpProfile\$CLIENT_NAME** konfiguriert werden:

```
1 [DEFAULT_PRINTER]
2
3 printername=
4
5 model=
6
7 ppdpath=
8
9 drivertype=
10 <!--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 **drvertype**, 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**:

```
1  lpinfo -m
2
3  ...
4
5  xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
6
7  xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
8  xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
9
10 <!--NeedCopy-->
```

Sie können dann das Modell gemäß dem Drucker festlegen:

```
1  model=xerox/ph3115.ppd.gz
2  <!--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.

```
1  ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
2  <!--NeedCopy-->
```

- Citrix bietet drei universelle Druckertreibertypen: postscript, pcl5 und pcl6. Sie können den Treibertyp gemäß Ihren Druckereigenschaften konfigurieren.

Wenn der Standarddruckertreibertyp des Client beispielsweise PCL5 ist, definieren Sie **drvertype** wie folgt:

```
1  drvertype=pcl5
2  <!--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:

1. Melden Sie sich bei einer veröffentlichten Desktopsitzung an.
2. Führen Sie folgenden Befehl aus: **vi ~/.CtxlpProfile\$CLIENT_NAME**.
3. Fügen Sie das folgende Feld hinzu, um die Spooldatei auf dem Linux VDA zu speichern:

```
1 deletespoolfile=no
2 <!--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/\$login_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 mit einem anderen Druckertreiber.

8. Wechseln Sie den zugeordneten Drucker, um einen anderen Druckertreiber zu verwenden. Im folgenden Beispiel wird beispielsweise der PostScript-Clientdrucker verwendet:
 - a) Melden Sie sich bei einer aktiven Sitzung an und öffnen Sie einen Browser auf dem Clientdesktop.
 - b) Öffnen Sie das Druckverwaltungsportal:

```
1 localhost:631
2 <!--NeedCopy-->
```

- c) Wählen Sie den zugeordneten Drucker **CitrixUniversalPrinter:\$ClientName:app/dsk\$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 in den Feldern **Make** und **Model** einen anderen Druckertreiber als den Citrix UPD-Treiber aus. Wenn beispielsweise der virtuelle CUPS-PDF-Drucker installiert ist, wählen Sie den Druckertreiber “Generic CUPS-PDF Printer”. Speichern Sie die Änderung.
- f) Wenn der Vorgang Erfolg hat, konfigurieren Sie den PPD-Dateipfad des Treibers in **.Ctulp-Profile\$CLIENT_NAME** so, dass der zugeordnete Drucker den neu ausgewählten Treiber 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/s/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:

```
1 <Policy default>
2
3     # Job/subscription privacy...
4
5     JobPrivateAccess default
6
7     JobPrivateValues default
```

```
8
9     SubscriptionPrivateAccess default
10
11     SubscriptionPrivateValues default
12
13     ... ..
14
15     <Limit Create-Printer-Subscription>
16
17         Require user @OWNER
18
19         Order deny,allow
20
21     </Limit>
22
23     <Limit All>
24
25         Order deny,allow
26
27     </Limit>
28
29 </Policy>
30 <!--NeedCopy-->
```

PDF-Druck

October 5, 2022

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](#).

Remote-PC-Zugriff

October 5, 2022

Übersicht

Remote-PC-Zugriff ist eine Erweiterung von Citrix Virtual Apps and Desktops. Damit können Unternehmen einfach und sicher den Remotezugriff auf ihre physischen Büro-PCs ermöglichen. Wenn Benutzer auf ihre Büro-PCs zugreifen können, können sie auf alle Anwendungen, Daten und Ressourcen zugreifen, die sie für ihre Arbeit benötigen.

Remote-PC-Zugriff verwendet dieselben Citrix Virtual Apps and Desktops-Komponenten zum Bereitstellen von virtuellen Desktops und Anwendungen. Die Anforderungen und der Prozess für die Bereitstellung und Konfiguration des Remote-PC-Zugriffs sind mit den Anforderungen und dem Prozess für die Bereitstellung von Citrix Virtual Apps and Desktops identisch. Diese Einheitlichkeit bietet eine konsistente und gemeinsame administrative Erfahrung. Benutzer erhalten die beste Benutzererfahrung, wenn sie Citrix HDX für die Bereitstellung ihrer Büro-PC-Remotesitzungen verwenden.

Weitere Informationen finden Sie unter [Remote-PC-Zugriff](#) in der Citrix Virtual Apps and Desktops-Dokumentation.

Überlegungen

Diese Überlegungen gelten speziell für den Linux-VDA:

- Verwenden Sie auf physischen Maschinen den Linux VDA nur im Nicht-3D-Modus. Aufgrund von Einschränkungen des NVIDIA-Treibers kann der lokale Bildschirm des PCs nicht ausgeblendet werden, wenn der HDX 3D-Modus aktiviert ist. Das Anzeigen dieses Bildschirms ist ein potenzielles Sicherheitsrisiko.
- Verwenden Sie Maschinenkataloge des Typs “Einzelsitzungs-OS” für physische Linux-Maschinen.

- Die automatische Benutzerzuweisung ist für Linux-Maschinen nicht verfügbar. Bei automatischer Benutzerzuweisung werden Benutzer automatisch ihren Maschinen zugewiesen, wenn sie sich lokal an den PCs anmelden. Die Anmeldung erfolgt ohne Administratoreingriff. Die Citrix Workspace-App auf dem Client erleichtert Benutzern den Zugriff auf Anwendungen und Daten auf dem Büro-PC von der Remote-PC-Zugriff-Desktopsitzung aus.
- Wenn Benutzer bereits lokal an ihren PCs angemeldet sind, schlagen Versuche, die PCs über StoreFront zu starten, fehl.
- Energiesparoptionen sind für Linux-Maschinen nicht verfügbar.

Konfiguration

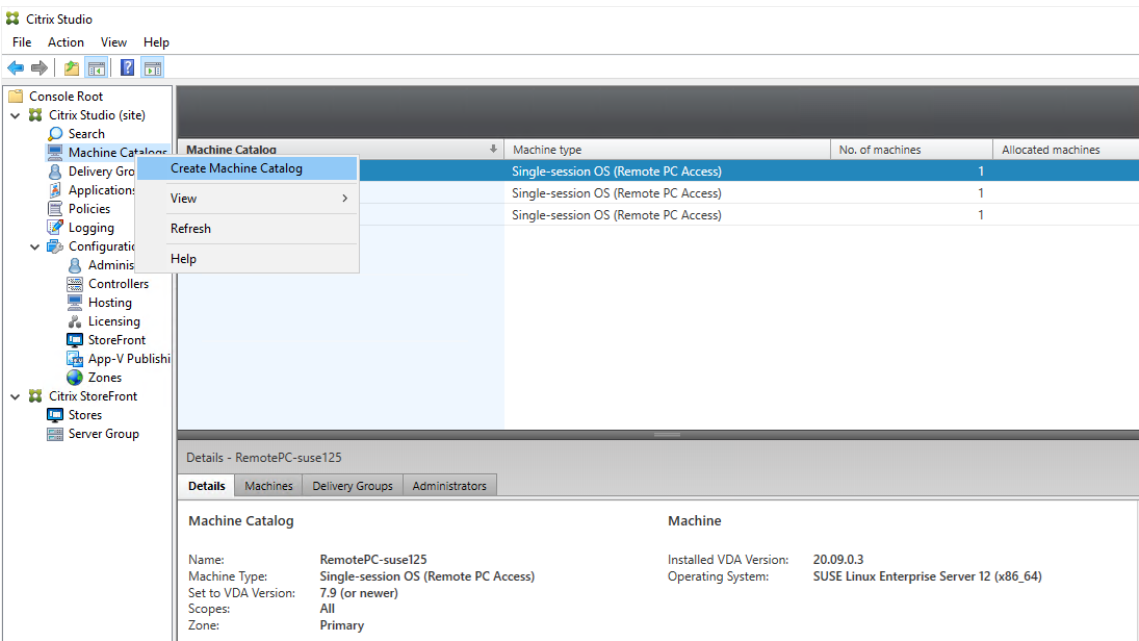
Um Linux-PC-Sitzungen bereitzustellen, installieren Sie den Linux VDA auf Ziel-PCs, erstellen Sie einen Maschinenkatalog vom Typ **Remote-PC-Zugriff** und erstellen Sie eine Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern. Im folgenden Abschnitt wird das Verfahren beschrieben:

Schritt 1 –Installieren des Linux VDA auf Ziel-PCs

Es wird empfohlen, den Linux VDA mit [Easy Install](#) zu installieren. Legen Sie während der Installation für die Variable `CTX_XDL_VDI_MODE` den Wert `Y` fest.

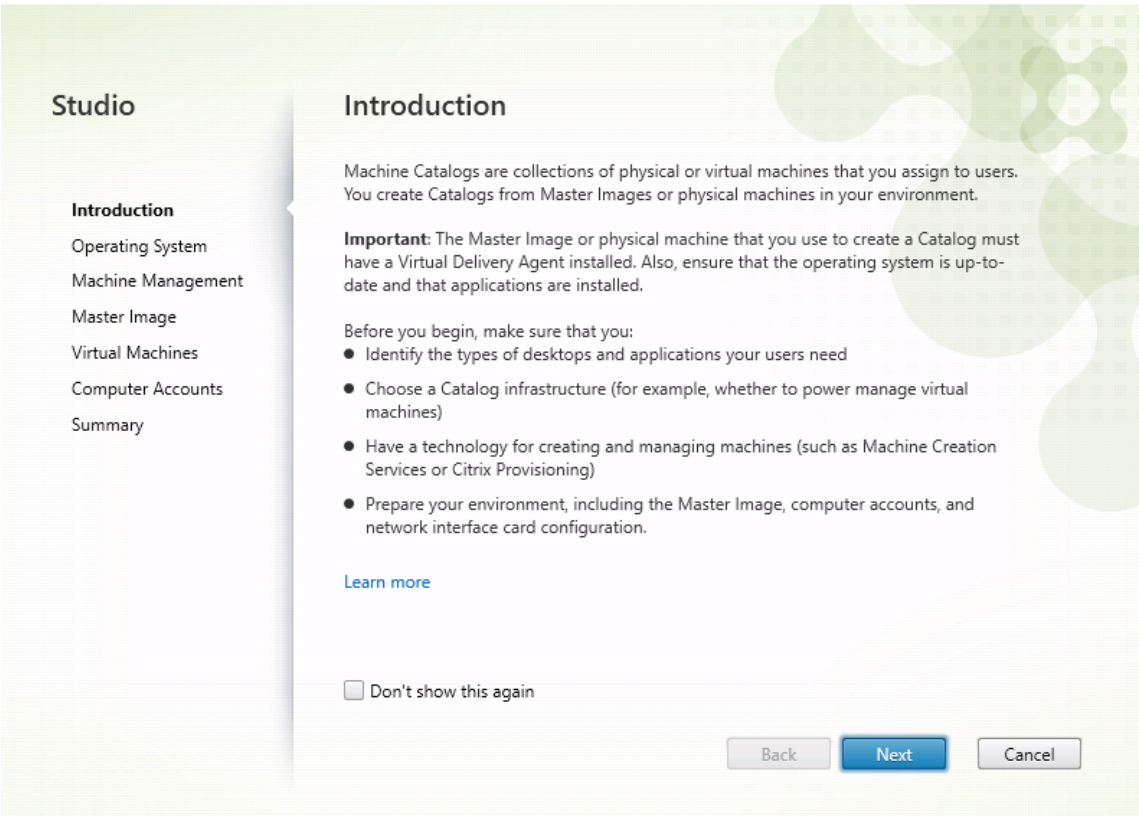
Schritt 2 –Erstellen eines Maschinenkatalogs vom Typ Remote-PC-Zugriff

1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Maschinenkataloge** und wählen Sie im Kontextmenü **Maschinenkatalog erstellen** aus.



2. Klicken Sie auf der Seite **Einführung auf Weiter**.

Machine Catalog Setup



3. Wählen Sie auf der Seite **Betriebssystem** die Option **Remote-PC-Zugriff** aus.

Machine Catalog Setup

Studio

- ✓ Introduction
- Operating System**
- Machine Accounts
- Summary

Operating System

Select an operating system for this Machine Catalog.

- ☐ Multi-session OS
The multi-session OS machine catalog provides hosted shared desktops for a large-scale deployment of standardized Windows multi-session OS or Linux OS machines.
- ☐ Single-session OS
The single-session OS machine catalog provides VDI desktops ideal for a variety of different users.
- ☒ Remote PC Access
The Remote PC Access machine catalog provides users with remote access to their physical office desktops, allowing them to work at any time.

There are currently no power management connections suitable for use with Remote PC Access, but you can create one after completing this wizard. Then edit this machine catalog to specify that connection.

Back Next Cancel

4. Klicken Sie auf **Organisationseinheiten hinzufügen**, um Organisationseinheiten auszuwählen, die die Ziel-PCs enthalten, oder klicken Sie auf **Maschinenkonten hinzufügen**, um dem Maschinenkatalog einzelne Maschinen hinzuzufügen.

Machine Catalog Setup

The screenshot shows the 'Machine Accounts' step of the 'Machine Catalog Setup' wizard. On the left, a sidebar titled 'Studio' contains a list of steps: 'Introduction', 'Operating System', 'Machine Accounts' (which is highlighted), and 'Summary'. The main area is titled 'Machine Accounts' and contains the following text: 'Machines in your network domain have an associated machine account. The machine account name is usually the same name as the machine. The machine accounts you choose must match the machines that users use for remote access. To add groups of machines by Organizational Units (OUs), select Add OUs.' Below this text, it says 'Select the machine accounts and/or OUs associated with your users:' followed by a large empty rectangular box with a light green patterned background. Below the box are three buttons: 'Add machine accounts...', 'Add OUs...' (which is highlighted with a blue border), and 'Remove'. Below these buttons is a dropdown menu with a blue information icon and the text 'Select the minimum functional level for this catalog:' followed by the value '7.9 (or newer)'. Below the dropdown, it says 'Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. [Learn more](#)'. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

Studio

- ✓ Introduction
- ✓ Operating System
- Machine Accounts**
- Summary

Machine Accounts

Machines in your network domain have an associated machine account. The machine account name is usually the same name as the machine. The machine accounts you choose must match the machines that users use for remote access. To add groups of machines by Organizational Units (OUs), select Add OUs.

Select the machine accounts and/or OUs associated with your users:

To get started, add a machine account or OU.
[Learn more](#)

Add machine accounts... Add OUs... Remove

i Select the minimum functional level for this catalog: 7.9 (or newer) ▾

Machines will require the selected VDA version (or newer) in order to register in Delivery Groups that reference this machine catalog. [Learn more](#)

Back Next Cancel

5. Benennen Sie den Maschinenkatalog.

Machine Catalog Setup

Studio

- ✓ Introduction
- ✓ Operating System
- ✓ Machine Accounts
- Summary**

Summary

Machine type:	Remote PC Access
Machines added:	1 organizational unit (OU)
VDA version:	7.9 (or newer)
Scopes:	-
Zone:	Primary

Machine Catalog name:

RemotePC_RHEL81

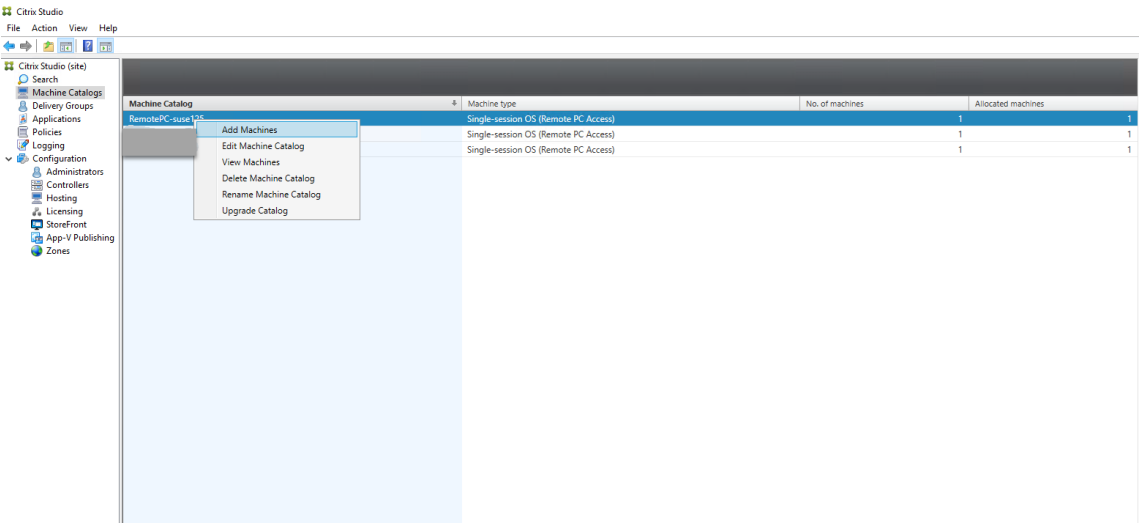
Machine Catalog description for administrators: (Optional)

Example: Windows 7 SP1 desktops for the London Sales office

To complete the deployment, assign this Machine Catalog to a Delivery Group by selecting Delivery Groups and then Create or Edit a Delivery Group.

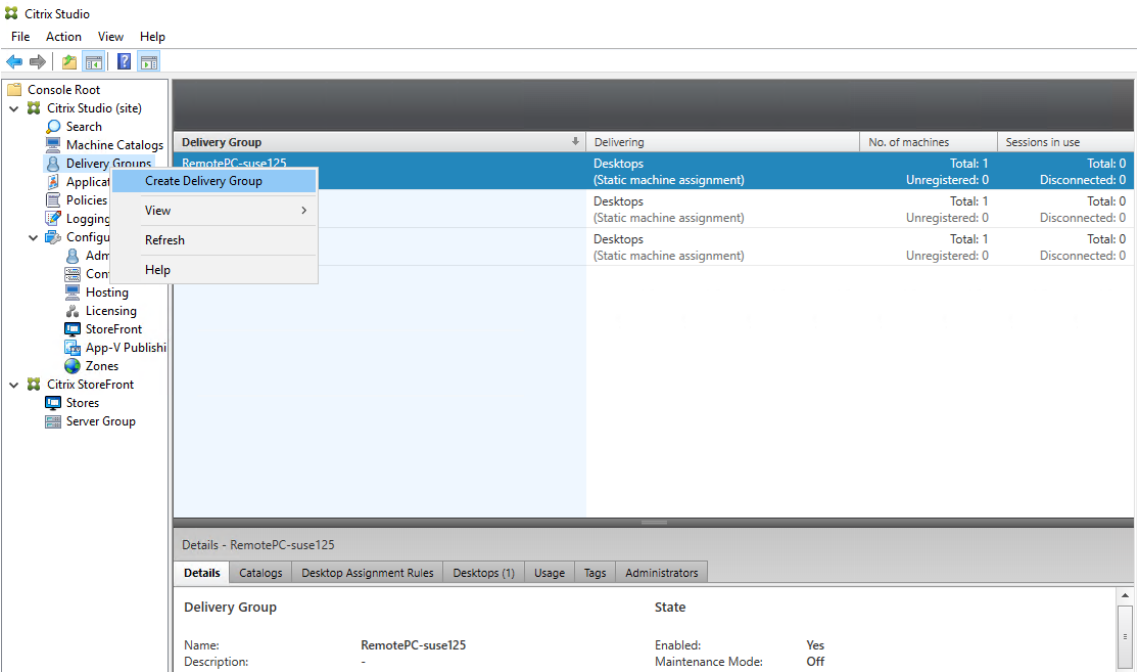
Back Finish Cancel

6. (Optional) Klicken Sie mit der rechten Maustaste auf den Maschinenkatalog, um relevante Vorgänge auszuführen.

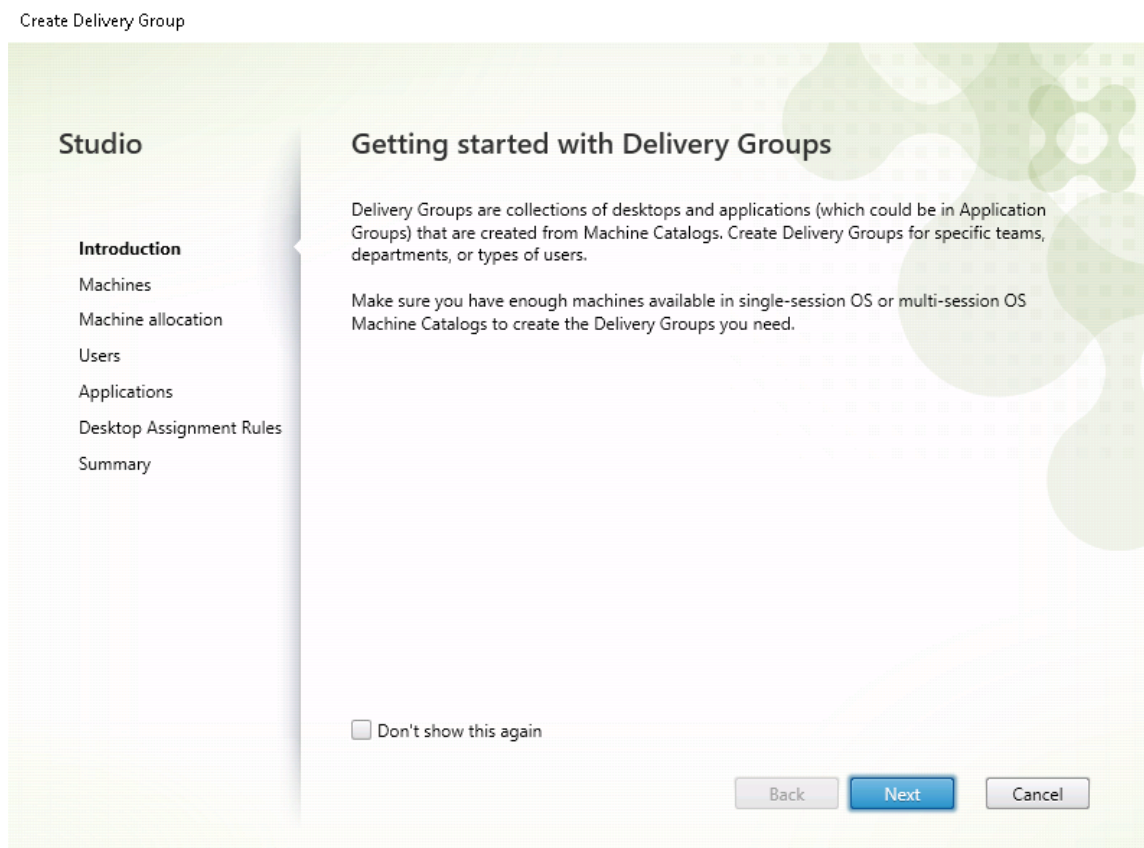


Schritt 3 –Erstellen einer Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern

1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Bereitstellungsgruppen** und wählen Sie im Kontextmenü **Bereitstellungsgruppe erstellen** aus.



2. Klicken Sie auf der Seite **Erste Schritte für Bereitstellungsgruppen** auf **Weiter**.



3. Wählen Sie den in Schritt 2 erstellten Maschinenkatalog aus, um ihn der Bereitstellungsgruppe zuzuordnen.

Create Delivery Group

Studio

- ✓ Introduction
- Machines**
- Machine allocation
- Users
- Applications
- Desktop Assignment Rules
- Summary

Machines

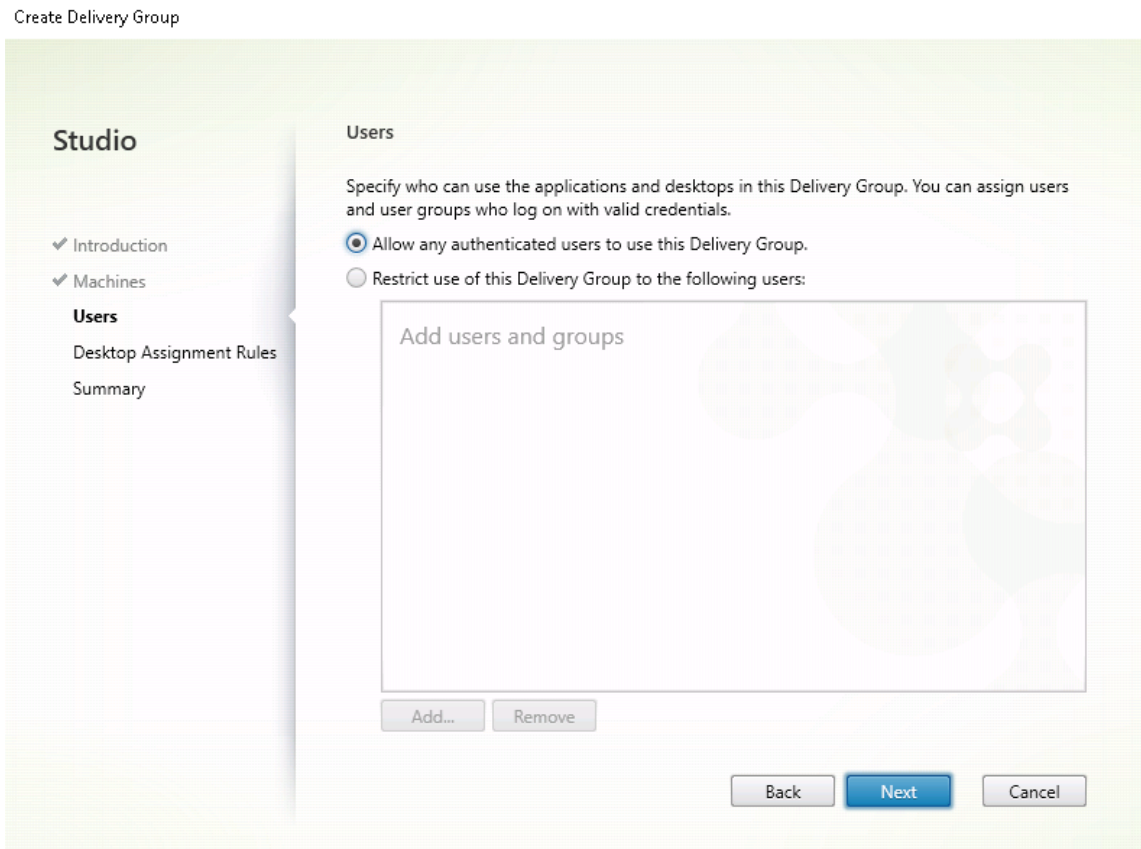
Select a Machine Catalog.

	Catalog	Type	Machines
<input type="radio"/>	RemotePC_2020_06	Remote PC Access	-
<input checked="" type="radio"/>	RemotePC_RHEL81	Remote PC Access	-

i This will set up an association between this Delivery Group and the selected Catalog. This association means machine accounts added to the Remote PC Access catalog in the future, will automatically be assigned to this Delivery Group.

Back Next Cancel

4. Fügen Sie Benutzer hinzu, die auf die PCs im Maschinenkatalog zugreifen können. Die von Ihnen hinzugefügten Benutzer können mit der Citrix Workspace App auf einem Clientgerät remote auf die PCs zugreifen.



Wake-On-LAN

Remote-PC-Zugriff unterstützt Wake-On-LAN, sodass physische PCs remote eingeschaltet werden können. Dieses Feature ermöglicht es Benutzern, ihre Büro-PCs ausgeschaltet zu lassen, wenn diese nicht verwendet werden, um Energiekosten zu sparen. Außerdem ist ein Remotezugriff möglich, wenn Maschinen unabsichtlich ausgeschaltet wurden.

Mit dem Wake-On-LAN-Feature werden die Magic Packets auf Befehl des Delivery Controllers direkt vom VDA, der auf dem PC ausgeführt wird, an das Subnetz gesendet, in dem sich der PC befindet. Dadurch kann das Feature ohne Abhängigkeiten von zusätzlichen Infrastrukturkomponenten oder Drittanbieterlösungen für die Bereitstellung von Magic Packets funktionieren.

Das Wake-On-LAN-Feature unterscheidet sich vom älteren SCCM-basierten Wake-On-LAN-Feature. Weitere Informationen zu SCCM-basiertem Wake-on-LAN finden Sie unter [Wake-On-LAN –SCCM-integriert](#).

Systemanforderungen

Folgende Systemanforderungen gelten für die Verwendung des Wake-On-LAN-Feature:

- Steuerungsebene:
 - Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
 - Citrix Virtual Apps and Desktops 2012 oder höher
- Physische PCs:
 - VDA-Version 2012 oder höher
 - Wake-On-LAN, aktiviert im BIOS und auf der Netzwerkkarte

Konfigurieren von Wake-On-LAN

Derzeit kann integriertes Wake-On-LAN nur mit PowerShell konfiguriert werden.

Konfigurieren von Wake-On-LAN:

1. Erstellen Sie den Maschinenkatalog für den Remote-PC-Zugriff (falls noch nicht vorhanden).
2. Erstellen Sie die Wake-On-LAN-Hostverbindung (falls noch nicht vorhanden).

Hinweis:

Wenn Sie über eine Hostverbindung vom Typ "Microsoft Configuration Manager Wake-On-LAN" verfügen, erstellen Sie eine Hostverbindung, um das Wake-On-LAN-Feature zu verwenden.

3. Rufen Sie den eindeutigen Bezeichner der Wake-On-LAN-Hostverbindung ab.
4. Ordnen Sie die Wake-On-LAN-Hostverbindung einem Maschinenkatalog zu.

Erstellen der Wake-On-LAN-Hostverbindung:

```
1 # Load Citrix SnapIns
2 Add-PSSnapIn -Name "*citrix*"
3
4 # Provide the name of the Wake on LAN host connection
5 [string]$connectionName = "Remote PC Access Wake on LAN"
6
7 # Create the hypervisor connection
8 $hypHc = New-Item -Path xdhyp:\Connections `
9             -Name $connectionName `
10            -HypervisorAddress "N/A" `
11            -UserName "woluser" `
12            -Password "wolpwd" `
13            -ConnectionType Custom `
14            -PluginId VdaWOLMachineManagerFactory `
15            -CustomProperties "<CustomProperties></CustomProperties>" `
16            -Persist
17
```

```

18 $bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
    $hypHc.HypervisorConnectionUid
19
20 # Wait for the connection to be ready before trying to use it
21 while (-not $bhc.IsReady)
22 {
23
24     Start-Sleep -s 5
25     $bhc = Get-BrokerHypervisorConnection -
        HypHypervisorConnectionUid $hypHc.HypervisorConnectionUid
26 }
27
28 <!--NeedCopy-->

```

Wenn die Hostverbindung bereit ist, führen Sie die folgenden Befehle aus, um den eindeutigen Bezeichner der Hostverbindung abzurufen:

```

1 $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2 $hypUid = $bhc.Uid
3 <!--NeedCopy-->

```

Nachdem Sie den eindeutigen Bezeichner der Verbindung abgerufen haben, führen Sie die folgenden Befehle aus, um die Verbindung dem Remote-PC-Zugriff-Maschinenkatalog zuzuordnen:

```

1 Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
2 <!--NeedCopy-->

```

5. Aktivieren Sie Wake-On-LAN im BIOS und auf der Netzwerkkarte auf jeder VM im Maschinenkatalog.

Hinweis: Die Methode zum Aktivieren von Wake-On-LAN variiert je nach Maschinenkonfiguration.

- Aktivieren von Wake-On-LAN im BIOS:
 - a) Öffnen Sie das BIOS und aktivieren Sie das Wake-On-LAN-Feature.
Die Methode für den Zugriff auf das BIOS hängt vom Hersteller der Hauptplatine und dem von ihm gewählten BIOS-Anbieter ab.
 - b) Speichern Sie Ihre Einstellungen und starten Sie die Maschine neu.
- Aktivieren von Wake-On-LAN auf der Netzwerkkarte:
 - a) Prüfen Sie mit dem Befehl `sudo ethtool <NIC>`, ob Ihre Netzwerkkarte Magic Packets unterstützt.
<NIC> ist der Gerätenamen Ihrer Netzwerkkarte, also beispielsweise `eth0`. Der Befehl `sudo ethtool <NIC>` liefert Angaben zu den Fähigkeiten Ihrer Netzwerkkarte:

- Wenn die Befehlsausgabe eine Zeile wie `Supports Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` enthält, unterstützt Ihre Netzwerkkarte die Wake-On-LAN-Methode mit Magic Packets.
 - Wenn die Befehlsausgabe eine Zeile wie `Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` und nicht den Buchstaben `d` enthält, ist die Wake-On-LAN-Methode mit Magic Packets aktiviert. Wenn `<letters>` jedoch den Buchstaben `d` enthält, ist das Wake-On-LAN-Feature deaktiviert. Führen Sie in diesem Fall den Befehl `sudo ethtool -s <NIC> wol g` aus, um Wake-On-LAN zu aktivieren.
- b) Bei den meisten Distributionen ist der Befehl `sudo ethtool -s <NIC> wol g` nach jedem Start erforderlich. Um die Option dauerhaft festzulegen, führen Sie die folgenden Schritte basierend auf Ihren Distributionen aus:

Ubuntu:

Fügen Sie in der Schnittstellenkonfigurationsdatei `/etc/network/interfaces` die Zeile `up ethtool -s <NIC> wol g` hinzu. Beispiel:

```
1 # ifupdown has been replaced by netplan(5) on this system.
   See
2 # /etc/netplan for current configuration.
3 # To re-enable ifupdown on this system, you can run:
4 # sudo apt install ifupdown
5 auto eth0
6 iface eth0 inet static
7     address 10.0.0.1
8     netmask 255.255.240.0
9     gateway 10.0.0.1
10    up ethtool -s eth0 wol g
11 <!--NeedCopy-->
```

RHEL/SUSE:

Fügen Sie der Schnittstellenkonfigurationsdatei `/etc/sysconfig/network-scripts/ifcfg-<NIC>` den Parameter `ETHTOOL_OPTS` hinzu :

```
1 ETHTOOL_OPTS="-s ${
2   DEVICE }
3   wol g"
4 <!--NeedCopy-->
```

Designüberlegungen

Wenn Sie planen, Wake-On-LAN mit Remote-PC-Zugriff zu verwenden, sollten Sie Folgendes beachten:

- Mehrere Maschinenkataloge können dieselbe Wake-On-LAN-Hostverbindung verwenden.
- Damit ein PC einen anderen PC reaktivieren kann, müssen beide PCs sich im gleichen Subnetz

befinden und dieselbe Wake-On-LAN-Hostverbindung verwenden. Die PCs können sich im gleichen oder in unterschiedlichen Maschinenkatalogen befinden.

- Hostverbindungen werden bestimmten Zonen zugewiesen. Wenn Ihre Bereitstellung mehr als eine Zone enthält, benötigen Sie in jeder Zone eine Wake-On-LAN-Hostverbindung. Gleiches gilt für Maschinenkataloge.
- Magic Packets werden mit der globalen Broadcast-Adresse 255.255.255.255 übertragen. Stellen Sie sicher, dass diese Adresse nicht blockiert ist.
- Um Maschinen in einem Subnetz zu reaktivieren, muss in diesem Subnetz (für jede Wake-On-LAN-Verbindung) mindestens ein PC aktiviert sein.

Operative Überlegungen

Berücksichtigen Sie Folgendes bei der Verwendung des Wake-On-LAN-Features:

- Der VDA muss sich mindestens einmal registrieren, bevor der PC über die integrierte Wake-On-LAN-Funktion reaktiviert werden kann.
- Wake-on-LAN kann nur zum Reaktivieren von PCs verwendet werden. Andere Energieaktionen wie Neustart oder Herunterfahren werden nicht unterstützt.
- Nachdem die Wake-On-LAN-Verbindung erstellt wurde, ist sie in Studio sichtbar. Das Bearbeiten ihrer Eigenschaften in Studio wird jedoch nicht unterstützt.
- Es gibt zwei Situationen, in denen ein Magic Packet gesendet wird:
 - Ein Benutzer versucht, eine Sitzung auf dem PC zu starten und der VDA ist nicht registriert.
 - Ein Administrator sendet manuell einen Einschaltbefehl über Studio oder PowerShell.
- Da der Delivery Controller den Energiezustand eines PCs nicht kennt, wird in Studio unter “Energiezustand” **Nicht unterstützt** angezeigt. Der Delivery Controller ermittelt anhand des VDA-Registrierungsstatus, ob ein PC ein- oder ausgeschaltet ist.

Weitere Ressourcen

Im Folgenden finden Sie weitere Ressourcen für Remote-PC-Zugriff:

- Solution design guidance: [Remote PC Access Design Decisions](#).
- Remote-PC-Zugriff-Musterarchitekturen: [Referenzarchitektur für Citrix Remote-PC-Zugriff-Lösung](#).

Sitzungsfortbestehen

October 5, 2022

Dieser Abschnitt behandelt die folgenden Themen:

- [Adaptiver Transport](#)
- [Anmeldung mit einem temporären Basisverzeichnis](#)
- [Veröffentlichen von Anwendungen](#)
- [Sitzungszuverlässigkeit](#)
- [Rendezvous V1](#)
- [Rendezvous V2](#)
- [Sichere Benutzersitzungen mit TLS](#)
- [Sichere Benutzersitzungen mit DTLS](#)

Adaptiver Transport

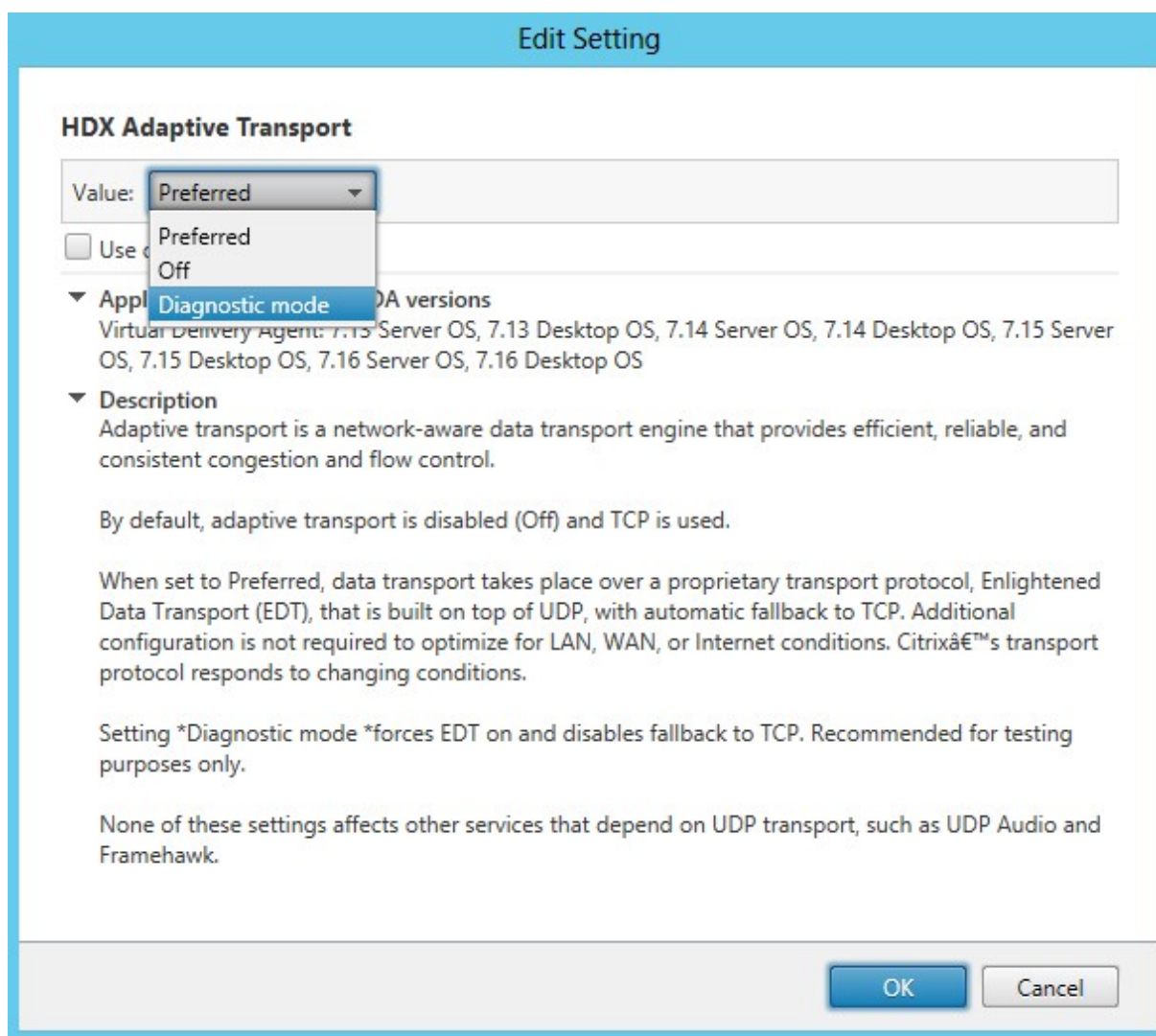
October 5, 2022

Adaptiver Transport ist eine Datenübertragungsmethode für Citrix Virtual Apps and Desktops. Sie ist schneller, skalierbarer, verbessert die Anwendungsinteraktivität und ist bei schwierigen Langstrecken-WAN- und Internetverbindungen interaktiver. Informationen zum adaptiven Transport finden Sie unter [Adaptiver Transport](#).

Aktivieren des adaptiven Transports

Vergewissern Sie sich in Citrix Studio, dass die Richtlinie **Adaptiver HDX-Transport** auf den Modus **Bevorzugt** oder **Diagnose** festgelegt ist. **Bevorzugt** ist standardmäßig ausgewählt.

- **Bevorzugt:** Nach Möglichkeit wird adaptiver Transport über EDT (Enlightened Data Transport) verwendet, andernfalls erfolgt ein Fallback auf TCP.
- **Diagnose:** EDT wird erzwungen und das Fallback auf TCP wird deaktiviert.



Deaktivieren des adaptiven Transports

Um den adaptiven Transport zu deaktivieren, legen Sie die Richtlinie **Adaptiver HDX-Transport** in Citrix Studio auf **Aus** fest.

Überprüfen, ob der adaptive Transport aktiviert ist

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob UDP-Listener ausgeführt werden:

```
1 netstat -an | grep "1494|2598"
2 <!--NeedCopy-->
```

Normalerweise sieht die Ausgabe in etwa so aus:

```
1 udp          0          0 0.0.0.0:2598      0.0.0.0:*
```

```
2
3  udp          0          0 :::1494      :::*
4  <!--NeedCopy-->
```

MTU-Discovery durch EDT

EDT ermittelt bei der Einrichtung einer Sitzung automatisch die maximale Übertragungseinheit (MTU). Dadurch wird eine EDT-Paketfragmentierung verhindert, die zu einer Leistungsminderung oder einem Fehler beim Einrichten der Sitzung führen kann.

Mindestanforderungen:

- Linux VDA 2012
- Citrix Workspace-App 1911 für Windows
- Citrix ADC:
 - 13.0.52.24
 - 12.1.56.22
- Sitzungszuverlässigkeit muss aktiviert sein.

Bei Verwendung von Clientplattformen oder Versionen, die dieses Feature nicht unterstützen, können Sie eine benutzerdefinierte EDT-MTU konfigurieren, die für Ihre Umgebung geeignet ist. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX231821](#).

Warnung:

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des **Registrierungs-Editors** zurückzuführen sind, behoben werden können. Die Verwendung des **Registrierungs-Editors** geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Aktivieren oder Deaktivieren der MTU-Discovery durch EDT auf dem VDA

Die MTU-Discovery durch EDT ist standardmäßig deaktiviert.

- Um die MTU-Discovery durch EDT zu aktivieren, setzen Sie mit folgendem Befehl den Registrierungsschlüssel `MtuDiscovery`, starten den VDA neu und warten, bis der VDA registriert ist:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd"-t "REG_DWORD"-v "MtuDiscovery"-d "0x00000001"--force
```

- Zum Deaktivieren der MTU-Discovery durch EDT löschen Sie den Registrierungswert `MtuDiscovery`.

Steuern der MTU-Discovery durch EDT auf dem Client

Sie können die MTU-Discovery durch EDT selektiv auf Clients steuern, indem Sie den Parameter `MtuDiscovery` in der ICA-Datei hinzufügen. Um das Feature zu deaktivieren, legen Sie im Abschnitt `Application` Folgendes fest:

```
MtuDiscovery=Off
```

Um das Feature wieder zu aktivieren, löschen Sie den Parameter `MtuDiscovery` aus der ICA-Datei.

Wichtig:

Dieser Parameter in der ICA-Datei funktioniert nur, wenn Sie die MTU-Discovery durch EDT auf dem VDA aktivieren. Ist die MTU-Discovery durch EDT auf dem VDA nicht aktiviert, zeigt der Parameter in der ICA-Datei keine Wirkung.

Benutzerdefinierte Hintergründe und Bannermeldungen auf Anmeldebildschirmen

October 5, 2022

Mit den folgenden Befehlen können Sie auf dem **Anmeldebildschirm** einer Sitzung einen benutzerdefinierten Hintergrund oder eine Bannermeldung hinzufügen. Um beides (Hintergrund und Bannermeldung) zum **Anmeldebildschirm** einer Sitzung hinzuzufügen, können Sie die Bannermeldung in das Hintergrundbild einbetten.

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v  
    "LogonDisplayString" -d "<text of custom logon banner message>" --  
    force  
2 <!--NeedCopy-->
```

```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v  
    "BackgroundImagePath" -d "<path to your custom logon screen  
    background image>" --force  
2 <!--NeedCopy-->
```

Um das Feature in SUSE 15.3 zu verwenden, installieren Sie `imlib2` von <http://download.opensuse.org/distribution/leap/15.3/repo/oss/>.

Tipp:

Wenn Sie eine benutzerdefinierte Bannermeldung mit LogonDisplayString hinzufügen, ist der Hintergrund des Anmeldebildschirms standardmäßig blau.

Anmeldung mit einem temporären Basisverzeichnis

October 5, 2022

Sie können ein temporäres Basisverzeichnis angeben, das verwendet wird, wenn der Bereitstellungspunkt auf dem Linux VDA fehlschlägt. Wenn ein temporäres Basisverzeichnis angegeben ist, wird bei der Sitzungsanmeldung eine Eingabeaufforderung angezeigt, wenn der Bereitstellungspunkt fehlschlägt. Benutzerdaten werden dann im temporären Basisverzeichnis gespeichert.

Die folgende Tabelle enthält Registrierungsschlüssel, die das Festlegen der Einstellungen für Ihr Basisverzeichnis erleichtern.

Registrierungsschlüssel	Beschreibung	Befehl
LogNoHome	Legt fest, ob Benutzer sich an Sitzungen ohne Basisverzeichnis anmelden können. Der Standardwert ist 1 und bedeutet "Ja". Wenn der Wert auf 0 gesetzt ist, werden Sitzungsanmeldungen ohne Basisverzeichnis deaktiviert.	<code>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "LogNoHome"-d "0x00000001"--force</code>

Registrierungsschlüssel	Beschreibung	Befehl
<code>HomeMountPoint</code>	Richtet einen lokalen Bereitstellungspunkt auf dem Linux VDA ein. Wenn der Bereitstellungspunkt beispielsweise <code>/mnt/home</code> ist, ist das Basisverzeichnis eines Benutzers <code>/mnt/home/domain/<user_name></code> . Stellen Sie sicher, dass der Bereitstellungspunkt mit dem Basisverzeichnis des Benutzers in Ihrer Umgebung übereinstimmt.	<code>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "HomeMountPoint"-d "<A directory where the NFS share is to be mounted>"--force</code>
<code>TempHomeDirectoryPath</code>	Richtet ein temporäres Basisverzeichnis auf dem Linux VDA ein für den Fall, dass der Bereitstellungspunkt fehlschlägt. Der Standardwert ist <code>/tmp</code> . Der Registrierungsschlüssel ist abhängig von <code>HomeMountPoint</code> . Er wird nur wirksam, wenn der Bereitstellungspunkt vom System als nicht verfügbar erkannt wird. Ein temporäres Basisverzeichnis für einen Benutzer ist <code>/tmp/domain/user_id</code> .	<code>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "TempHomeDirectoryPath"-d "</tmp by default>"--force</code>
<code>RemoveHomeOnLogoff</code>	Legt fest, ob temporäre Basisverzeichnisse nach der Abmeldung des Benutzers zu entfernen sind. 1 bedeutet "Ja". 0 bedeutet "Nein".	<code>create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "RemoveHomeOnLogoff"-d "0x00000000"--force</code>

Veröffentlichen von Anwendungen

October 5, 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).

Hinweis:

- Achten Sie beim Konfigurieren von Bereitstellungsgruppen darauf, als Bereitstellungstyp **Desktop und Anwendungen** oder **Anwendungen** festzulegen.
- 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, empfehlen wir, für App- und Desktop-Bereitstellungen separate Bereitstellungsgruppen zu erstellen.
- 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.

Einschränkung

Der Linux VDA unterstützt keinen Start mehrerer Instanzen einer Anwendung durch einen Benutzer.

In App-Sitzungen funktionieren nur App-spezifische Verknüpfungen einwandfrei.

Bekannte Probleme

Beim Veröffentlichen von Anwendungen sind folgende Probleme bekannt:

- 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.
- 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/title/Qt>.

Rendezvous V1

October 5, 2022

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerebene herzustellen.

Es sind zwei Arten von Datenverkehr zu berücksichtigen: 1) Steuerungsdatenverkehr für die VDA-Registrierung und die Sitzungsvermittlung; 2) HDX-Sitzungsdatenverkehr.

Rendezvous V1 ermöglicht es, dass HDX-Sitzungsdatenverkehr Cloud Connectors umgeht. Cloud Connectors sind jedoch weiterhin erforderlich, um als Proxy für den gesamten Steuerungsdatenverkehr für die VDA-Registrierung und das Sitzungsbrokering zu fungieren.

Anforderungen

- Zugriff auf die Umgebung mit Citrix Workspace und Citrix Gateway Service.
- Steuerungsebene: Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- Linux VDA Version 2112 oder höher.
 - Version 2112 ist die erforderliche Mindestversion für nicht transparente HTTP-Proxys.
 - Version 2204 ist die erforderliche Mindestversion für transparente Proxys und SOCKS5-Proxys.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix Richtlinie. Weitere Informationen finden Sie unter [Richtlinieneinstellung für Rendezvous-Protokoll](#).

- Die VDAs müssen Zugriff auf https://*.nssvc.net einschließlich aller Unterdomänen haben. Wenn Sie nicht alle Unterdomänen auf diese Weise auf die Positivliste setzen können, verwenden Sie stattdessen https://*.c.nssvc.net und https://*.g.nssvc.net. Weitere Informationen finden Sie im Abschnitt [Anforderungen an die Internetkonnektivität](#) der Citrix Cloud-Dokumentation (unter “Virtual Apps and Desktops Service”) und im Knowledge Center-Artikel [CTX270584](#).
- Cloud Connectors müssen beim Brokering einer Sitzung die FQDNs der VDAs abrufen. Um dieses Ziel zu erreichen, aktivieren Sie die DNS-Auflösung für die Site: Führen Sie mit dem Remote PowerShell SDK von Citrix DaaS den Befehl `Set-BrokerSite -DnsResolutionEnabled $true` aus. Weitere Informationen zum Remote PowerShell SDK von Citrix DaaS finden Sie unter [SDKs und APIs](#).

Proxykonfiguration

Der VDA unterstützt Rendezvous-Verbindungen über HTTP- und SOCKS5-Proxys.

Überlegungen zum Proxy

Berücksichtigen Sie Folgendes, wenn Sie Proxys mit Rendezvous verwenden:

- Nicht transparente HTTP-Proxys und SOCKS5-Proxys werden unterstützt.
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der ICA-Datenverkehr zwischen dem VDA und Gateway Service nicht abgefangen, entschlüsselt oder überprüft wird. Ansonsten bricht die Verbindung ab.
- HTTP-Proxys unterstützen die maschinenbasierte Authentifizierung über Aushandlungs- und Kerberos-Authentifizierungsprotokolle. Wenn Sie eine Verbindung mit dem Proxyserver herstellen, wählt das Aushandlungsauthentifizierungsschema automatisch das Kerberos-Protokoll aus. Kerberos ist das einzige Schema, das vom Linux VDA unterstützt wird.

Hinweis:

Um Kerberos zu verwenden, müssen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver erstellen und ihn mit dem Active Directory-Konto des Proxys verknüpfen. Der VDA generiert den Dienstprinzipalnamen (SPN) im Format `HTTP/<proxyURL>` beim Einrichten einer Sitzung, wobei die Proxy-URL aus der Richtlinieneinstellung **Rendezvousproxy** abgerufen wird. Wenn Sie keinen Dienstprinzipalnamen erstellen, schlägt die Authentifizierung fehl.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Bei Verwendung eines SOCKS5-Proxy müssen Sie eine Ausnahme konfigurieren, damit Datenverkehr an die in

den Anforderungen angegebenen Gateway Service-Adressen die Authentifizierung umgehen kann.

- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Verwenden Sie für einen HTTP-Proxy TCP als Transportprotokoll für ICA.

Transparenter Proxy

Rendezvous-Verbindungen über transparente HTTP-Proxys werden unterstützt. Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist auf dem VDA keine zusätzliche Konfiguration erforderlich.

Nicht transparenter Proxy

Wenn Sie einen nicht transparenten Proxy in Ihrem Netzwerk verwenden, konfigurieren Sie die Einstellung [Rendezvousproxykonfiguration](#). Wenn die Einstellung aktiviert ist, geben Sie die HTTP- oder SOCKS5-Proxyadresse an, damit der VDA weiß, welcher Proxy zu verwenden ist. Beispiel:

- Proxyadresse: `http://<URL or IP>:<port>` oder `socks5://<URL or IP>:<port>`

Rendezvous-Validierung

Wenn alle Anforderungen erfüllt sind, überprüfen Sie folgendermaßen, ob Rendezvous verwendet wird:

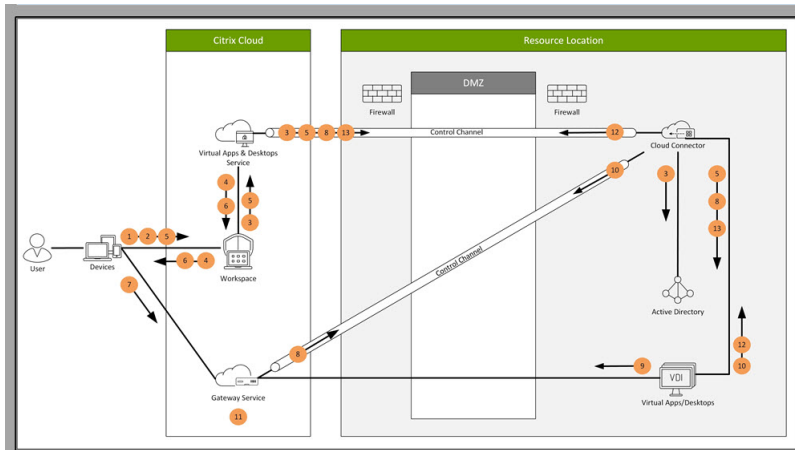
1. Starten Sie ein Terminal auf dem VDA.
2. Führen Sie `/opt/Citrix/VDA/bin/ctxquery -f iP` aus.
3. Die verwendeten TRANSPORTPROTOKOLLE geben die Art der Verbindung an:
 - TCP-Rendezvous: TCP - TLS - CGP - ICA
 - EDT-Rendezvous: UDP - DTLS - CGP - ICA
 - Proxy über Cloud Connector: TCP - PROXY - SSL - CGP - ICA oder UDP - PROXY - DTLS - CGP - ICA

Tipp:

Wenn der VDA bei aktiviertem Rendezvous den Citrix Gateway Service nicht direkt erreichen kann, greift der VDA auf eine Proxyumleitung der HDX-Sitzung über den Cloud Connector zurück.

Funktionsweise von Rendezvous

Diese Abbildung bietet eine Übersicht über den Rendezvous-Verbindungsfluss.



Folgen Sie den Schritten, um den Fluss zu verstehen.

1. Navigieren Sie zu Citrix Workspace.
2. Geben Sie die Anmeldeinformationen in Citrix Workspace ein.
3. Wenn Sie Active Directory on-premises verwenden, authentifiziert Citrix DaaS die Anmeldeinformationen mit Active Directory über den Cloud Connector-Kanal.
4. Citrix Workspace zeigt enumerierte Ressourcen aus Citrix DaaS an.
5. Wählen Sie Ressourcen aus Citrix Workspace aus. Citrix DaaS sendet eine Nachricht an den VDA zur Vorbereitung auf eine eingehende Sitzung.
6. Citrix Workspace sendet eine ICA-Datei an den Endpunkt, der ein von Citrix Cloud generiertes STA-Ticket enthält.
7. Der Endpunkt stellt eine Verbindung mit Citrix Gateway Service her und stellt das Ticket zur Verbindung mit dem VDA bereit. Citrix Cloud validiert das Ticket.
8. Citrix Gateway Service sendet Verbindungsinformationen an den Cloud Connector. Der Cloud Connector bestimmt, ob die Verbindung eine Rendezvous-Verbindung ist, und sendet die Informationen an den VDA.
9. Der VDA stellt eine direkte Verbindung zu Citrix Gateway Service her.
10. Wenn eine direkte Verbindung zwischen VDA und Citrix Gateway Service nicht möglich ist, erstellt der VDA eine Proxyverbindung über den Cloud Connector.
11. Citrix Gateway Service stellt eine Verbindung zwischen Endpunktgerät und VDA her.
12. Der VDA überprüft seine Lizenz mit Citrix DaaS über den Cloud Connector.
13. Citrix DaaS sendet Sitzungsrichtlinien über den Cloud Connector an den VDA. Diese Richtlinien werden angewendet.

Rendezvous V2

October 24, 2022

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerebene herzustellen.

Es sind zwei Arten von Datenverkehr zu berücksichtigen: 1) Steuerungsdatenverkehr für die VDA-Registrierung und die Sitzungsvermittlung; 2) HDX-Sitzungsdatenverkehr.

Rendezvous V1 ermöglicht es, dass HDX-Sitzungsdatenverkehr Cloud Connectors umgeht. Cloud Connectors sind jedoch weiterhin erforderlich, um als Proxy für den gesamten Steuerungsdatenverkehr für die VDA-Registrierung und das Sitzungsbrokering zu fungieren.

Für reguläre mit AD-Domänen verbundene Maschinen und für nicht mit Domänen verbundene Maschinen wird Rendezvous V2 mit Einzelsitzungs- und Multisitzungs-Linux-VDAs unterstützt. Bei Maschinen, die nicht mit der Domäne verbunden sind, ermöglicht Rendezvous V2 sowohl dem HDX-Datenverkehr als auch dem Steuerungsdatenverkehr die Cloud Connectors zu umgehen.

Anforderungen

Anforderungen für die Verwendung von Rendezvous V2:

- Zugriff auf die Umgebung mit Citrix Workspace und Citrix Gateway Service.
- Steuerungsebene: Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- VDA Version 2201 oder höher.
 - Version 2204 ist die erforderliche Mindestversion für HTTP- und SOCKS5-Proxys.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix Richtlinie. Weitere Informationen finden Sie unter [Richtlinieneinstellung für Rendezvous-Protokoll](#).
- Die VDAs müssen Zugriff auf https://*.nssvc.net einschließlich aller Unterdomänen haben. Wenn Sie nicht alle Unterdomänen auf diese Weise auf die Positivliste setzen können, verwenden Sie stattdessen https://*.c.nssvc.net und https://*.g.nssvc.net. Weitere Informationen finden Sie im Abschnitt [Anforderungen an die Internetkonnektivität](#) der Citrix Cloud-Dokumentation (unter “Virtual Apps and Desktops Service”) und im Knowledge Center-Artikel [CTX270584](#).
- Die VDAs müssen eine Verbindung zu den zuvor genannten Adressen herstellen können:
 - An TCP 443 für TCP Rendezvous.
 - An UDP 443 für EDT Rendezvous.

Proxykonfiguration

Der VDA unterstützt die Verbindung über Proxys für Steuerungsverkehr und HDX-Sitzungsverkehr bei Verwendung von Rendezvous. Die Anforderungen und Richtlinien für beide Arten von Datenverkehr sind unterschiedlich. Überprüfen Sie sie daher sorgfältig.

Richtlinien für Proxys für den Steuerungsverkehr

- Es werden nur HTTP-Proxys unterstützt.
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der Steuerungsdatenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder überprüft wird. Andernfalls schlägt die Verbindung fehl.
- Proxyauthentifizierung wird nicht unterstützt.
- Um einen Proxy zur Steuerung des Datenverkehrs zu konfigurieren, bearbeiten Sie die Registrierung wie folgt:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\  
VirtualDesktopAgent" -t "REG_SZ" -v "ProxySettings" -d "http  
://<URL or IP>:<port>" --force  
2 <!--NeedCopy-->
```

Richtlinien für Proxys für den HDX-Datenverkehr

- HTTP- und SOCKS5-Proxys werden unterstützt.
- EDT kann nur mit SOCKS5-Proxys verwendet werden.
- Um einen Proxy für den HDX-Datenverkehr zu konfigurieren, wählen Sie die Richtlinieneinstellung [Rendezvous-Proxykonfiguration](#).
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der HDX-Datenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder überprüft wird. Andernfalls schlägt die Verbindung fehl.
- HTTP-Proxys unterstützen die maschinenbasierte Authentifizierung über Aushandlungs- und Kerberos-Authentifizierungsprotokolle. Wenn Sie eine Verbindung mit dem Proxyserver herstellen, wählt das Aushandlungsauthentifizierungsschema automatisch das Kerberos-Protokoll aus. Kerberos ist das einzige Schema, das vom Linux VDA unterstützt wird.

Hinweis:

Um Kerberos zu verwenden, müssen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver erstellen und ihn mit dem Active Directory-Konto des Proxys verknüpfen. Der VDA generiert den Dienstprinzipalnamen (SPN) im Format `HTTP/<proxyURL>` beim Einrichten einer Sitzung, wobei die Proxy-URL aus der Richtlinieneinstellung **Rendezvousproxy** abgerufen wird. Wenn Sie keinen Dienstprinzipalnamen erstellen, schlägt die Authentifizierung fehl.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Bei Verwendung eines SOCKS5-Proxy müssen Sie eine Ausnahme konfigurieren, damit Datenverkehr an die in den Anforderungen angegebenen Gateway Service-Adressen die Authentifizierung umgehen kann.
- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Verwenden Sie für einen HTTP-Proxy TCP als Transportprotokoll für ICA.

Transparenter Proxy

Rendezvous-Verbindungen über transparente HTTP-Proxys werden unterstützt. Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist auf dem VDA keine zusätzliche Konfiguration erforderlich.

Konfigurieren von Rendezvous V2

Im Folgenden werden die Schritte zum Konfigurieren von Rendezvous aufgeführt:

1. Stellen Sie sicher, dass [alle Anforderungen](#) erfüllt sind.
2. Nachdem der VDA installiert wurde, führen Sie den folgenden Befehl aus, um den erforderlichen Registrierungsschlüssel festzulegen:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent" -t "REG_DWORD" -v "GctRegistration" -d "0
  x00000001" --force
2 <!--NeedCopy-->
```

3. Starten Sie die VDA-Maschine neu.
4. Erstellen Sie eine Citrix Richtlinie oder bearbeiten Sie eine vorhandene:
 - Legen Sie die Einstellung “Rendezvous-Protokoll” auf **Zugelassen** fest.
 - Stellen Sie sicher, dass die Citrix Richtlinienfilter richtig eingestellt sind. Die Richtlinie gilt für die Maschinen, für die Rendezvous aktiviert sein muss.

- Stellen Sie sicher, dass die Citrix Richtlinie die richtige Priorität hat, damit sie keine weitere außer Kraft setzt.

Rendezvous-Validierung

Um zu überprüfen, ob eine Sitzung das Rendezvous-Protokoll verwendet, führen Sie den Befehl `/opt/Citrix/VDA/bin/ctxquery -f iP` im Terminal aus.

Die angezeigten Transportprotokolle geben die Art der Verbindung an:

- TCP-Rendezvous: TCP - TLS - CGP - ICA
- EDT-Rendezvous: UDP - DTLS - CGP - ICA
- Proxy über Cloud Connector: TCP - PROXY - SSL - CGP - ICA oder UDP - PROXY - DTLS - CGP - ICA

Wenn Rendezvous V2 verwendet wird, wird für die Protokollversion 2.0 angezeigt.

Tipp:

Wenn der VDA bei aktiviertem Rendezvous den Citrix Gateway Service nicht direkt erreichen kann, greift der VDA auf eine Proxyumleitung der HDX-Sitzung über den Cloud Connector zurück.

Sichere Benutzersitzungen mit DTLS

October 5, 2022

Die DTLS-Verschlüsselung ist ab Release 7.18 ein vollständig unterstütztes Feature. Dieses Feature ist standardmäßig im Linux VDA aktiviert. Weitere Informationen finden Sie unter [TLS \(Transport Layer Security\)](#).

Aktivieren der DTLS-Verschlüsselung

Überprüfen der Aktivierung des adaptiven Transports

Vergewissern Sie sich in Citrix Studio, dass die Richtlinie **Adaptiver HDX-Transport** auf den Modus **Bevorzugt** oder **Diagnose** festgelegt ist.

Aktivieren der SSL-Verschlüsselung auf dem Linux VDA

Verwenden Sie auf dem Linux VDA das Tool **enable_vdassl.sh** im Verzeichnis `/opt/Citrix/VDA/sbin`, um die SSL-Verschlüsselung zu aktivieren oder zu deaktivieren. Informationen zu den Optionen

des Tools können Sie über den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh -h` aufrufen.

Hinweis:

Derzeit unterstützt der Linux VDA sowohl DTLS 1.0 als auch DTLS 1.2. Für DTLS 1.2 ist Citrix Receiver für Windows 4.12 oder Citrix Workspace-App 1808 für Windows oder höher erforderlich. Wenn Ihr Client nur DTLS 1.0 unterstützt (z. B. Citrix Receiver für Windows 4.11), setzen Sie mit dem **Tool enable_vdassl.sh** die Werte **SSLMinVersion** auf **TLS_1.0** und **SSLCipherSuite** auf **COM** oder **ALL**.

Sichere Benutzersitzungen mit TLS

October 5, 2022

Ab Version 7.16 unterstützt der Linux VDA die TLS-Verschlüsselung für sichere Benutzersitzungen. Die TLS-Verschlüsselung ist standardmäßig deaktiviert.

TLS-Verschlüsselung aktivieren

Zum Aktivieren der TLS-Verschlüsselung für sichere Benutzersitzungen installieren Sie Zertifikate und aktivieren Sie die TLS-Verschlüsselung auf Linux VDA und auf dem Delivery Controller (dem Controller).

Installieren von Zertifikaten auf dem Linux VDA

Beschaffen Sie Serverzertifikate im PEM-Format und Stammzertifikate im CRT-Format. Serverzertifikate enthalten die folgenden Abschnitte:

- Zertifikat
- Nicht verschlüsselter privater Schlüssel
- Zwischenzertifikate (optional)

Ein Beispiel eines Serverzertifikats:

```
-----BEGIN CERTIFICATE-----

MIIDTCCArAgAwIBAgIJALtuncp1qGXCMAGCSqGSIb3DQEBBQUAMGcxCA3BgNV
BAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEU
MBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owYXoCZAJBgNVBAYTA1VL
MRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEUMBIGA1UE
CHMLQ210cm14IFRlc3QxGzAZBgNVBAStE1N1cnZ1c18DZXJ0aWZpY2FOZTEgMB4G
A1UEAXMYZ2EwMDEtc2MwMDEuY210cm10ZS5uZXQwZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALCTD0xc1vbIOL0F66xg05gkNeIGKVP+37p5KV8B661wCVzr6p9
t72Fa+9oCcF2x/ue274NXFcq4fqGRDsrEwL3yxM6CoYBf7L6psrSCDNnBP1q8TJH
4xoPIXUeaw4MvK/3PvyfHhKs4fz8yy1I4VdnXVhHw+OfQ2Bq3NhwsRhnAgMBAAGj
gdwmgdkwCQYDVROTBAlwADADBgnVHMQ4EFgQUrLi4zYot+CUXSh9xHfp1M+/O8yOw
gZkGAlUdIwSBkTCBjOAU85kN1EP30cVhcoss1s1seDQwGSKha6RpMGcxCZAJBgNV
BAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEU
MBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnhMDAxLmNpdHJpdGUubmV0
ggkAY8nC8dc832EwEQYJYIZIAWb4QgeBBAQDAgVgMAOGCSqGSIb3DQEBBQUAA4GB
AD5ax8YHwIXjCJ2Nt2zdXnbp200yUTowE16wqe/9cGaP6CpjoXJ7F3a2/8IpaT68
Ve18u1SEY1GKGCw93pc7SPKqb8pGBRIS/dygb+geFkiQ7Kyvbu0Ijotr3pkx4e
b6CF3tNLudHUwF610rB72zbyz3PiIx+HEnt1jOj8z4K

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIICXgIBAAKBgqCnk0ncXIr2yNc98eusyYUjDXi811T/t+6U11fAeupvg1c6+q
fBe9HwvvaAnH9s7ntu+DVXXIOH6hk7KxMNd2MTGjsgX+y+qbK7AgzWt9avEy
R+MaDyF1Hm1uDFZP9Z1cn4RyROH8/MstSOFO511R4cPtEUNgatZyCLyZnIDAQAB
AoGBAKwBgZu/bk18edgB8YPYU7d1i8X89IOs4b/apJM+3dmjxb8N96RsPQ24p9Ea
FTUC9+1L8mEroLubSicCXjsjFc+cxg9VvaNa6EEkkBj75oCUERqSx0Yb/1Adck/
FXzu0tqytUe/KHgcSgjtjrSeqlJqMm+yxzBAaTVRTTzGdwAhAKEA311KRZjINSuz
Enmi2RTI3ngBhEP/S3GEbvjFkSd5n2R190+ooEPxc1vvp5ne8Q0zupshbjFEpbOC
ykZ6UassFw3BAMTI5yPnV9ewPzJoanJZiZCMtNXDch51xx1j1yzv+Qmr8RuQz9Pv
fIenmTrfZ+wo4DaKg+8ar20vOnKF0HFAMDECOQDEwR1H6cE3wyCfNu942M9Xkhr
GvSpr7+b///vL6Nwv3CwPV9n8DTPL+wuDKJ29nCVRte1T9M1aMTYjs3a1NvAKEA
qy5JzZcBnryZMbV032jjU7ZPISnhTG01xdjzMSLLPtGpNLN34b0k3sTc1r8L42E
uQjttQrm+wdsrVF31FazkQJANudmsUVv3gZkhWGaV2hzIdXIfhYOIVv+31eZhQY6
h5EmxSZS50TyvNGt2e6m2ZgaZmjTagH59TCBHV85nof2g==

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIDTCCAokAgAwIBAgIJAMVjwvHXAd9HMAOGCSqGSIb3DQEBBQUAMGcxCA3BgNV
BAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNVBACTUNhbwJvdXJzUTEU
MBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNDEwNTk1M1oXDTI4MDkyNTEwNDEwNDEwZzELMAkGA1UEBHMVusx
EjAQBgNVBAgTCUNhbwJyaWRnZTESMBAGA1UEBxMjQ2FtyM91cm51MRQwEgYDVQQK
EwtdaXRYaXgvgVzdDEaMBGA1UEAxMRyY2EwMDEuY210cm10ZS5uZXQwZ8wDQYJK
oZIhvcNAQEBBQADgY0AMIGJAoGBAKVzmF7Uj7u0nvo3Qwdf1Onr3qkNH2DxpHwZ
Zh8cI9Vv+UFRU1C6o87izLTBMFn3FOUP712cfkHN3ZG17pB8pdyjket1Ms1VeJw
acoqrYvD+fNNSvjJuntBaCywvtaLjmfSfHHeZJXVScKrpEhkn0nkMS16tcrya/K/
oss1Zv3AgMBAAGjcwGckwDAYDVROTBAlwAwEB/zAdBgNVHQ4EFgQU85kN1EP3
0cVhcoss1s1seDQwGSIwqZkGAlUdIwSBkTCBjOAU85kN1EP30cVhcoss1s1seDQw
GSKha6RpMGcxCZAJBgNVBAYTA1VLMRkwEAYDVQIEwTDYwL1cm1kZ2UxEjAQBgNV
BACTUNhbwJvdXJzUTEUMBIGA1UECHMLQ210cm14IFRlc3QxGjAYBgNVBAMTEWnh
MDAxLmNpdHJpdGUubmV0ggkAY8nC8dc832EwEQYJKoZIhvcNAQEFBQADgYEAI24Z
gXLXf12RNqh/awtsb44Ug8B8ZKasg5ZhnA1TiXbzz8C13ec53Fb6nigMwc5T1i
UNCLXmXRU1D400tESLX9ACUNH3194yxOgujKS0S8ni21jj2TVfB832Rmr5DBY3g
UmKORn/hdqM1cope5wO6as6+HN4wU0i+hETUMME=

-----END CERTIFICATE-----
```

TLS-Verschlüsselung aktivieren

Aktivieren der TLS-Verschlüsselung auf dem Linux VDA Verwenden Sie auf dem Linux VDA das Skript `enable_vdassl.sh` im Verzeichnis `/opt/Citrix/VDA/sbin`, um die TLS-Verschlüsselung zu aktivieren (oder zu deaktivieren). Informationen zu den Optionen des Skripts können Sie über den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help` aufrufen.

```
root@xul804:~# /opt/Citrix/VDA/sbin/enable_vdassl.sh
===Enable/Disable SSL on Linux VDA===
To enable SSL, a certificate file must be specified, otherwise the local certificate file under
/etc/xdl/.sslkeystore/ is used. If the local certificate file does not exist, the command
fails. You can specify the SSL port number, version and cipher suite, otherwise, their default
values are used!

Usage: enable_vdassl.sh -Disable
       Disable Linux VDA SSL.

Usage: enable_vdassl.sh -Enable [-Certificate <CERT-FILE>] [-SSLPort <SSL-PORT-NUMBER>]
       [-SSLMinVersion <SSL-MIN-VERSION>] [-SSLCipherSuite <SSL-CIPHER-SUITE>]
       Enable Linux VDA SSL.

Options:
  -Certificate <CERT-FILE>
    Specify a certificate file, where <CERT-FILE> must include the full file path. Only one format
    is currently supported, that is PEM.

  -RootCertificate <ROOT-CERT-FILE>
    Specify a root certificate file, where <ROOT-CERT-FILE> must include the full file path. The root certificate will be put in the local keystore(under /etc/xdl/.sslkeystore/cacerts).

  -SSLPort <SSL-PORT-NUMBER>
    Specify an SSL port number. Unless otherwise specified, the default port 443 used.

  -SSLMinVersion <TLS_1.0|TLS_1.1|TLS_1.2|TLS_1.3>
    Specify SSL version. Unless otherwise specified, the default value TLS_1.2 is used.

  -SSLCipherSuite <GOV|COM|ALL>
    Specify an SSL Cipher suite. Unless otherwise specified, the default value GOV is used.

Examples:
enable_vdassl.sh -Enable -Certificate "/home/cert001.pem"
Enable Linux VDA SSL using Certificate cert001.pem.

enable_vdassl.sh -Enable -RootCertificate "/home/rootCR.cer"
Enable Linux VDA SSL using Root Certificate rootCR.cer with local certificate(under /etc/xdl/.sslkeystore).

enable_vdassl.sh -Enable -SSLPort 445
Enable Linux VDA SSL on port 445 using local certificate(under /etc/xdl/.sslkeystore).

enable_vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445
Enable Linux VDA SSL using Certificate cert001.pem on port 445, with default SSLMinVersion and SSLCipherSuite.

enable_vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2"
Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and default SSLCipherSuite..

enable_vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2" -SSLCipherSuite "GOV"
Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and SSLCipherSuite GOV.
```

Tipp: Auf jedem Linux VDA-Server muss ein Serverzertifikat installiert sein und auf jedem Linux VDA-Server und -Client müssen Stammzertifikate installiert sein.

Enable TLS encryption on the Controller

Hinweis:

Sie können die TLS-Verschlüsselung nur für ganze Bereitstellungsgruppen aktivieren. Für einzelne Anwendungen können Sie die TLS-Verschlüsselung nicht aktivieren.

Führen Sie in einem PowerShell-Fenster auf dem Controller die folgenden Befehle nacheinander aus, um die TLS-Verschlüsselung für die gewünschte Bereitstellungsgruppe zu aktivieren.

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true`

Hinweis:

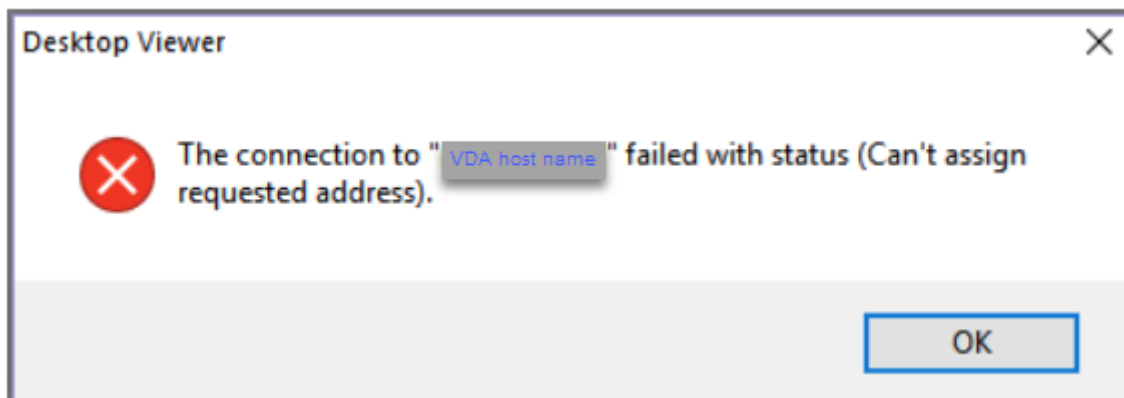
Um sicherzustellen, dass nur VDA-FQDNs in einer ICA-Sitzungsdatei enthalten sind, können Sie auch den Befehl `Set-BrokerSite -DnsResolutionEnabled $true` ausführen. Der Befehl aktiviert die DNS-Auflösung. Wenn Sie die DNS-Auflösung deaktivieren, legt eine ICA-Sitzungsdatei VDA-IP-Adressen offen und stellt FQDNs nur für TLS-bezogene Elemente wie `SSLProxyHost` und `UDPDTLSPort` bereit.

Zum Deaktivieren der TLS-Verschlüsselung auf dem Controller führen Sie die folgenden Befehle nacheinander aus:

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule -DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule -HdxSslEnabled $false`
3. `Set-BrokerSite -DnsResolutionEnabled $false`

Problembehandlung

Der folgende Fehler “Angeforderte Adresse kann nicht zugewiesen werden” kann in Citrix Workspace-App für Windows auftreten, wenn Sie versuchen, auf eine veröffentlichte Desktopsitzung zuzugreifen:



Fügen Sie als Workaround der Datei **hosts** einen Eintrag hinzu, der folgendem Beispiel folgt:

```
<IP address of the Linux VDA>      <FQDN of the Linux VDA>
```

Auf Windows-Computern ist die **Hosts**-Datei normalerweise unter `C:\Windows\System32\drivers\etc\hosts`.

Sitzungszuverlässigkeit

October 5, 2022

Citrix führt die Sitzungszuverlässigkeit für alle unterstützten Linux-Plattformen ein. Die Sitzungszuverlässigkeit ist standardmäßig aktiviert.

Die Sitzungszuverlässigkeit gewährleistet eine nahtlose Wiederverbindung von ICA-Sitzungen bei Netzwerkunterbrechungen. Weitere Informationen zur Sitzungszuverlässigkeit finden Sie unter [Automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit](#).

Hinweis: Daten, die über eine Verbindung zur Sitzungszuverlässigkeit übertragen werden, sind standardmäßig im Nur-Text-Format. Aus Sicherheitsgründen empfehlen wir, die TLS-Verschlüsselung zu aktivieren. Weitere Informationen zur TLS-Verschlüsselung finden Sie unter [Schützen von Benutzersitzungen mit TLS](#).

Konfiguration

Richtlinieneinstellungen in Citrix Studio

Sie können die folgenden Richtlinien für die Sitzungszuverlässigkeit in Citrix Studio festlegen:

- Sitzungszuverlässigkeit - Verbindungen
- Sitzungszuverlässigkeit - Timeout
- Sitzungszuverlässigkeit –Portnummer
- UI-Transparenzstufe während Wiederverbindung

Weitere Informationen finden Sie unter [Richtlinieneinstellungen für die Sitzungszuverlässigkeit](#) und [Richtlinieneinstellungen für die automatische Wiederverbindung von Clients](#).

Hinweis: Nach dem Festlegen des Parameters **Sitzungszuverlässigkeit - Verbindungen** oder **Sitzungszuverlässigkeit - Portnummer** starten Sie erst den VDA-Service und anschließend den HDX-Service neu, damit die Einstellungen wirksam werden.

Einstellungen auf dem Linux VDA

- **Aktivieren oder Deaktivieren des TCP-Listeners der Sitzungszuverlässigkeit**

Standardmäßig ist der TCP-Listener der Sitzungszuverlässigkeit aktiviert und überwacht Port 2598. Führen Sie folgenden Befehl aus, um den Listener zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\WinStations\cgp" -v "
   fEnableWinStation" -d "0x00000000"
2 <!--NeedCopy-->
```

Hinweis: Starten Sie den HDX-Service neu, damit die Einstellungen wirksam werden. Durch das Deaktivieren des TCP-Listeners wird die Sitzungszuverlässigkeit selbst nicht deaktiviert. Die Sitzungszuverlässigkeit ist weiterhin über andere Listener (z. B. SSL) verfügbar, wenn das Feature über die Richtlinie **Sitzungszuverlässigkeit - Verbindungen** aktiviert ist.

- **Sitzungszuverlässigkeit –Portnummer**

Sie können die Portnummer für die Sitzungszuverlässigkeit auch mit dem folgenden Befehl festlegen (als Beispiel dient Portnummer 2599):

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Citrix\WinStations\cgp" -v "PortNumber"
   -d "2599"
2 <!--NeedCopy-->
```

Hinweis: Starten Sie den HDX-Service neu, damit die Einstellung wirksam wird. Wenn die Portnummer über die Richtlinieneinstellung in **Citrix Studio** festgelegt wurde, wird die Einstellung auf dem Linux VDA ignoriert. Stellen Sie sicher, dass die Firewall auf dem VDA so konfiguriert ist, dass Netzwerkverkehr über den festgelegten Port nicht verhindert wird.

- **Server-zu-Client-Keep-Alive-Intervall**

Keep-Alive-Meldungen werden zwischen dem Linux VDA und dem Client übertragen, wenn in einer Sitzung keine Aktivität stattfindet (keine Mausbewegung, keine Bildschirmaktualisierung o. Ä.). Die Keep-Alive-Meldungen testen, ob der Client noch antworten kann. Wenn der Client nicht antwortet, wird die Sitzung angehalten, bis der Client die Verbindung wieder herstellt. Mit dieser Einstellung geben Sie die Anzahl der Sekunden zwischen aufeinanderfolgenden Keep-Alive-Meldungen an. Standardmäßig ist diese Einstellung nicht konfiguriert. Führen Sie zum Konfigurieren folgenden Befehl aus (Beispielintervall = 10 Sekunden):

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\XTEConfig" -t "REG_DWORD" -v "CgpServerToClientKeepAlive"
   -d "10" --force
```

- **Client-zu-Server-Keep-Alive-Intervall**

Mit dieser Einstellung geben Sie die Anzahl der Sekunden zwischen aufeinanderfolgenden ICA-Keep-Alive-Meldungen an, die vom ICA-Client an den Linux VDA gesendet werden. Standardmäßig ist diese Einstellung nicht konfiguriert. Führen Sie zum Konfigurieren folgenden Befehl aus (Beispielintervall = 10 Sekunden):

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\  
Citrix\XTEConfig" -t "REG_DWORD" -v "CgpClientToServerKeepAlive"  
-d "10" --force  
2 <!--NeedCopy-->
```

Problembehandlung

Nach dem Aktivieren der Sitzungszuverlässigkeit über die RichtlinienEinstellung können Sitzungen nicht gestartet werden.

Sie umgehen das Problem wie folgt:

1. Stellen Sie sicher, dass Sie nach dem Aktivieren der Sitzungszuverlässigkeit über die Richtlinieneinstellung in Citrix Studio zunächst den VDA-Service und dann den HDX-Service neu starten.
2. Prüfen Sie auf dem VDA mit folgendem Befehl, ob der TCP-Listener der Sitzungszuverlässigkeit ausgeführt wird (Beispielport = 2598):

```
1 netstat -an | grep 2598  
2 <!--NeedCopy-->
```

Wenn am Port für die Sitzungszuverlässigkeit kein TCP-Listener vorhanden ist, aktivieren Sie den Listener mit dem folgenden Befehl:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\  
CurrentControlSet\Control\Citrix\WinStations\cgp" -v "  
fEnableWinStation" -d "0x00000001"  
2 <!--NeedCopy-->
```

USB-Umleitung

October 24, 2022

USB-Geräte werden von der Citrix Workspace-App und Linux VDA-Desktop gemeinsam verwendet. Wenn ein USB-Gerät an einen Desktop umgeleitet wird, können Sie es wie ein lokal verbundenes Gerät verwenden.

Tipp:

Bei einer Netzwerklatenz unter 100 Millisekunden empfehlen wir die Verwendung einer USB-Umleitung. Verwenden Sie keine USB-Umleitung, wenn die Netzwerklatenz höher als 200 Millisekunden ist.

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 der Citrix Workspace-App 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 dient als 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.

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 flash drive	0781:5580	FAT32
WD HDD	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. Der Gerätetyp kann außerdem 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

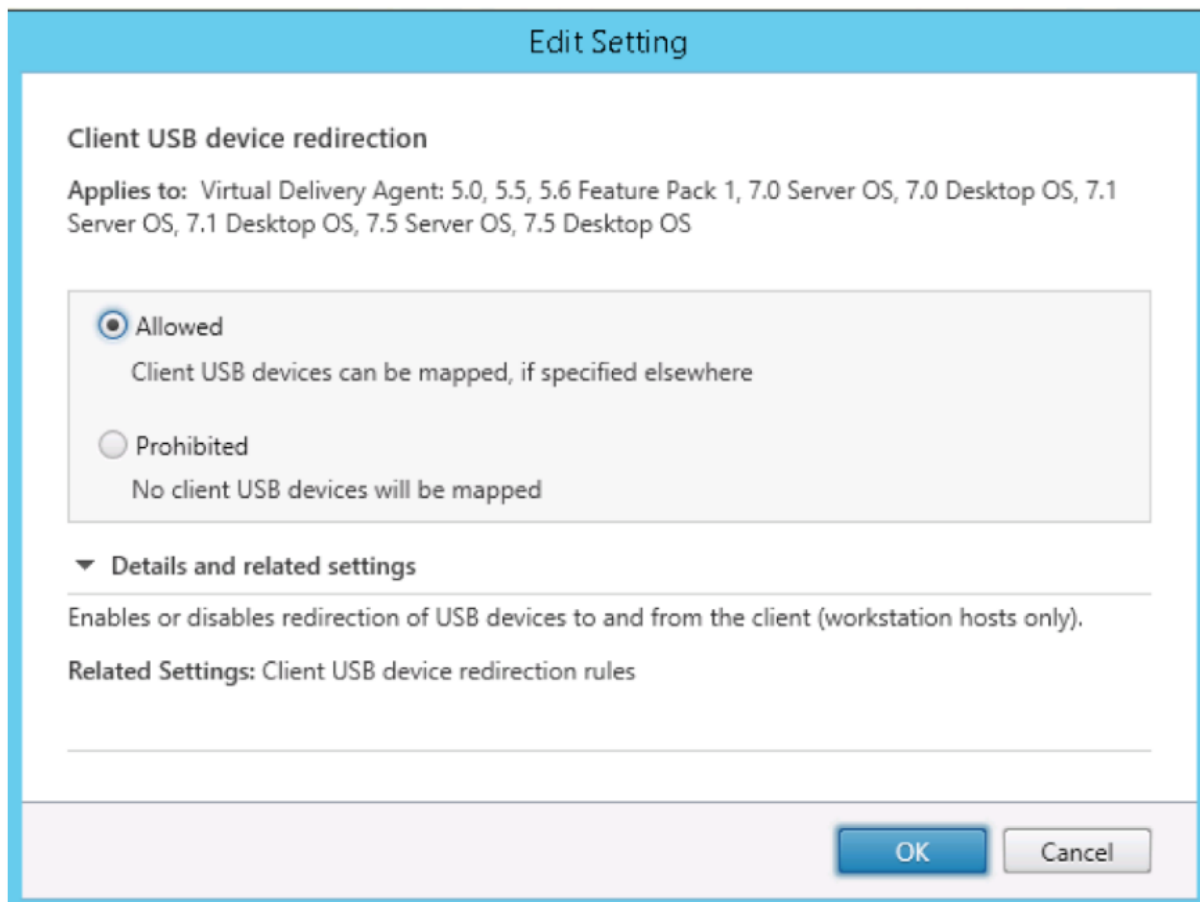
USB-Umleitung aktivieren

In Citrix Studio können Sie die Umleitung von USB-Geräten zum und vom Client (nur Arbeitsstation-shosts) aktivieren und deaktivieren.

Führen Sie im Dialogfeld **Einstellung bearbeiten** folgende Schritte aus:

1. Wählen Sie **Zugelassen**.

2. Klicken Sie auf **OK**.



Edit Setting

Client USB device redirection

Applies to: Virtual Delivery Agent: 5.0, 5.5, 5.6 Feature Pack 1, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Server OS, 7.5 Desktop OS

☒ **Allowed**
Client USB devices can be mapped, if specified elsewhere

☐ **Prohibited**
No client USB devices will be mapped

▼ **Details and related settings**

Enables or disables redirection of USB devices to and from the client (workstation hosts only).

Related Settings: Client USB device redirection rules

OK **Cancel**

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**.

Edit Setting

Client USB device redirection rules

Applies to: Virtual Delivery Agent: 5.0, 5.5, 5.6 Feature Pack 1, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Server OS, 7.5 Desktop OS

Values:

Allow: #all ok

New

Edit

Delete

Move Up

Move Down

☐ Use default value:

Details and related settings

Lists redirection rules for USB devices.

Weitere Informationen zum Konfigurieren der generischen USB-Umleitung finden Sie im [Citrix Generic USB Redirection Configuration Guide](#).

Erstellen des VHCI-Kernelmoduls

Die USB-Umleitung ist abhängig von den VHCI-Kernelmodulen (`usb-vhci-hcd.ko` und `usb-vhci-icof.ko`). 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
Amazon Linux 2	4.14.268-205
Debian 11.3	5.10.0-10
Debian 10.9	4.19.0-19
RHEL 8.x	4.18.0-240
RHEL 7.9, CentOS 7.9	3.10.0-1160

Unterstützte Linux-Distribution	Kernelversion
SUSE 15	5.3.18
Ubuntu 20.04	5.4.0-81
Ubuntu 18.04	4.15.0-154

Wichtig:

Wenn der Kernel Ihrer Maschine nicht mit dem 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:

```
1 insmod /opt/Citrix/VDA/lib64/usb-vhci-hcd.ko
2 <!--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 Downloadsite](#) herunter. Wählen Sie die Datei im Abschnitt “**Linux Virtual Delivery Agent (sources)**” aus.
2. Extrahieren Sie die Datei **citrix-linux-vda-sources.zip**. Gehen Sie zu **linux-vda-sources/vhci-hcd-1.15.zip** und extrahieren Sie die VHCI-Quelldateien mit dem Befehl `unzip vhci-hcd-1.15.zip`.
3. Stellen Sie sicher, dass Sie das Linux VDA-Paket installiert haben, und führen Sie dann einen der folgenden Befehle aus:
 - `sudo bash ctxusbcfg.sh dkms`

Über diesen Befehl können Sie das DKMS-Programm (Dynamic Kernel Module Support) verwenden, um Ihre VHCI-Kernelmodule zu verwalten. DKMS ist für SUSE nicht verfügbar.

Hinweis:

Der Befehl `sudo bash ctxusbcfg.sh dkms` installiert die Programme `kernel-devel` und `DKMS` auf dem VDA. Unter RHEL und CentOS installiert und aktiviert der Befehl das Repository “Extra Packages for Enterprise Linux (EPEL)” auf dem VDA.

DKMS kann die VHCI-Kernelmodule (`usb-vhci-hcd.ko` und `usb-vhci-iocif.ko`) möglicherweise nicht erstellen, wenn Sie ein größeres Kernel-Upgrade durchführen, z. B. von Version 4.x.y auf Version 5.x.y. Wenn DKMS fehlschlägt, führen Sie `sudo bash ctxusbcfg.sh dkms` erneut aus.

- `sudo bash ctxusbcfg.sh build`

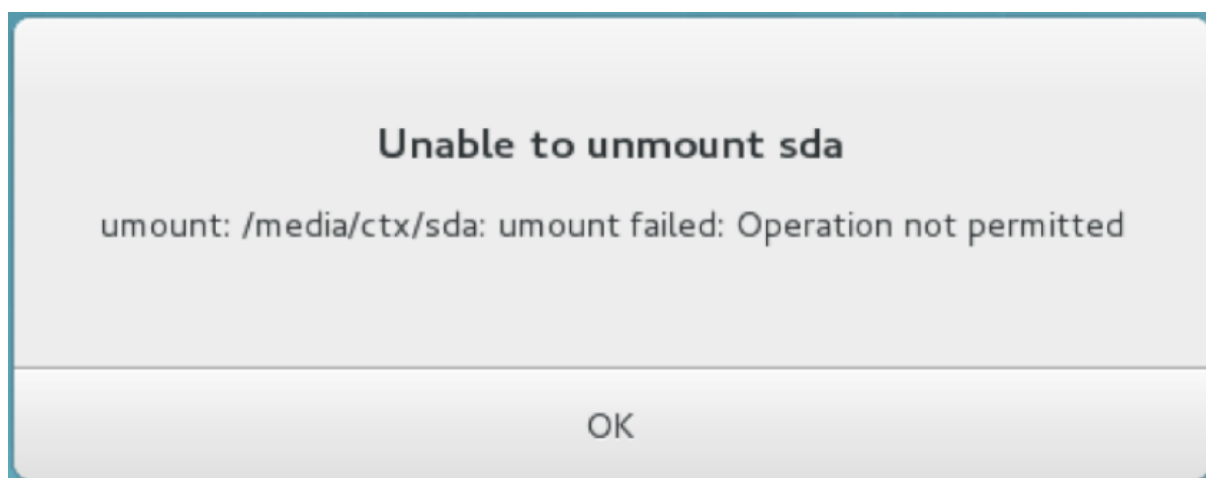
Der Befehl erstellt und installiert die VHCI-Kernelmodule ohne DKMS-Option.

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.

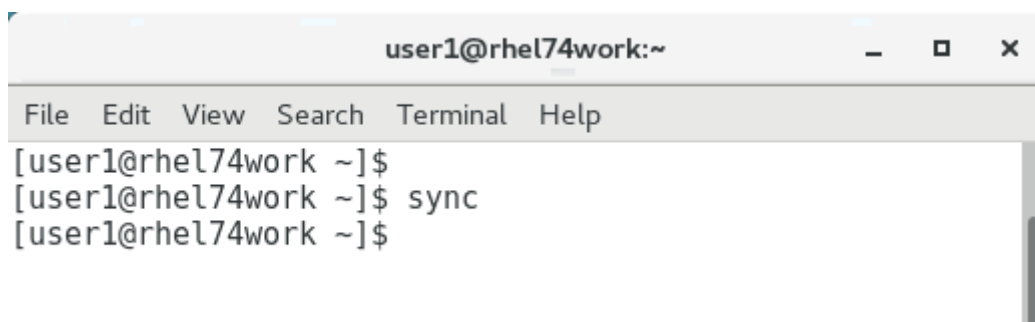
Bereitstellung eines umgeleiteten USB-Datenträgers kann nicht aufgehoben werden

Der Linux VDA verwaltet alle von der Citrix Workspace-App umgeleiteten USB-Datenträger unter Verwendung von Administratorrechten, damit nur der Besitzer eines umgeleiteten Geräts darauf zugreifen kann. Daher können Sie die Bereitstellung des Geräts nur mit Administratorrechten aufheben.



Bei Beenden der Umleitung eines USB-Datenträgers geht eine Datei verloren

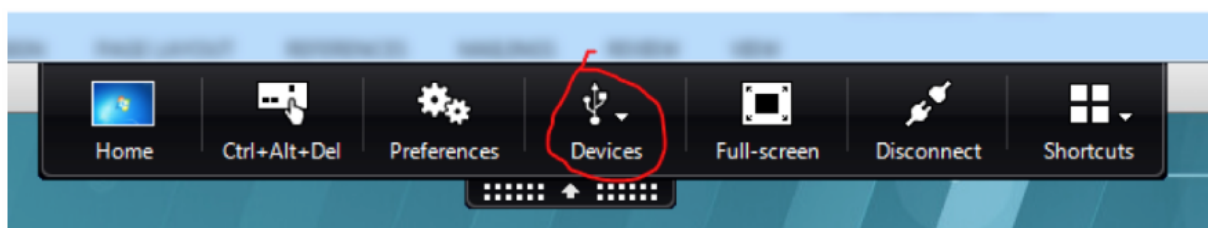
Wenn Sie die Umleitung eines USB-Datenträgers sofort über die Symbolleiste der Citrix Workspace-App beenden, können die Dateien, die Sie auf dem Datenträger geändert oder erstellt haben, verloren gehen. Dieses Problem tritt auf, weil beim Schreiben von Daten in ein Dateisystem der Speichercache im Dateisystem eingebunden wird. Die Daten werden nicht auf den Datenträger selbst geschrieben. Wenn Sie die Umleitung über die Symbolleiste der Citrix Workspace-App 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 der Citrix Workspace-App

Es kann vorkommen, dass in der Symbolleiste der Citrix Workspace-App 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 der Citrix Workspace-App für Linux nicht verfügbar.

Die Umleitung schlägt fehl, wenn in der Symbolleiste der Citrix Workspace-App angezeigte USB-Geräte als *richtlinienbeschränkt* ausgewiesen sind

Wenn das Problem auftritt, führen Sie die folgenden Schritte aus:

- Konfigurieren Sie die Linux VDA-Richtlinie zum Aktivieren der Umleitung.
- Prüfen Sie, ob in der Registrierung der Citrix Workspace-App weitere Richtlinieneinschränkungen konfiguriert sind. Prüfen Sie **DeviceRules** im Registrierungspfad, um sicherzustellen, dass dem Gerät durch diese Einstellung kein Zugriff verweigert wird:

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

Weitere Informationen finden Sie im Knowledge

Center-Artikel [How to Configure Automatic Redirection of USB Devices](#).

Ein USB-Gerät wird umgeleitet, kann jedoch nicht in einer Sitzung verwendet werden

In der Regel können nur [unterstützte USB-Geräte](#) umgeleitet werden. Auch andere Geräte werden evtl. in eine aktive Linux VDA-Sitzung umgeleitet. Es wird 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:

Für USB-Laufwerke 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.

Virtual Channel SDK (experimentell)

October 5, 2022

Mit dem Virtual Channel SDK für den Linux VDA können Sie serverseitige Anwendungen schreiben, die auf dem VDA ausgeführt werden. Weitere Informationen finden Sie in der [Dokumentation zum Citrix Virtual Channel SDK für Linux VDAs](#).

Das Citrix Virtual Channel SDK für Linux VDAs ist auf der [Citrix Virtual Apps and Desktops-Downloadseite](#) zum Download verfügbar. Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um den Linux VDA-Download auszuwählen.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).