Was ist neu

Neuerungen in Version 2107

Version 2107 des Linux VDA enthält die folgenden neuen Features und Verbesserungen:

Centrify-Unterstützung für mit MCS erstellte RHEL 7/CentOS 7- und RHEL 8/CentOS 8-Maschinen

Wir haben die Centrify-Unterstützung für das Beitreten von mit MCS erstellten RHEL 7/CentOS 7- und RHEL 8/CentOS 8-Maschinen zu Windows-Domänen hinzugefügt. Weitere Informationen finden Sie unter Verwenden von Machine Creation Services (MCS) zum Erstellen von Linux-VMs.

Vereinfachter Neuaufbau des Kernelmoduls für die USB-Umleitung

Wir stellen jetzt `ctxusbcfg.sh` in der Linux VDA-Quelldatei citrix-linux-vda-sources.zip bereit. Das Skript vereinfacht das Erstellen der VHCI-Kernelmodule (`usb-vhci-hcd.ko` und `usb-vhci-iocif.ko`) mit und ohne die Option Dynamic Kernel Module Support (DKMS). DKMS hilft, die VHCI-Kernelmodule automatisch neu zu erstellen, wenn ein Kernel aktualisiert wird. Weitere Informationen finden Sie unter Konfigurieren der USB-Umleitung.

Unterstützung für RHEL 8.4 und CentOS 8 (2105)

Wir haben RHEL 8.4 und CentOS 8 (2105) als unterstützte Distributionen hinzugefügt. Weitere Informationen finden Sie unter Systemanforderungen.

Smartcard-Unterstützung für Debian

Sie können eine mit dem Clientgerät verbundene Smartcard zur Authentifizierung verwenden, wenn Sie sich bei einer virtuellen Linux-Desktopsitzung anmelden. Diese Version ermöglicht Ihnen außerdem die Verwendung von Smartcards in Debian 10.7-Sitzungen. Weitere Informationen finden Sie unter Smartcard-Unterstützung.

Behobene Probleme

Die folgenden Probleme wurden seit Linux Virtual Delivery Agent 2106 behoben:

- Der in Amazon Web Services (AWS) gehostete Linux VDA kann sich möglicherweise nicht bei Citrix Cloud registrieren. Das Problem tritt auf, wenn Sie CTX_XDL_VDA_PORT auf einen anderen Port als 80 einstellen.

Bekannte Probleme

Die folgenden Probleme wurden in dieser Version identifiziert:

- Nicht-nahtlose veröffentlichte Anwendungen können kurz nach dem Start beendet werden. Das Problem tritt nach einem Mutter-Upgrade auf eine Version auf, die neuer als mutter-3.28.3-4 ist. Um das Problem zu umgehen, verwenden Sie mutter-3.28.3-4 oder eine frühere Version.
- Der Linux VDA funktioniert nicht wie erwartet, wenn Sie NVIDIA GRID 3D-Karten verwenden, ohne HDX 3D Pro zu aktivieren. Das Problem tritt unter RHEL 7.7 und früher, SUSE 12.5 und früher sowie Ubuntu 16.04 auf. Der Grund ist, dass mehrere OpenGL-Bibliotheken in den Grafiksystemen dieser Linux-Distributionen nicht koexistieren können.
- Während des Dateidownloads wird ein unerwartetes Fenster angezeigt. Das Fenster beeinträchtigt die Dateidownload-Funktionalität nicht und verschwindet nach einer Weile automatisch.
- Die Standardeinstellungen von PulseAudio bewirken, dass das Soundserver-Programm nach 20 Sekunden Inaktivität beendet wird. Wenn PulseAudio beendet wird, funktioniert der Ton nicht. Um dieses Problem zu umgehen, setzen Sie exit-idle-time=-1 in der Datei /etc/pulse/daemon.conf.
- `libtcmalloc 4.3.0` in SUSE 12.5 kann dazu führen, dass Prozesse unerwartet beendet werden.
- Der Dienst `ctxhdx` kann auf den Ubuntu 16.04- und SUSE 12.5-VDAs unerwartet beendet werden. Das Problem tritt bei den GNU C Library (`glibc`) Versionen 2.22 bis 2.24 auf. Das Problem ist in `glibc 2.25` behoben. Wenn Sie die SUSE 12.5-Distribution verwenden, können Sie den Patch installieren, den SUSE zur Behebung des Problems bereitstellt. Zum Zeitpunkt der Veröffentlichung des Linux VDA ist keine Korrektur für Ubuntu 16.04 verfügbar.
- Sitzungen können in der Citrix Workspace™-App für Linux nicht gestartet werden, wenn die SSL-Verschlüsselung aktiviert und die Sitzungszuverlässigkeit deaktiviert ist.
- Der Prozess `indicator-datetime-service` verwendet die Umgebungsvariable $TZ nicht. Wenn sich Client und Sitzung in verschiedenen Zeitzonen befinden, zeigt das Unity-Panel auf dem Ubuntu 16.04 Unity Desktop die Uhrzeit des Clients nicht an.

- Ubuntu-Grafik: In HDX™ 3D Pro kann nach dem Ändern der Größe des Desktop Viewer ein schwarzer Rahmen um Anwendungen erscheinen, oder manchmal kann der Hintergrund schwarz erscheinen.
- Drucker, die durch die Druckumleitung des Linux VDA erstellt wurden, werden möglicherweise nach dem Abmelden von einer Sitzung nicht entfernt.
- CDM-Dateien fehlen, wenn ein Verzeichnis zahlreiche Dateien und Unterverzeichnisse enthält. Dieses Problem kann auftreten, wenn die Clientseite zu viele Dateien oder Verzeichnisse hat.
- Für nicht-englische Sprachen wird nur die UTF-8-Kodierung unterstützt.
- Der CAPS LOCK-Status der Citrix Workspace-App für Android kann während des Sitzungsroamings umgekehrt werden. Der CAPS LOCK-Status kann verloren gehen, wenn eine bestehende Verbindung zur Citrix Workspace-App für Android geräumt wird. Als Problemumgehung verwenden Sie die Umschalttaste auf der erweiterten Tastatur, um zwischen Groß- und Kleinschreibung zu wechseln.
- Tastenkombinationen mit ALT funktionieren nicht immer, wenn Sie über die Citrix Workspace-App für Mac eine Verbindung zum Linux VDA herstellen. Die Citrix Workspace-App für Mac sendet standardmäßig AltGr für die linke und rechte Options-/Alt-Taste. Sie können dieses Verhalten in den Einstellungen der Citrix Workspace-App ändern, aber die Ergebnisse variieren je nach Anwendung.
- Die Registrierung schlägt fehl, wenn der Linux VDA erneut der Domäne beigetreten wird. Der erneute Beitritt generiert einen neuen Satz Kerberos-Schlüssel. Der Broker verwendet jedoch möglicherweise ein zwischengespeichertes, veraltetes VDA-Dienstticket, das auf dem vorherigen Satz von Kerberos-Schlüsseln basiert. Wenn der VDA versucht, eine Verbindung zum Broker herzustellen, kann der Broker möglicherweise keinen Rücksicherheitskontext zum VDA herstellen. Das übliche Symptom ist, dass die VDA-Registrierung fehlschlägt.

  Dieses Problem kann sich schließlich von selbst lösen, wenn das VDA-Dienstticket abläuft und erneuert wird. Da Diensttickets jedoch langlebig sind, kann dies lange dauern.

  Als Problemumgehung löschen Sie den Ticket-Cache des Brokers. Starten Sie den Broker neu oder führen Sie den folgenden Befehl auf dem Broker über eine Eingabeaufforderung als Administrator aus:

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

  Dieser Befehl löscht alle Diensttickets im LSA-Cache, die vom Prinzipal des Netzwerkdiensts gehalten werden, unter dem der Citrix Broker Service ausgeführt wird. Er entfernt Diensttickets

für andere VDAs und potenziell andere Dienste. Dies ist jedoch harmlos – diese Diensttickets können bei Bedarf erneut vom KDC abgerufen werden.

- Audio-Plug-and-Play wird nicht unterstützt. Sie können ein Audioaufnahmegerät an den Clientcomputer anschließen, bevor Sie mit der Audioaufnahme in der ICA®-Sitzung beginnen. Wenn ein Aufnahmegerät angeschlossen wird, nachdem die Audioaufzeichnungsanwendung gestartet wurde, reagiert die Anwendung möglicherweise nicht mehr und Sie müssen sie neu starten. Wenn ein Aufnahmegerät während der Aufnahme getrennt wird, kann ein ähnliches Problem auftreten.
- Die Citrix Workspace-App für Windows kann während der Audioaufnahme Audioverzerrungen aufweisen.

Hinweise von Drittanbietern

Linux Virtual Delivery Agent Version 2107 (PDF-Download)

Diese Version des Linux VDA kann Software von Drittanbietern enthalten, die unter den im Dokument definierten Bedingungen lizenziert ist.

Einstellung

Die Ankündigungen in diesem Artikel sollen Sie frühzeitig über Plattformen, Citrix®-Produkte und Funktionen informieren, die eingestellt werden, damit Sie rechtzeitig Geschäftsentscheidungen treffen können. Citrix überwacht die Kundennutzung und das Feedback, um zu bestimmen, wann diese zurückgezogen werden. Ankündigungen können sich in nachfolgenden Releases ändern und möglicherweise nicht jede veraltete Funktion oder Funktionalität umfassen. Einzelheiten zur Produktlebenszyklusunterstützung finden Sie im Artikel Produktlebenszyklus-Supportrichtlinie.

Einstellungen und Entfernungen

Die folgende Tabelle zeigt die Plattformen, Citrix-Produkte und Funktionen, die veraltet oder entfernt wurden. **Veraltete** Elemente werden nicht sofort entfernt. Citrix unterstützt sie in diesem Release weiterhin, aber sie werden in einem zukünftigen Current Release entfernt. **Entfernte** Elemente werden im Linux VDA entweder entfernt oder nicht mehr unterstützt.

FUNKTION	VERALTUNG ANGEKÜNDIGT IN	ENTFERNT IN
Unterstützung für RHEL 7.7, CentOS 7.7	2006	2009

FUNKTION	VERALTUNG ANGEKÜNDIGT IN	ENTFERNT IN
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
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

Linux-Distributionen

> **Hinweis:**
>
> Die Systemanforderungen für hier nicht behandelte Komponenten (wie z. B. Citrix Workspace™ app) werden in den jeweiligen Dokumentationssätzen beschrieben.

> Installieren Sie vor der Installation des Linux VDA die .NET Core Runtime 3.1 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

> Weitere Informationen zur Verwendung dieses Current Release (CR) in einer Long Term Service (LTSR)-Umgebung und andere häufig gestellte Fragen finden Sie im Knowledge Center-Artikel.

Der Linux VDA unterstützt die folgenden Linux-Distributionen:

> **Wichtig:**
>
> Wenn der Support Ihres Betriebssystemanbieters abläuft, ist Citrix® möglicherweise nur eingeschränkt in der Lage, Probleme zu beheben.

- SUSE Linux Enterprise:
  - Server 12 Service Pack 5 + SUSE Linux Enterprise Workstation Extension 12 SP5
  - Server 12 Service Pack 5
- Red Hat Enterprise Linux
  - Workstation 8.4

    - Workstation 8.3
    - Workstation 8.2
    - Workstation 8.1
    - Workstation 7.9
    - Workstation 7.8
    - Server 8.4
    - Server 8.3
    - Server 8.2
    - Server 8.1
    - Server 7.9
    - Server 7.8
- CentOS Linux
    - CentOS 8 (2105)
    - CentOS 8.3
    - CentOS 8.2
    - CentOS 8.1
    - CentOS 7.9
    - CentOS 7.8
- Ubuntu Linux
    - Ubuntu Desktop 20.04
    - Ubuntu Server 20.04
    - Ubuntu Desktop 18.04
    - Ubuntu Server 18.04
    - Ubuntu Live Server 18.04
    - Ubuntu Desktop 16.04
    - Ubuntu Server 16.04
- Debian Linux
    - Debian 10.7

Hinweis:

- Das CentOS-Projekt verlagert den Fokus auf CentOS Stream. CentOS Linux 8, als Neuaufbau von RHEL 8, endet Ende 2021. CentOS Stream wird nach diesem Datum fortgesetzt und dient als Upstream- (Entwicklungs-) Zweig von Red Hat Enterprise Linux. Weitere Informationen finden Sie unter `<https://www.redhat.com/en/blog/centos-stream-building-innovative-future-enterprise-linux>`.
- Wenn Sie Citrix Provisioning™ verwenden, um Linux-Zielgeräte zu streamen, erstellen Sie eine separate Boot-Partition auf dem einzelnen freigegebenen Datenträger-Image, damit die bereitgestellten Geräte wie erwartet booten können.
- Vermeiden Sie es, Partitionen mit btrfs zu formatieren. GRUB2 hat ein intrinsisches Problem beim Auffinden von btrfs-Partitionen. GRUB steht für GRand Unified Bootloader.

Der Linux VDA unterstützt mehrere Methoden zur Integration von Linux-Maschinen in Microsoft Active Directory (AD):

	WINBIND	SSSD	CENTRIFY	PBIS	QUEST
RHEL 8.4	Ja	Ja	Ja	Ja	Nein
CentOS 8 (2105)	Ja	Ja	Ja	Ja	Nein
RHEL 8.3	Ja	Ja	Ja	Ja	Nein
CentOS 8.3	Ja	Ja	Ja	Ja	Nein
RHEL 8.2	Ja	Ja	Ja	Ja	Nein
CentOS 8.2	Ja	Ja	Ja	Ja	Nein
RHEL 8.1	Ja	Ja	Ja	Ja	Nein
CentOS 8.1	Ja	Ja	Ja	Ja	Nein
RHEL 7.9	Ja	Ja	Ja	Ja	Ja
CentOS 7.9	Ja	Ja	Ja	Ja	Ja

	WINBIND	SSSD	CENTRIFY	PBIS	QUEST
RHEL 7.8	Ja	Ja	Ja	Ja	Ja
CentOS 7.8	Ja	Ja	Ja	Ja	Ja
Ubuntu 20.04	Ja	Ja	Ja	Ja	Ja
Ubuntu 18.04	Ja	Ja	Ja	Ja	Ja
Ubuntu 16.04	Ja	Ja	Ja	Ja	Ja
Debian 10.7	Ja	Ja	Ja	Ja	Nein
SUSE 12.5	Ja	Ja	Ja	Ja	Ja

Eine Matrix der Linux-Distributionen und der Xorg-Versionen, die diese Version des Linux VDA unterstützt, finden Sie in der folgenden Tabelle. Weitere Informationen finden Sie unter XorgModuleABIVersions.

LINUX-DISTRIBUTION	XORG-VERSION
RHEL 8.4, CentOS 8 (2105)	1.20.10
RHEL 8.3, CentOS 8.3	1.20.8
RHEL 8.2, CentOS 8.2	1.20.8
RHEL 8.1, CentOS 8.1	1.20.8
RHEL 7.9, CentOS 7.9	1.20
RHEL 7.8, CentOS 7.8	1.20
Ubuntu 20.04	1.20
Ubuntu 18.04	1.19
Ubuntu 16.04	1.18

LINUX-DISTRIBUTION	XORG-VERSION
Debian 10.7	1.20
SUSE 12.5	1.19

Verwenden Sie keinen HWE-Kernel oder HWE Xorg unter Ubuntu.

Verwenden Sie PulseAudio 13.99 unter RHEL 8.x und CentOS 8.x.

In allen Fällen ist die unterstützte Prozessorarchitektur x86-64.

Hinweis:

- GNOME- und KDE-Desktops werden unter SUSE 12, RHEL 7, CentOS 7, RHEL 8 und CentOS 8 unterstützt. Der Unity-Desktop wird unter Ubuntu 16.04 unterstützt. Der GNOME-Desktop wird unter Ubuntu 20.04, Ubuntu 18.04 und Debian 10.7 unterstützt. Der MATE-Desktop wird auf allen Linux-Distributionen unterstützt, die der Linux VDA unterstützt, mit Ausnahme von SUSE 12.5. Mindestens ein Desktop muss installiert sein.

Citrix Virtual Desktops™

Der Linux VDA ist mit allen derzeit unterstützten Versionen von Citrix Virtual Apps and Desktops kompatibel. Informationen zum Citrix-Produktlebenszyklus und wann Citrix die Unterstützung für bestimmte Produktversionen einstellt, finden Sie in der Citrix Product Lifecycle Matrix.

Der Konfigurationsprozess für Linux VDAs unterscheidet sich geringfügig von dem für Windows VDAs. Jede Delivery Controller™-Farm kann jedoch sowohl Windows- als auch Linux-Desktops vermitteln.

Unterstützte Hostplattformen und Virtualisierungsumgebungen

- Bare-Metal-Server
- Citrix Hypervisor™
- VMware ESX und ESXi
- Microsoft Hyper-V
- Nutanix AHV

- Microsoft Azure Resource Manager
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

Tipp:

Die Liste der unterstützten Plattformen finden Sie in der Dokumentation des Herstellers.

Hinweis:

Azure, AWS und GCP sind nur mit dem Citrix Virtual Apps and Desktops™-Dienst kompatibel. Bare-Metal-Server werden nicht unterstützt, wenn MCS zum Erstellen virtueller Maschinen verwendet wird.

Active Directory-Integrationspakete

Der Linux VDA unterstützt die folgenden Active Directory-Integrationspakete oder -Produkte:

- Samba Winbind
- Quest Authentication Services v4.1 oder höher
- Centrify DirectControl
- SSSD
- PBIS (kompatibel mit RHEL 7, Ubuntu und Debian)

Tipp:

Eine Liste der unterstützten Plattformen finden Sie in der Dokumentation der Anbieter der Active Directory-Integrationspakete.

HDX™ 3D Pro

Die folgenden Hypervisoren und NVIDIA GRID™ GPUs sind zur Unterstützung von HDX 3D Pro erforderlich.

Hypervisoren

- Citrix Hypervisor
- VMware ESX und ESXi
- Nutanix AHV

> **Hinweis:**

> Die Hypervisoren sind mit bestimmten Linux-Distributionen kompatibel.

GPU

Der Linux VDA unterstützt die folgenden GPUs für GPU-Passthrough:

- NVIDIA GRID - Tesla T4
- NVIDIA GTX750Ti
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - K2
- NVIDIA GRID - Tesla P40
- NVIDIA GRID - Tesla P4
- NVIDIA GRID - Tesla P100

Der Linux VDA unterstützt die folgenden GPUs für vGPU:

- NVIDIA GRID - Tesla T4
- NVIDIA GRID - Tesla V100
- NVIDIA GRID - Tesla M60
- NVIDIA GRID - Tesla M10
- NVIDIA GRID - Tesla P40
- NVIDIA GRID - Tesla P4
- NVIDIA GRID - Tesla P100

Installationsübersicht

Dieser Abschnitt führt Sie durch die folgenden Verfahren:

- Schnelle Installation mit Easy Install (empfohlen für Neuinstallationen)
- Manuelle Installation basierend auf verschiedenen Linux-Distributionen
- Verwenden Sie MCS, um Linux-VMs zu erstellen
- Erstellen Sie domänenverbundene und nicht domänenverbundene Linux-VDAs in Citrix Virtual Apps and Desktops™ Standard für Azure
- Verwenden Sie Citrix Provisioning™, um Linux-VMs zu erstellen
- Delivery Controller für XenDesktop 7.6 und frühere Versionen konfigurieren

Schnelle Installation mit Easy Install (Empfohlen)

Wichtig:

Für Neuinstallationen empfehlen wir Ihnen, diesen Artikel für eine schnelle Installation zu verwenden. Dieser Artikel beschreibt die Installation und Konfiguration des Linux VDA mit Easy Install. Easy Install spart Zeit und Arbeitsaufwand und ist weniger fehleranfällig als die manuelle Installation. Es hilft Ihnen, eine funktionierende Umgebung des Linux VDA einzurichten, indem die erforderlichen Pakete installiert und die Konfigurationsdateien automatisch angepasst werden.

Schritt 1: Konfigurationsinformationen und Linux-Maschine vorbereiten

Erfassen Sie die folgenden Konfigurationsinformationen, die für Easy Install benötigt werden:

- 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

- Realm-Name – Der Kerberos-Realm-Name
- FQDN der Active Domain – Vollqualifizierter Domänenname

> **Wichtig:**

> - Um den Linux VDA zu installieren, stellen Sie sicher, dass die Repositorys auf der Linux-Maschine korrekt hinzugefügt wurden.
> - Um eine Sitzung zu starten, stellen Sie sicher, dass das X Window System und die Desktop-Umgebungen installiert sind.

Überlegungen

- Der Arbeitsgruppenname ist standardmäßig der Domänenname. Um die Arbeitsgruppe in Ihrer Umgebung anzupassen, gehen Sie wie folgt vor:

  a. Erstellen Sie die Datei /tmp/ctxinstall.conf auf der Linux VDA-Maschine.

  b. Fügen Sie die Zeile workgroup=\<your workgroup\> zur Datei hinzu und speichern Sie Ihre Änderungen.

- Centrify unterstützt keine reine IPv6-DNS-Konfiguration. Mindestens ein DNS-Server mit IPv4 ist in /etc/resolv.conf erforderlich, damit `adclient` AD-Dienste ordnungsgemäß finden kann.

  Protokoll:

  ```
  ADSITE   : Check that this machine's subnet is in a site known by AD
    : Failed

           : This machine's subnet is not known by AD.

           : We guess you should be in the site Site1.
  ```

  Dieses Problem ist spezifisch für Centrify und dessen Konfiguration. Um dieses Problem zu beheben, gehen Sie wie folgt vor:

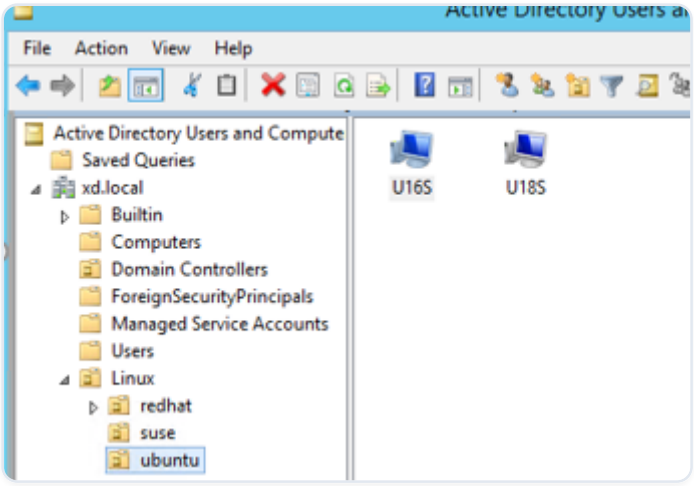
  a. Öffnen Sie die **Verwaltungstools** auf dem Domänencontroller.

  b. Wählen Sie **Active Directory-Standorte und -Dienste** aus. c. Fügen Sie eine geeignete Subnetzadresse für **Subnetze** hinzu.

- Um Ihr VDA einer bestimmten OU beizutreten, gehen Sie wie folgt vor:

  a. Stellen Sie sicher, dass die spezifische OU auf dem Domänencontroller vorhanden ist.

     Ein Beispiel für eine OU finden Sie im folgenden Screenshot



  b. Erstellen Sie die Datei /tmp/ctxinstall.conf auf dem VDA.

  c. Fügen Sie die Zeile ou=\<your ou\> zur Datei /tmp/ctxinstall.conf hinzu.

     OU-Werte variieren je nach AD-Methode. Siehe folgende Tabelle.

BETRIEBSSYSTEM	WINBIND	SSSD	CENTRIFY	PBIS
RHEL 8	ou="OU=redhat,OU=Linux"	ou="OU=redhat,OU=Linux"	ou="XD.LOCAL/Linux/redhat"	ou="Linux/redhat"
RHEL 7	ou="Linux/redhat"	ou="Linux/redhat"	ou="XD.LOCAL/Linux/redhat"	ou="Linux/redhat"
Ubuntu	ou="Linux/ubuntu"	ou="Linux/ubuntu"	ou="XD.LOCAL/Linux/ubuntu"	ou="Linux/ubuntu"
SUSE 12.5	ou="Linux/suse"	ou="Linux/suse"	ou="XD.LOCAL/Linux/suse"	ou="Linux/suse"
Debian	ou="Linux/debian"	ou="Linux/debian"	ou="XD.LOCAL/Linux/debian"	ou="Linux/debian"

- Die einfache Installation unterstützt reines IPv6 ab Linux VDA 7.16. Es gelten die folgenden Voraussetzungen und Einschränkungen:
  - Ihr Linux-Repository muss so konfiguriert sein, dass Ihr Computer die erforderlichen Pakete über reine IPv6-Netzwerke herunterladen kann.
  - Centrify wird in reinen IPv6-Netzwerken nicht unterstützt.

> **Hinweis:**
>
> Wenn Ihr Netzwerk reines IPv6 ist und alle Ihre Eingaben im korrekten IPv6-Format vorliegen, registriert sich der VDA über IPv6 beim Delivery Controller™. Wenn Ihr Netzwerk eine hybride IPv4- und IPv6-Konfiguration aufweist, bestimmt der Typ der ersten DNS-IP-Adresse, ob IPv4 oder IPv6 für die Registrierung verwendet wird.

- Wenn Sie Centrify als Methode zum Beitritt zu einer Domäne wählen, benötigt das Skript ctxinstall.sh das Centrify-Paket. Es gibt zwei Möglichkeiten für ctxinstall.sh, das Centrify-Paket zu erhalten:
  - Die einfache Installation hilft, das Centrify-Paket automatisch aus dem Internet herunterzuladen. Im Folgenden sind die URLs für jede Distribution aufgeführt:

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

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

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

    Für Ubuntu/Debian: wget `<https://downloads.centrify.com/products/infrastructure-services/19.9/centrify-infrastructure-services-19.9-deb8-x86_64.tgz?_ga=2.151462329.1042350071.1592881996-604509155.1572850145>`
  - Rufen Sie das Centrify-Paket aus einem lokalen Verzeichnis ab. Um das Verzeichnis des Centrify-Pakets festzulegen, gehen Sie wie folgt vor:

a. Erstellen Sie die Datei /tmp/ctxinstall.conf auf dem Linux-VDA-Server, falls sie nicht existiert.

b. Fügen Sie die Zeile „centrifypkgpath=\<Pfadname\>“ zur Datei hinzu.

Zum Beispiel:

```
cat /tmp/ctxinstall.conf

set “centrifypkgpath=/home/mydir”

ls  -ls  /home/mydir

    9548 -r-xr-xr-x. 1 root root  9776688 May 13  2016 adcheck-
rhel4-x86_64

    4140 -r--r--r--. 1 root root  4236714 Apr 21  2016
centrifyda-3.3.1-rhel4-x86_64.rpm

    33492 -r--r--r--. 1 root root 34292673 May 13  2016
centrifydc-5.3.1-rhel4-x86_64.rpm

    4 -rw-rw-r--. 1 root root     1168 Dec  1  2015 centrifydc-
install.cfg

    756 -r--r--r--. 1 root root   770991 May 13  2016 centrifydc-
ldapproxy-5.3.1-rhel4-x86_64.rpm

    268 -r--r--r--. 1 root root   271296 May 13  2016 centrifydc-
nis-5.3.1-rhel4-x86_64.rpm

    1888 -r--r--r--. 1 root root  1930084 Apr 12  2016 centrifydc-
openssh-7.2p2-5.3.1-rhel4-x86_64.rpm

    124 -rw-rw-r--. 1 root root   124543 Apr 19  2016 centrify-
suite.cfg

    0 lrwxrwxrwx. 1 root root       10 Jul  9  2012 install-
express.sh -> install.sh

    332 -r-xr-xr--. 1 root root   338292 Apr 10  2016 install.sh

    12 -r--r--r--. 1 root root    11166 Apr  9  2015 release-notes-
```

```
agent-rhel4-x86_64.txt

    4 -r--r--r--. 1 root root     3732 Aug 24  2015 release-notes-
da-rhel4-x86_64.txt

    4 -r--r--r--. 1 root root     2749 Apr  7  2015 release-notes-
nis-rhel4-x86_64.txt

    12 -r--r--r--. 1 root root     9133 Mar 21  2016 release-notes-
openssh-rhel4-x86_64.txt
```

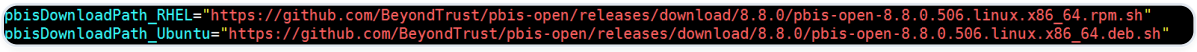
- Wenn Sie PBIS als Methode zum Beitreten einer Domäne wählen, benötigt das Skript ctxinstall.sh das PBIS-Paket. Es gibt zwei Möglichkeiten, wie ctxinstall.sh das PBIS-Paket beziehen kann:
  - Die einfache Installation hilft, das PBIS-Paket automatisch aus dem Internet herunterzuladen. Im Folgenden sind die URLs für jede Distribution aufgeführt:

    RHEL 7 / CentOS 7 / SUSE 12.5: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.rpm.sh`

    RHEL 8 / CentOS 8: `wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh`

    Ubuntu/Debian: `wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh`
  - Rufen Sie eine bestimmte Version des PBIS-Pakets aus dem Internet ab. Ändern Sie dazu die Zeile „pbisDownloadPath“ in der Datei /opt/Citrix/VDA/sbin/ctxinstall.sh, um die URL des PBIS-Pakets festzulegen.

    Ein Beispiel finden Sie im folgenden Screenshot:



Schritt 2: Den Hypervisor vorbereiten

Einige Änderungen sind erforderlich, wenn der Linux-VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausgeführt wird. Nehmen Sie die folgenden Änderungen entsprechend der verwendeten Hypervisor-Plattform vor. Es sind keine Änderungen erforderlich, wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen.

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

Wenn die Citrix Hypervisor Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und Citrix Hypervisor auf, da beide versuchen, die Systemuhr zu verwalten. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit dem NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen können Sie, wenn Sie einen paravirtualisierten Linux-Kernel mit installierten Citrix VM Tools ausführen, innerhalb der Linux-VM überprüfen, ob die Citrix Hypervisor Zeitsynchronisierungsfunktion vorhanden und aktiviert ist:

```
su -



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

Dieser Befehl gibt 0 oder 1 zurück:

- 0 – Die Zeitsynchronisierungsfunktion ist aktiviert und muss deaktiviert werden.
- 1 – Die Zeitsynchronisierungsfunktion ist deaktiviert, und es sind keine weiteren Maßnahmen erforderlich.

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

Falls aktiviert, deaktivieren Sie die Zeitsynchronisierungsfunktion, indem Sie 1 in die Datei schreiben:

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

Um diese Änderung dauerhaft und nach einem Neustart beizubehalten, bearbeiten Sie die Datei ***/etc/sysctl.conf*** und fügen Sie die Zeile hinzu:

`xen.independent_wallclock = 1`

Um diese Änderungen zu überprüfen, starten Sie das System neu:

```
su -



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

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

Die Linux-VMs mit installierten Hyper-V Linux Integration Services können die Hyper-V Zeitsynchronisierungsfunktion anwenden, um die Zeit des Host-Betriebssystems zu nutzen. Um sicherzustellen, dass die Systemuhr genau bleibt, müssen Sie diese Funktion zusammen mit den NTP-Diensten aktivieren.

Vom Verwaltungsbetriebssystem aus:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Für die Einstellungen einer Linux-VM wählen Sie **Integrationsdienste**.
3. Stellen Sie sicher, dass **Zeitsynchronisierung** ausgewählt ist.

> **Hinweis:**

> Dieser Ansatz unterscheidet sich von VMware und Citrix Hypervisor, wo die Host-Zeitsynchronisierung deaktiviert ist, um Konflikte mit NTP zu vermeiden. Die Hyper-V-Zeitsynchronisierung kann mit der NTP-Zeitsynchronisierung koexistieren und diese ergänzen.

Zeitsynchronisierung auf ESX und ESXi beheben

Wenn die VMware-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und dem Hypervisor auf, da beide versuchen, die Systemuhr zu synchronisieren. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit NTP synchronisiert wird. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel mit installierten VMware Tools ausführen:

1. Öffnen Sie den vSphere Client.

2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Eigenschaften der virtuellen Maschine** die Registerkarte **Optionen**.
4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Erweitert** die Option **Gastzeit mit Host synchronisieren**.

Schritt 3: (Nur für Ubuntu 16.04) OpenJDK 11 installieren

Installieren Sie unter Ubuntu 16.04 OpenJDK 11, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das neueste OpenJDK 11 von `<https://jdk.java.net/archive/>` herunter.
2. Führen Sie den Befehl `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` aus, um das heruntergeladene Paket zu entpacken.
3. (Optional) Führen Sie den Befehl `mv jdk-11.0.2/ <target directory>` aus, um OpenJDK in einem Zielverzeichnis zu speichern.
4. Führen Sie den Befehl `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` aus, um die Java-Laufzeitumgebung einzurichten.
5. Führen Sie den Befehl `java -version` aus, um die Java-Version zu überprüfen.

Schritt 4: Linux VDA-Paket herunterladen

Gehen Sie zur Citrix Virtual Apps and Desktops Downloadseite. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Komponenten**, um das Linux VDA-Paket herunterzuladen, das Ihrer Linux-Distribution entspricht.

Schritt 5: Linux VDA-Paket installieren

Um die Umgebung für den Linux VDA einzurichten, führen Sie die folgenden Befehle aus.

Für RHEL- und CentOS-Distributionen:

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

Für Ubuntu-/Debian-Distributionen:

```
sudo dpkg -i <PATH>/<Linux VDA deb>

sudo apt-get install -f
```

Hinweis:

Um die erforderlichen Abhängigkeiten für eine Debian-Distribution zu installieren, fügen Sie die Zeile `deb http://deb.debian.org/debian/ oldstable main` zur Datei /etc/apt/sources.list hinzu.

Für SUSE-Distributionen:

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

Schritt 6: Laufzeitumgebung einrichten, um die Installation abzuschließen

Hinweis:

Bevor Sie die Laufzeitumgebung einrichten, stellen Sie 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. Bearbeiten Sie für Debian die Datei `/etc/locale.gen`, indem Sie die Zeile `# en_US.UTF-8 UTF-8` auskommentieren, und führen Sie dann den Befehl `sudo locale-gen` aus.

Nach der Installation des Linux VDA-Pakets konfigurieren Sie die Laufzeitumgebung mit dem Skript ctxinstall.sh. Sie können das Skript im interaktiven Modus oder im unbeaufsichtigten Modus ausführen.

Hinweis:

Die einfache Installation kann während des Downloads der .NET Core Runtime, die über 27 MB groß ist, nicht reagieren. Den Download-Fortschritt können Sie in /var/log/ctxinstall.log überprüfen.

Interaktiver Modus:

Führen Sie für eine manuelle Konfiguration den folgenden Befehl aus und geben Sie den entsprechenden Parameter bei jeder Aufforderung ein.

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

Stiller Modus:

Um die einfache Installation im stillen Modus zu verwenden, legen Sie die folgenden Umgebungsvariablen fest, bevor Sie ctxinstall.sh ausführen.

- **CTX_EASYINSTALL_HOSTNAME=host-name** – Bezeichnet den Hostnamen 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-Realm-Name.
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**
- **CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind \| sssd \| centrify \| pbis** – Bezeichnet die Active Directory-Integrationsmethode.
- **CTX_EASYINSTALL_USERNAME=domain-user-name** – Bezeichnet den Namen des Domänenbenutzers; wird zum Beitreten zur Domäne verwendet.
- **CTX_EASYINSTALL_PASSWORD=password** – Gibt das Kennwort des Domänenbenutzers an; wird zum Beitreten zur Domäne verwendet.

Das Skript ctxsetup.sh verwendet die folgenden Variablen:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA benötigt eine durch Leerzeichen getrennte Liste von Fully Qualified Domain Names (FQDNs) der Delivery Controller, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. 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 Start der Maschine gestartet.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux Virtual Desktop-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig die Ports 80 und 1494) automatisch in der System-Firewall für den Linux Virtual Desktop öffnen.
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung von grafikintensiven Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für VDI-Desktops (Einzelsitzung) konfiguriert – (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Gibt an, ob die Maschine als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes freigegebenes Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie den Wert auf Y.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf eine lokale Site zu beschränken, geben Sie einen DNS-Sitenamen an. Falls nicht erforderlich, setzen Sie den Wert auf **\<none\>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum Beispiel ad1.mycompany.com:389. Falls nicht erforderlich, setzen Sie den Wert auf **\<none\>**.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne gesetzt ist (z. B. DC=mycompany,DC=com). Um die Suchleistung zu verbessern, können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Falls nicht erforderlich, setzen Sie den Wert auf **\<none\>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt keine AD-Gruppenrichtlinie, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen.
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** – Der Pfad zur Installation der .NET Core Runtime 3.1 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.

- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/mate** – Gibt die GNOME- oder MATE-Desktop-Umgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der derzeit auf dem VDA installierte Desktop verwendet. Wenn der derzeit installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

> **Hinweis:**
>
> Sie können die Desktop-Umgebung für einen Ziel-Sitzungsbenutzer auch ändern, indem Sie die folgenden Schritte ausführen:
>
> a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.
> b. Bearbeiten Sie die `.xsession`-Datei, um eine Desktop-Umgebung basierend auf Distributionen anzugeben.
>
> **Für MATE-Desktop unter CentOS, Ubuntu und Debian**
>
> MSESSION="$(type -p mate-session)"
>
> \> wenn ; dann
>
> ```
> exec mate-session
> ```
>
> \> fi
>
> ```
> **Für GNOME-Desktop unter CentOS**
>
>
>
>    GSESSION="$(type -p gnome-session)"
> ```
>
> \> if ; then

```
    export GNOME_SHELL_SESSION_MODE=classic
```

\> exec gnome-session --session=gnome-classic

```
    fi

**Für GNOME-Desktop unter Ubuntu und Debian**



    GSESSION="$(type -p gnome-session)"
```

\> wenn ; dann

```
    exec gnome-session
```

\> fi

a. Teilen Sie die Dateiberechtigung 700 mit dem Ziel-Sitzungsbenutzer.

- **CTX_XDL_START_SERVICE=Y \| N** – Gibt an, ob die Linux VDA-Dienste gestartet werden, wenn die Konfiguration abgeschlossen ist.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Abhören von Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT** – Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

Wenn Parameter nicht festgelegt sind, wird die Installation in den interaktiven Modus zurückgesetzt, mit einer Aufforderung zur Benutzereingabe. Wenn alle Parameter bereits über die Umgebungsvariablen festgelegt wurden, fordert das Skript ctxinstall.sh weiterhin zur Benutzereingabe für den Pfad zur Installation von .NET Core Runtime 3.1 auf.

Im unbeaufsichtigten Modus müssen Sie die folgenden Befehle ausführen, um Umgebungsvariablen festzulegen und dann das Skript ctxinstall.sh auszuführen.

```
export CTX_EASYINSTALL_HOSTNAME=host-name


export CTX_EASYINSTALL_DNS=ip-address-of-dns


export CTX_EASYINSTALL_NTPS=address-of-ntps


export CTX_EASYINSTALL_DOMAIN=domain-name


export CTX_EASYINSTALL_REALM=realm-name


export CTX_EASYINSTALL_FQDN=ad-fqdn-name


export CTX_EASYINSTALL_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis


export CTX_EASYINSTALL_USERNAME=domain-user-name


export CTX_EASYINSTALL_PASSWORD=password


export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
```

```
export CTX_XDL_DDC_LIST=‘list-ddc-fqdns’

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y | N

export CTX_XDL_ADD_FIREWALL_RULES=Y | N

export CTX_XDL_HDX_3D_PRO=Y | N

export CTX_XDL_VDI_MODE=Y | N

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

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

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

export CTX_XDL_FAS_LIST=‘list-fas-servers’ | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
```

```
export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y | N

sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh
```

Wenn Sie den Befehl sudo ausführen, geben Sie die Option -E ein, um die vorhandenen Umgebungsvariablen an die neue Shell zu übergeben, die er erstellt. Wir empfehlen, dass Sie eine Shell-Skriptdatei aus den vorhergehenden Befehlen mit **#\!/bin/bash** als erster Zeile erstellen.

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \
```

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

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \
```

```
CTX_XDL_START_SERVICE=Y|N \


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

Schritt 7: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um häufige Konfigurationsprobleme in einer Linux VDA-Umgebung zu überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 8: Linux VDA ausführen

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start


sudo /sbin/service ctxvda start
```

Linux VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop


sudo /sbin/service ctxhdx stop
```

Hinweis:

Bevor Sie die Dienste `ctxvda` und `ctxhdx` beenden, führen Sie den Befehl `service ctxmonitorservice stop` aus, um den Überwachungsdienst-Daemon zu beenden. Andernfalls startet der Überwachungsdienst-Daemon die von Ihnen beendeten Dienste neu.

Linux VDA neu starten:

So starten Sie die Linux VDA-Dienste neu:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart



sudo /sbin/service ctxvda start
```

Status des Linux VDA überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

Schritt 9: Maschinenkataloge in Citrix Virtual Apps oder Citrix Virtual Desktops™ erstellen

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt dem traditionellen Windows VDA-Ansatz. Eine detailliertere Beschreibung zum Ausführen dieser Aufgaben finden Sie unter Maschinenkataloge erstellen und Maschinenkataloge verwalten.

Für die Erstellung von Maschinenkatalogen, die Linux VDA-Maschinen enthalten, gibt es einige Einschränkungen, die den Prozess von der Erstellung von Maschinenkatalogen für Windows VDA-Maschinen unterscheiden:

- Wählen Sie für das Betriebssystem Folgendes aus:
  - Die Option **Multi-session OS** für ein Bereitstellungsmodell mit gehosteten Shared Desktops.
  - Die Option **Single-session OS** für ein dediziertes VDI-Desktop-Bereitstellungsmodell.

- Mischen Sie keine Linux- und Windows-VDA-Maschinen im selben Maschinenkatalog.

Hinweis:

Frühere Versionen von Citrix Studio unterstützten den Begriff „Linux-Betriebssystem“ nicht. Die Auswahl der Option **Windows Server OS** oder **Server OS** impliziert jedoch ein äquivalentes Bereitstellungsmodell für gehostete Shared Desktops. Die Auswahl der Option **Windows Desktop OS** oder **Desktop OS** impliziert ein Bereitstellungsmodell mit einem Benutzer pro Maschine.

Tipp:

Wenn Sie eine Maschine aus der Active Directory-Domäne entfernen und wieder hinzufügen, müssen Sie die Maschine erneut aus dem Maschinenkatalog entfernen und hinzufügen.

Schritt 10: Bereitstellungsgruppen in Citrix Virtual Apps™ oder Citrix Virtual Desktops erstellen

Der Prozess zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen, die Linux-VDA-Maschinen enthalten, ist nahezu identisch mit dem für Windows-VDA-Maschinen. Eine detailliertere Beschreibung zur Ausführung dieser Aufgaben finden Sie unter Bereitstellungsgruppen erstellen.

Für die Erstellung von Bereitstellungsgruppen, die Linux-VDA-Maschinenkataloge enthalten, gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die von Ihnen ausgewählten AD-Benutzer und -Gruppen ordnungsgemäß für die Anmeldung an den Linux-VDA-Maschinen konfiguriert wurden.
- Lassen Sie die Anmeldung von nicht authentifizierten (anonymen) Benutzern nicht zu.
- Mischen Sie die Bereitstellungsgruppe nicht mit Maschinenkatalogen, die Windows-Maschinen enthalten.

Wichtig:

> Die Veröffentlichung von Anwendungen wird ab Linux VDA Version 1.4 unterstützt. Der Linux VDA unterstützt jedoch nicht die Bereitstellung von Desktops und Apps auf derselben Maschine.

> Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2106.

Problembehandlung

Verwenden Sie die Informationen in diesem Abschnitt, um Probleme zu beheben, die bei der Verwendung der einfachen Installation auftreten können.

Beitritt zu einer Domäne mit SSSD schlägt fehl

Es kann ein Fehler auftreten, wenn Sie versuchen, einer Domäne beizutreten, wobei die Ausgabe der folgenden ähnelt (Protokolle für Bildschirmausgabe überprüfen):

`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:

```
2016-11-04 02:11:52.317 [INFO ] - The Citrix Desktop Service successfully
obtained the following list of 1 delivery controller(s) with which to
register: 'CTXDDC.citrixlab.local (10.158.139.214)'.

2016-11-04 02:11:52.362 [ERROR] -
RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register
with http://CTXDDC.citrixlab.local:80/Citrix/CdsController/IRegistrar.
Error: General security error (An error occurred in trying to obtain a
TGT: Client not found in Kerberos database (6))

2016-11-04 02:11:52.362 [ERROR] - The Citrix Desktop Service cannot
connect to the delivery controller 'http://CTXDDC.citrixlab.local:80/
Citrix/CdsController/IRegistrar' (IP Address '10.158.139.214')

Check the following:- The system clock is in sync between this machine and
the delivery controller.

-  The Active Directory provider (e.g. winbind daemon) service is running
and correctly configured.
```

```
-  Kerberos is correctly configured on this machine.

If the problem persists, please refer to Citrix Knowledge Base article
CTX117248 for further information.

Error Details:

Exception 'General security error (An error occurred in trying to obtain a
TGT: Client not found in Kerberos database (6))' of type 'class
javax.xml.ws.soap.SOAPFaultException'.

2016-11-04 02:11:52.362 [INFO ] -
RegistrationManager.AttemptRegistrationWithSingleDdc: The current time for
this VDA is Fri Nov 04 02:11:52 EDT 2016.

Ensure that the system clock is in sync between this machine and the
delivery controller.

Verify the NTP daemon is running on this machine and is correctly
configured.

2016-11-04 02:11:52.364 [ERROR] - Could not register with any controllers.
Waiting to try again in 120000 ms. Multi-forest - false

2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
register with any controllers in the last 470 minutes.
```

/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`

So beheben Sie dieses Problem:

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 auf dem Delivery Controller.

4. Führen Sie /opt/Citrix/VDA/sbin/ctxinstall.sh aus.
5. Erstellen Sie den Maschinenkatalog und die Bereitstellungsgruppe auf dem Delivery Controller.

Ubuntu-Desktopsitzungen zeigen einen grauen Bildschirm an

Dieses Problem tritt auf, wenn Sie eine Sitzung starten, die dann in einem leeren Desktop blockiert wird. Außerdem zeigt die Konsole des Computers einen grauen Bildschirm an, wenn Sie sich mit einem lokalen Benutzerkonto anmelden.

So beheben Sie dieses Problem:

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 die folgende Zeile zu `/etc/lightdm/lightdm.conf` hinzu:

   `greeter-show-manual-login=true`

Versuche, Ubuntu-Desktopsitzungen zu starten, schlagen aufgrund eines fehlenden Home-Verzeichnisses fehl

/var/log/xdl/hdx.log:

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



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



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



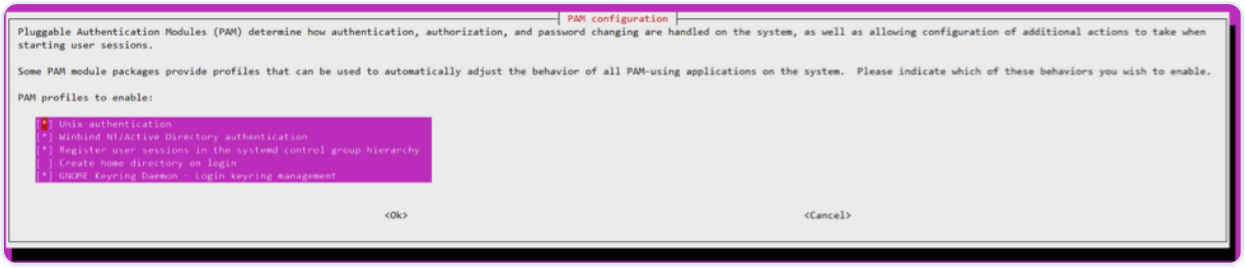
2016-11-02 13:21:59.217 <P22449:S1> citrix-ctxgfx: main: Exiting normally.
```

Tipp:

> Die Hauptursache dieses Problems ist, dass das Home-Verzeichnis für den Domänenadministrator nicht erstellt wurde.

> So beheben Sie dieses Problem:

1. Geben Sie in einer Befehlszeile **pam-auth-update** ein.
2. Vergewissern Sie sich im daraufhin angezeigten Dialogfeld, dass **Create home directory login** ausgewählt ist.



Sitzung startet nicht oder wird schnell mit dbus-Fehler beendet

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

```
Oct 27 04:17:16 CentOS7 citrix-ctxhdx[8978]: Session started for user
CITRIXLAB\ctxadmin.



Oct 27 04:17:18 CentOS7 kernel: traps: gnome-session[19146] trap int3
ip:7f89b3bde8d3 sp:7fff8c3409d0 error:0



Oct 27 04:17:18 CentOS7 gnome-session[19146]: ERROR: Failed to connect to
system bus: Exhausted all available authentication mechanisms (tried:
EXTERNAL, DBUS_COOKIE_SHA1, ANONYMOUS) (available: EXTERNAL,
DBUS_COOKIE_SHA1, ANONYMOUS)#012aborting...



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

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


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


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

Oder, alternativ für Ubuntu-Distributionen, verwenden Sie das Protokoll /var/log/syslog:

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


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


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


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


Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: message repeated 10
```

```
times: [ [pulseaudio] core-util.c: Failed to connect to system bus: Did
not receive a reply. Possible causes include: the remote application did
not send a reply, the message bus security policy blocked the reply, the
reply timeout expired, or the network connection was broken.]



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
```

Einige Gruppen oder Module werden erst nach einem Neustart wirksam. Wenn die **dbus**-Fehlermeldungen im Protokoll erscheinen, empfehlen wir Ihnen, das System neu zu starten und es erneut zu versuchen.

SELinux verhindert, dass SSHD auf das Home-Verzeichnis zugreift

Der Benutzer kann eine Sitzung starten, sich aber nicht anmelden.

/var/log/ctxinstall.log:

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



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



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



If you want to allow polyinstantiation to enabled



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

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

    Do

       setsebool -P polyinstantiation_enabled 1

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

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

Then you should report this as a bug.

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

      Do

       allow this access for now by executing:

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

```
# semodule -i mypol.pp
```

So beheben Sie dieses Problem:

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

   SELINUX=deaktiviert
2. Starten Sie den VDA neu.

Linux Virtual Delivery Agent für RHEL/CentOS manuell installieren

Wichtig:

Für Neuinstallationen empfehlen wir die Verwendung von Easy Install für eine schnelle Installation. Easy Install spart Zeit und Aufwand und ist weniger fehleranfällig als die in diesem Artikel beschriebene manuelle Installation.

Schritt 1: RHEL 8/CentOS 8, RHEL 7/CentOS 7 für die VDA-Installation vorbereiten

Schritt 1a: Netzwerkkonfiguration überprüfen

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

Schritt 1b: Hostnamen festlegen

Um sicherzustellen, dass der Hostname des Computers korrekt gemeldet wird, ändern Sie die Datei **/etc/hostname** so, dass sie nur den Hostnamen des Computers enthält.

`hostname`

Schritt 1c: Eine Loopback-Adresse dem Hostnamen zuweisen

Um sicherzustellen, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) des Computers korrekt zurückgemeldet werden, ändern Sie die folgende Zeile der Datei `/etc/hosts`, sodass sie den FQDN und den Hostnamen als erste zwei Einträge enthält:

127.0.0.1 **Hostname-FQDN Hostname** localhost localhost.localdomain localhost4 localhost4.localdomain4

Zum 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 keine NetBIOS-Namenskürzung. Daher darf der Hostname 15 Zeichen nicht überschreiten.

> **Tipp:**

> Verwenden Sie nur die Zeichen a–z, A–Z, 0–9 und Bindestrich (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Beginnen Sie einen Hostnamen nicht mit einer Zahl und beenden Sie ihn nicht mit einem Bindestrich. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Schritt 1d: Hostnamen überprüfen

Überprüfen Sie, ob der Hostname korrekt festgelegt ist:

```
hostname
```

Dieser Befehl gibt nur den Hostnamen des Computers zurück und nicht seinen vollqualifizierten Domänennamen (FQDN).

Überprüfen Sie, ob der FQDN korrekt festgelegt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN des Computers zurück.

Schritt 1e: Namensauflösung und Dienstverfügbarkeit prüfen

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

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

Wenn Sie den FQDN nicht auflösen oder keine der Maschinen anpingen können, überprüfen Sie die Schritte, bevor Sie fortfahren.

Schritt 1f: Uhrensynchronisierung konfigurieren

Eine genaue Uhrensynchronisierung zwischen den VDAs, Delivery Controllern und Domänencontrollern ist entscheidend. Das Hosten des Linux VDA als virtuelle Maschine kann zu Problemen mit der Zeitverschiebung führen. Aus diesem Grund wird die Synchronisierung der Zeit mit einem externen Zeitdienst bevorzugt.

Eine Standardumgebung von RHEL 8/RHEL 7 verwendet den Chrony-Daemon (`chronyd`) zur Uhrensynchronisierung.

Chrony-Dienst konfigurieren

Bearbeiten Sie als Root-Benutzer die Datei **/etc/chrony.conf** und fügen Sie einen Servereintrag für jeden externen Zeitserver 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-Pool-Servern. Fügen Sie einen Servereintrag für jeden Active Directory-Domänencontroller in der Domäne hinzu.

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

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

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

Schritt 1g: OpenJDK 11 installieren

Der Linux VDA erfordert die Installation von OpenJDK 11. Die Laufzeitumgebung wird bei der Installation des Linux VDA automatisch als Abhängigkeit installiert.

Bestätigen Sie die korrekte Version:

```
sudo yum info java-11-openjdk
```

Das vorinstallierte OpenJDK ist möglicherweise eine frühere Version. Aktualisieren Sie auf OpenJDK 11:

```
sudo yum -y update java-11-openjdk
```

Schritt 1h: PostgreSQL installieren

Der Linux VDA erfordert entweder PostgreSQL 10.5 oder höher unter RHEL 8 oder PostgreSQL 9.2 oder höher unter RHEL 7.

Installieren Sie die folgenden Pakete:

```
sudo yum -y install postgresql-server



sudo yum -y install postgresql-jdbc
```

Der folgende Schritt nach der Installation ist erforderlich, um die Datenbank zu initialisieren und sicherzustellen, dass der Dienst beim Start des Computers gestartet wird. Diese Aktion erstellt

Datenbankdateien unter **/var/lib/pgsql/data**. Der Befehl unterscheidet sich zwischen PostgreSQL 10 und 9:

```
sudo postgresql-setup initdb
```

Schritt 1i: PostgreSQL starten

Starten Sie den Dienst beim Systemstart und starten Sie den Dienst sofort:

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

Überprüfen Sie die Version von PostgreSQL mit:

```
psql --version
```

(Nur RHEL 7) Überprüfen Sie, ob das Datenverzeichnis mit dem Befehlszeilendienstprogramm **psql** festgelegt ist:

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

Schritt 2: Hypervisor vorbereiten

Einige Änderungen sind erforderlich, wenn der Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausgeführt wird. Nehmen Sie die folgenden Änderungen entsprechend der verwendeten Hypervisor-Plattform vor. Es sind keine Änderungen erforderlich, wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen.

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

Wenn die Citrix Hypervisor Time Sync-Funktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und Citrix Hypervisor auf, da beide versuchen, die Systemuhr zu verwalten. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit dem NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen können Sie, wenn Sie einen paravirtualisierten Linux-Kernel mit installierten Citrix VM Tools ausführen, innerhalb der Linux-VM überprüfen, ob die Citrix Hypervisor Time Sync-Funktion vorhanden und aktiviert ist:

```
su -


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

Dieser Befehl gibt 0 oder 1 zurück:

- 0 – Die Zeitsynchronisierungsfunktion ist aktiviert und muss deaktiviert werden.
- 1 – Die Zeitsynchronisierungsfunktion ist deaktiviert, und es sind keine weiteren Maßnahmen erforderlich.

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

Falls aktiviert, deaktivieren Sie die Zeitsynchronisierungsfunktion, indem Sie 1 in die Datei schreiben:

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

Um diese Änderung dauerhaft und nach einem Neustart beizubehalten, bearbeiten Sie die Datei ***/etc/sysctl.conf*** und fügen Sie die Zeile hinzu:

`xen.independent_wallclock = 1`

Um diese Änderungen zu überprüfen, starten Sie das System neu:

```
su -


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

Dieser Befehl gibt den Wert 1 zurück.

Beheben der Zeitsynchronisierung auf Microsoft Hyper-V

Die Linux-VMs mit installierten Hyper-V Linux Integration Services können die Hyper-V-Zeitsynchronisierungsfunktion verwenden, um die Zeit des Host-Betriebssystems zu nutzen. Um sicherzustellen, dass die Systemuhr genau bleibt, müssen Sie diese Funktion zusammen mit den NTP-Diensten aktivieren.

Vom Verwaltungsbetriebssystem aus:

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

> **Hinweis:**
>
> Dieser Ansatz unterscheidet sich von VMware und Citrix Hypervisor, wo die Host-Zeitsynchronisierung deaktiviert ist, um Konflikte mit NTP zu vermeiden. Die Hyper-V-Zeitsynchronisierung kann mit der NTP-Zeitsynchronisierung koexistieren und diese ergänzen.

Zeitsynchronisierung auf ESX und ESXi beheben

Wenn die VMware-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und dem Hypervisor auf, die beide versuchen, die Systemuhr zu synchronisieren. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel mit installierten VMware Tools ausführen:

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** die Option **Synchronize guest time with host**.

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

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

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

Befolgen Sie die Anweisungen entsprechend der von Ihnen gewählten Methode.

> **Hinweis:**
>
> Sitzungsstarts können fehlschlagen, wenn derselbe Benutzername für das lokale Konto im Linux VDA und das Konto in AD verwendet wird.

Samba Winbind

Installieren oder aktualisieren Sie die erforderlichen Pakete:

Für RHEL 8/CentOS 8:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation
oddjob-mkhomedir realmd authselect
```

Für RHEL 7/CentOS 7:

```
sudo yum -y install samba-winbind samba-winbind-clients krb5-workstation
authconfig oddjob-mkhomedir
```

Winbind-Daemon beim Systemstart aktivieren

Der Winbind-Daemon muss so konfiguriert werden, dass er beim Systemstart gestartet wird:

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

Winbind-Authentifizierung konfigurieren

Konfigurieren Sie den Computer für die Kerberos-Authentifizierung mithilfe von Winbind:

1. Führen Sie den folgenden Befehl aus.

   Für RHEL 8:

   ```
   sudo authselect select winbind with-mkhomedir --force
   ```

   Für RHEL 7:

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

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

   Wenn eine DNS-basierte Suche nach dem KDC-Server und dem Realm-Namen erforderlich ist, fügen Sie die folgenden zwei Optionen zum vorherigen Befehl hinzu:

   `--enablekrb5kdcdns --enablekrb5realmdns`

   Ignorieren Sie alle Fehler, die vom `authconfig` Befehl bezüglich des Fehlers beim Starten des `winbind` Dienstes zurückgegeben werden. Die Fehler können auftreten, wenn `authconfig` versucht, den `winbind` Dienst zu starten, ohne dass der Computer bereits der Domäne beigetreten ist.

2. Öffnen Sie **/etc/samba/smb.conf** und fügen Sie die folgenden Einträge unter dem Abschnitt \[Global\] hinzu, aber nach dem Abschnitt, der vom `authconfig` Tool generiert wurde:

   `kerberos method = secrets and keytab`

   `winbind refresh tickets = true` `winbind offline logon = no`

3. (Nur RHEL 8) Öffnen Sie **/etc/krb5.conf** und fügen Sie Einträge unter den Abschnitten `[libdefaults]`, `[realms]` und `[domain_realm]` 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 System-Keytab-Datei /etc/krb5.keytab, um sich beim Delivery Controller zu authentifizieren und zu registrieren. Die vorherige Kerberos-Methodeneinstellung zwingt Winbind dazu, die System-Keytab-Datei zu erstellen, wenn der Computer zum ersten Mal der Domäne beitritt.

Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

RHEL 8:

```
sudo realm join -U user --client-software=winbind REALM
```

RHEL 7:

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

REALM ist der Kerberos-Realm-Name in Großbuchstaben, und **user** ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Domäne besitzt.

PAM für Winbind konfigurieren

Standardmäßig aktiviert die Konfiguration für das Winbind PAM-Modul (pam_winbind) weder das Kerberos-Ticket-Caching noch die Erstellung von Home-Verzeichnissen. Öffnen Sie **/etc/security/pam_winbind.conf** und fügen Sie die folgenden Einträge unter dem Abschnitt \[Global\] hinzu oder ändern Sie sie:

`krb5_auth = yes`

`krb5_ccache_type = FILE` `mkhomedir = yes`

Stellen Sie sicher, dass alle führenden Semikolons aus jeder Einstellung entfernt werden. Diese Änderungen erfordern einen Neustart des Winbind-Daemons:

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

Tipp:

Der `winbind`-Daemon bleibt nur aktiv, wenn der Computer einer Domäne beigetreten ist.

Öffnen Sie **/etc/krb5.conf** und ändern Sie die folgende Einstellung im Abschnitt \[libdefaults\] von KEYRING auf den Typ FILE:

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben.

Führen Sie den Befehl **net ads** von Samba aus, um zu überprüfen, ob der Computer einer Domäne beigetreten ist:

```
sudo net ads testjoin
```

Führen Sie den folgenden Befehl aus, um zusätzliche Informationen zum Domänen- und Computerobjekt zu überprüfen:

```
sudo net ads info
```

Kerberos-Konfiguration überprüfen

Um sicherzustellen, dass Kerberos korrekt für die Verwendung mit dem Linux VDA konfiguriert ist, überprüfen Sie, ob die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der verfügbaren Schlüssel für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten an. Führen Sie den Kerberos-Befehl `kinit` aus, um den Computer mit diesen Schlüsseln beim Domänencontroller zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Die Computer- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Computerkonto mit folgendem Befehl zwischengespeichert wurde:

```
sudo klist
```

Überprüfen Sie die Kontodetails des Computers mit folgendem Befehl:

```
sudo net ads status
```

Benutzerauthentifizierung überprüfen

Verwenden Sie das Tool **wbinfo**, um zu überprüfen, ob Domänenbenutzer sich bei der Domäne authentifizieren können:

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

Die hier angegebene Domäne ist der AD-Domänenname, nicht der Kerberos-Realm-Name. Für die Bash-Shell muss der Backslash (\\) mit einem weiteren Backslash maskiert werden. Dieser Befehl gibt eine Meldung zurück, die den Erfolg oder Misserfolg anzeigt.

Um zu überprüfen, ob das Winbind PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username

id -u
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformationscache gültig und nicht abgelaufen sind:

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

Ein ähnlicher Test kann durchgeführt werden, indem 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

Gehen Sie davon aus, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und Ihnen administrative Berechtigungen zum Erstellen von Computerobjekten in Active Directory erteilt wurden.

Domänenbenutzern die Anmeldung an Linux VDA-Maschinen ermöglichen

Um Domänenbenutzern das Herstellen von HDX™-Sitzungen auf einer Linux VDA-Maschine zu ermöglichen:

1. Öffnen Sie in der Verwaltungskonsole „Active Directory-Benutzer und -Computer“ die Active Directory-Benutzereigenschaften für dieses Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix-Konto** aus.
3. Aktivieren Sie **Unix-aktiviert**.
4. Legen Sie die **Primäre GID-Nummer** auf die Gruppen-ID einer tatsächlichen Domänenbenutzergruppe fest.

> **Hinweis:**
>
> Diese Anweisungen sind äquivalent für die Einrichtung von Domänenbenutzern zur Anmeldung über die Konsole, RDP, SSH oder jedes andere Remoting-Protokoll.

Quest auf Linux VDA konfigurieren

SELINUX-RICHTLINIENERZWINGUNG UMGEHEN

In der Standard-RHEL-Umgebung ist SELinux vollständig erzwungen. Diese Erzwingung beeinträchtigt die von Quest verwendeten IPC-Mechanismen für Unix-Domänensockets und verhindert, dass Domänenbenutzer sich anmelden können.

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

`SELINUX=permissive`

Diese Änderung erfordert einen Neustart des Computers:

```
reboot
```

> **Wichtig:**
>
> Verwenden Sie diese Einstellung mit Vorsicht. Das erneute Aktivieren der SELinux-Richtlinienerzwingung nach der Deaktivierung kann zu einer vollständigen Sperrung führen, selbst für den Root-Benutzer und andere lokale Benutzer.

VAS-Daemon konfigurieren

Die automatische Verlängerung von Kerberos-Tickets muss aktiviert und getrennt werden. Die Authentifizierung (Offline-Anmeldung) muss deaktiviert werden.

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Dieser Befehl setzt das Verlängerungsintervall auf neun Stunden (32.400 Sekunden), was eine Stunde weniger ist als die standardmäßige Ticket-Lebensdauer von 10 Stunden. Legen Sie diesen Parameter auf einen niedrigeren Wert fest, wenn die Ticket-Lebensdauer auf den Systemen kürzer ist.

PAM und NSS konfigurieren

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

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



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

Windows-Domäne beitreten

Fügen Sie die Linux-Maschine der Active Directory-Domäne mit dem Quest-Befehl **vastool** hinzu:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

Der Benutzer ist ein beliebiger Domänenbenutzer, der über Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne verfügt. Der **Domänenname** ist der DNS-Name der Domäne, zum Beispiel example.com.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine mit Quest verbundene Linux-Maschine in der Domäne ist:

```
sudo /opt/quest/bin/vastool info domain
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl den Domänennamen zurück. Wenn die Maschine keiner Domäne beigetreten ist, wird der folgende Fehler 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 zu überprüfen, ob Quest Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username

id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die UID erstellt wurde, die vom Befehl **id -u** zurückgegeben wird:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

```
exit
```

Ein ähnlicher Test kann durchgeführt werden, indem 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

Einer Windows-Domäne beitreten

Nachdem der Centrify DirectControl Agent installiert wurde, treten Sie mit der Linux-Maschine der Active Directory-Domäne mithilfe des Centrify-Befehls `adjoin` bei:

```
su –

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

Der Parameter user ist ein beliebiger Active Directory-Domänenbenutzer, der über Berechtigungen verfügt, Computer der Active Directory-Domäne beizutreten. Der **Domänenname** ist der Name der Domäne, der die Linux-Maschine beitreten soll.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine mit Centrify verbundene Linux-Maschine in der Domäne ist:

```
su –

adinfo
```

Überprüfen Sie, ob der Wert "Joined to domain" gültig ist und der CentrifyDC-Modus "connected" zurückgibt. Wenn der Modus im Startzustand hängen bleibt, treten beim Centrify-Client Probleme mit der Serververbindung oder Authentifizierung auf.

Umfassendere System- und Diagnoseinformationen sind verfügbar unter:

```
adinfo --sysinfo all

adinfo –diag
```

Testen Sie die Konnektivität zu den verschiedenen Active Directory- und Kerberos-Diensten.

```
adinfo --test
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

SSSD

Wenn Sie SSSD verwenden, befolgen Sie die Anweisungen in diesem Abschnitt. Dieser Abschnitt enthält Anweisungen zum Beitreten einer Linux VDA-Maschine zu einer Windows-Domäne und bietet Anleitungen zur Konfiguration der Kerberos-Authentifizierung.

Um SSSD unter RHEL und CentOS einzurichten, gehen Sie wie folgt vor:

1. Der Domäne beitreten und Host-Keytab erstellen
2. SSSD einrichten
3. SSSD aktivieren
4. Kerberos-Konfiguration überprüfen
5. Benutzerauthentifizierung überprüfen

Der Domäne beitreten und Host-Keytab erstellen

SSSD bietet keine Active Directory-Clientfunktionen für den Domänenbeitritt und die Verwaltung der System-Keytab-Datei. Stattdessen können Sie `adcli`, `realmd` oder `Samba` verwenden.

Dieser Abschnitt beschreibt die Ansätze `Samba` und `adcli` für RHEL 7 bzw. RHEL 8. Für `realmd` siehe die RHEL- oder CentOS-Dokumentation. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

- **Samba (RHEL 7):**

  Erforderliche Pakete installieren oder aktualisieren:

  ```
  sudo yum -y install krb5-workstation authconfig oddjob-mkhomedir samba-common-tools
  ```

  Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

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

  Maschine für Samba- und Kerberos-Authentifizierung konfigurieren:

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

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

  > **Hinweis:**
  >
  > Die Einstellungen in diesem Artikel sind für das Einzeldomänen-, Einzelforst-Modell vorgesehen. Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur.
  >
  > Wenn eine DNS-basierte Suche des KDC-Servers und des Realm-Namens erforderlich ist, fügen Sie die folgenden zwei Optionen zum vorhergehenden Befehl hinzu:

  `--enablekrb5kdcdns --enablekrb5realmdns`

Öffnen Sie **/etc/samba/smb.conf** und fügen Sie die folgenden Einträge unter dem Abschnitt **\[Global\]** hinzu, jedoch nach dem vom Tool **authconfig** generierten Abschnitt:

`kerberos method = secrets and keytab`

`winbind offline logon = no`

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

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

REALM ist der Kerberos-Realm-Name in Großbuchstaben und **user** ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Domäne hat.

- **Adcli (RHEL 8):**

Erforderliche Pakete installieren oder aktualisieren:

```
sudo yum -y install samba-common samba-common-tools krb5-workstation
authconfig oddjob-mkhomedir realmd oddjob authselect
```

Maschine für Samba- und Kerberos-Authentifizierung konfigurieren:

```
sudo authselect select sssd with-mkhomedir --force
```

Öffnen Sie **/etc/krb5.conf** und fügen Sie die Einträge unter den Abschnitten und hinzu.

Unter dem Abschnitt :

`REALM = {`

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

Unter dem Abschnitt :

`realm = REALM` `.realm = REALM`

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

```
sudo realm join REALM -U user
```

REALM ist der Kerberos-Realm-Name in Großbuchstaben und **user** ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Domäne besitzt.

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.
- Nehmen Sie Konfigurationsänderungen an verschiedenen Dateien vor (z. B. sssd.conf).
- Starten Sie den Dienst **sssd**.

Eine Beispielkonfiguration für **sssd.conf** 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**, **server.ad.example.com** durch die entsprechenden Werte. Weitere Informationen finden Sie unter sssd-ad(5) – Linux-Manpage.

(Nur RHEL 8) Öffnen Sie **/etc/sssd/sssd.conf** und fügen Sie die folgenden Einträge unter dem Abschnitt 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 den Dateibesitz und die Berechtigungen für sssd.conf fest:

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

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

SSSD aktivieren

RHEL 8:

Führen Sie die folgenden Befehle aus, um SSSD zu aktivieren:

```
sudo systemctl restart sssd

sudo systemctl enable sssd.service

sudo chkconfig sssd on
```

RHEL 7/CentOS 7:

Verwenden Sie `authconfig`, um SSSD zu aktivieren. Installieren Sie **oddjob-mkhomedir**, um sicherzustellen, dass die Erstellung des Home-Verzeichnisses mit SELinux kompatibel ist:

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



sudo service sssd start



sudo chkconfig sssd on
```

Kerberos-Konfiguration überprüfen

Überprüfen Sie, ob die Systemdatei **keytab** erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der verfügbaren Schlüssel für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten an. Führen Sie den Kerberos-Befehl **kinit** aus, um den Computer mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit –k MACHINE\$@REALM
```

Der Computer- und Realm-Name müssen in Großbuchstaben angegeben werden. Das Dollarzeichen (**$**) muss mit einem Backslash (****) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Computerkonto zwischengespeichert wurde, indem Sie Folgendes verwenden:

```
sudo klist
```

Benutzerauthentifizierung überprüfen

Verwenden Sie den Befehl **getent**, um zu überprüfen, ob das Anmeldeformat unterstützt wird und NSS funktioniert:

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

Der Parameter **DOMAIN** gibt den Kurznamen der Domäne an. Wenn ein anderes Anmeldeformat erforderlich ist, überprüfen Sie dies zuerst mit dem Befehl **getent**.

Die unterstützten Anmeldeformate sind:

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

Um zu überprüfen, ob das SSSD-PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

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



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die von dem Befehl zurückgegebene **uid** erstellt wurde:

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

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache des Benutzers gültig und nicht abgelaufen sind.

```
klist
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

Erforderliches PBIS-Paket herunterladen

Für RHEL 7/CentOS 7, zum Beispiel:

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/
pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Für RHEL 8/CentOS 8, zum Beispiel:

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

PBIS-Installationsskript ausführbar machen

Für RHEL 7/CentOS 7, zum Beispiel:

```
chmod +x pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Für RHEL 8/CentOS 8, zum Beispiel:

```
chmod +x pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

PBIS-Installationsskript ausführen

Für RHEL 7/CentOS 7, zum Beispiel:

```
sh pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Für RHEL 8/CentOS 8, zum Beispiel:

```
sh pbis-open-9.1.0.551.linux.x86_64.rpm.sh
```

Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
/opt/pbis/bin/domainjoin-cli join domain-name user
```

Der **Benutzer** ist ein Domänenbenutzer, der über Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne verfügt. Der **Domänenname** ist der DNS-Name der Domäne, zum Beispiel example.com.

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine PBIS-verbundene Linux-Maschine in der Domäne ist:

```
/opt/pbis/bin/domainjoin-cli query
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl Informationen über die aktuell beigetretene AD-Domäne und OU zurück. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen

Um zu überprüfen, ob PBIS Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\user



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die vom Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Schritt 4: Installieren von .NET Core Runtime 3.1 als Voraussetzung

Bevor Sie den Linux VDA installieren, installieren Sie .NET Core Runtime 3.1 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

Führen Sie nach der Installation von .NET Core Runtime 3.1 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Legen Sie basierend auf der Befehlsausgabe den Binärpfad der .NET Core-Laufzeit fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Linux VDA-Paket herunterladen

Rufen Sie die Citrix Virtual Apps and Desktops-Downloadseite auf. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das Linux VDA-Paket herunterzuladen, das Ihrer Linux-Distribution entspricht.

Schritt 6: Linux VDA installieren

Sie können eine Neuinstallation durchführen oder eine vorhandene Installation von den beiden vorherigen Versionen und von einer LTSR-Version aktualisieren.

So führen Sie eine Neuinstallation durch

1. (Optional) Alte Version deinstallieren

   Wenn Sie eine frühere Version als die beiden vorherigen und eine LTSR-Version installiert haben, deinstallieren Sie diese, bevor Sie die neue Version installieren.

   a. Linux VDA-Dienste beenden:

   ```
   sudo /sbin/service ctxvda stop



   sudo /sbin/service ctxhdx stop
   ```

   Hinweis:

   Bevor Sie die Dienste `ctxvda` und `ctxhdx` beenden, führen Sie den Befehl **service ctxmonitorservice stop** aus, um den Monitor-Dienst-Daemon zu beenden. Andernfalls startet der Monitor-Dienst-Daemon die von Ihnen beendeten Dienste neu.

   b. Paket deinstallieren:

   ```
   sudo rpm -e XenDesktopVDA
   ```

   Hinweis:

   Um einen Befehl auszuführen, ist der vollständige Pfad erforderlich; alternativ können Sie **/opt/Citrix/VDA/sbin** und **/opt/Citrix/VDA/bin** zum Systempfad hinzufügen.

2. Linux VDA-Paket herunterladen

Rufen Sie die Citrix Virtual Apps and Desktops-Downloadseite auf. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das Linux VDA-Paket herunterzuladen, das Ihrer Linux-Distribution entspricht.

3. Installieren Sie den Linux VDA

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

     Für RHEL 8/CentOS 8:

     ```
     sudo yum install -y XenDesktopVDA-<version>.el8_x.x86_64.rpm
     ```

     Für RHEL 7/CentOS 7:

     ```
     sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
     ```

   - Installieren Sie die Linux VDA-Software mit dem RPM-Paketmanager. Zuvor müssen Sie die folgenden Abhängigkeiten auflösen:

     Für RHEL 8/CentOS 8:

     ```
     sudo rpm -i XenDesktopVDA-<version>.el8_x.x86_64.rpm
     ```

     Für RHEL 7/CentOS 7:

     ```
     sudo rpm -i XenDesktopVDA-<version>.el7_x.x86_64.rpm
     ```

     RPM-Abhängigkeitsliste für RHEL 8/CentOS 8:

     ```
     ibus >= 1.5



     nss-tools >= 3.44.0



     gperftools-libs >= 2.4
     ```

```
cyrus-sasl-gssapi >= 2.1

python2 >= 2.7~

postgresql-jdbc >= 42.2.3

postgresql-server >= 10.6

java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.8.0

policycoreutils-python-utils >= 2.9

python3-policycoreutils >= 2.9

dbus >= 1.12.8

dbus-common >= 1.12.8
```

```
dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

motif >= 2.3.4

pam >= 1.3.1

util-linux >= 2.32.1
```

```
util-linux-user >= 2.32.1


xorg-x11-utils >= 7.5


bash >= 4.4


findutils >= 4.6


gawk >= 4.2


sed >= 4.5


cups >= 2.2


foomatic-filters >= 4.0.9


cups-filters >= 1.20.0


ghostscript >= 9.25


libxml2 >= 2.9
```

```
libmspack >= 0.7
```

RPM-Abhängigkeitsliste für RHEL 7/CentOS 7:

```
libmspack >= 0.5


ibus >= 1.5


cyrus-sasl-gssapi >= 2.1


gperftools-libs >= 2.4


nss-tools >= 3.44.0


postgresql-server >= 9.2


postgresql-jdbc >= 9.2


java-11-openjdk >= 11


ImageMagick >= 6.7.8.9


firewalld >= 0.3.9
```

```
policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

motif >= 2.3.4

pam >= 1.1.8

util-linux >= 2.23.2
```

```
bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

openldap >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9

python-requests >= 2.6.0
```

```
gperftools-libs >= 2.4

rpmlib(FileDigests) <= 4.6.0-1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

pmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsXz) <= 5.2-1
```

Hinweis:

Eine Matrix der Linux-Distributionen und Xorg-Versionen, die diese Version des Linux VDA unterstützt, finden Sie unter Systemanforderungen.

Nach der Installation des Linux VDA unter RHEL 7.x führen Sie den Befehl `sudo yum install -y python-websockify x11vnc` aus. Der Zweck ist die manuelle Installation von `python-websockify` und `x11vnc` zur Verwendung der Sitzungsschattenfunktion. Weitere Informationen finden Sie unter Sitzungen schatten.

So aktualisieren Sie eine vorhandene Installation

Sie können eine vorhandene Installation von den beiden vorherigen Versionen und von einer LTSR-Version aktualisieren.

Hinweis:

> Das Aktualisieren einer vorhandenen Installation überschreibt die Konfigurationsdateien unter /etc/xdl. Bevor Sie ein Upgrade durchführen, stellen Sie sicher, dass Sie die Dateien sichern.

- So aktualisieren Sie Ihre Software mit `Yum`:

  Für RHEL 7/CentOS 7:

  ```
  sudo yum install -y XenDesktopVDA-<version>.el7_x.x86_64.rpm
  ```

- So aktualisieren Sie Ihre Software mit dem RPM-Paketmanager:

  Für RHEL 7/CentOS 7:

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

Hinweis:

Wenn Sie RHEL 7 verwenden, stellen Sie sicher, dass Sie die folgenden Schritte ausführen, nachdem Sie die vorhergehenden Upgrade-Befehle ausgeführt haben:

1. `/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` ausführen, um den richtigen .NET-Laufzeitpfad festzulegen.
2. Starten Sie den `ctxvda`-Dienst neu.

Wichtig:

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

Schritt 7: NVIDIA GRID-Treiber installieren

Die Aktivierung von HDX 3D Pro erfordert zusätzliche Installationsschritte, um die erforderlichen Grafiktreiber auf dem Hypervisor und auf den VDA-Maschinen zu installieren.

Konfigurieren Sie Folgendes:

1. Citrix Hypervisor
2. VMware ESX

Befolgen Sie die Anweisungen für den von Ihnen gewählten Hypervisor.

Citrix Hypervisor:

Dieser detaillierte Abschnitt beschreibt die Installation und Konfiguration der NVIDIA GRID-Treiber auf Citrix Hypervisor.

VMware ESX:

Befolgen Sie die Informationen in diesem Handbuch, um die NVIDIA GRID-Treiber für VMware ESX zu installieren und zu konfigurieren.

VDA-Maschinen:

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

1. Stellen Sie vor dem Start sicher, dass die Linux-VM heruntergefahren ist.
2. Fügen Sie in XenCenter® eine GPU im GPU-Passthrough-Modus zur VM hinzu.
3. Starten Sie die RHEL-VM.

Um die Maschine für die NVIDIA GRID-Treiber vorzubereiten, führen Sie die folgenden Befehle aus:

```
yum install gcc



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



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

Befolgen Sie die Schritte im Red Hat Enterprise Linux-Dokument, um den NVIDIA GRID-Treiber zu installieren.

> **Hinweis:**

> Wählen Sie während der Installation des GPU-Treibers bei jeder Frage die Standardoption ('no').

> **Wichtig:**

> Nachdem GPU-Passthrough aktiviert wurde, ist die Linux-VM nicht mehr über XenCenter zugänglich. Verwenden Sie SSH zur Verbindung.

```
nvidia-smi

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

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

Legen Sie die korrekte Konfiguration für die Karte fest:

`etc/X11/ctx-nvidia.sh`

Um die Vorteile großer Auflösungen und Multi-Monitor-Funktionen nutzen zu können, benötigen Sie eine gültige NVIDIA-Lizenz. Um die Lizenz zu beantragen, befolgen Sie die Produktdokumentation aus dem „GRID Licensing Guide.pdf - DU-07757-001 September 2015“.

Schritt 8: Linux VDA konfigurieren

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Bevor Änderungen vorgenommen werden, überprüft das Skript die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Bei Bedarf können Sie das Skript jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell mit Eingabeaufforderung oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript, bevor Sie fortfahren:

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

Interaktive Konfiguration

Führen Sie eine manuelle Konfiguration mit interaktiven Fragen aus:

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

Automatisierte Konfiguration

Für eine automatisierte Installation geben Sie die vom Setup-Skript benötigten Optionen über Umgebungsvariablen an. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript keine Informationen an.

Unterstützte Umgebungsvariablen sind:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags. Standardmäßig auf N festgelegt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste von vollständig qualifizierten Domänennamen (FQDNs) der Delivery Controller, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. 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, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux Virtual Desktop-Dienste werden nach dem Start der Maschine gestartet. Der Wert ist standardmäßig auf Y festgelegt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux Virtual Desktop-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) automatisch in der System-Firewall für den Linux Virtual Desktop öffnen. Standardmäßig auf Y festgelegt.
- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4 \| 5** – Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird vom installierten und konfigurierten Active Directory-Integrationstool auf dem System bestimmt. Geben Sie die zu verwendende unterstützte 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, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung grafikintensiver Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für den VDI-Desktop-Modus (Einzelsitzung) konfiguriert – (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Gibt an, ob der Computer als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes freigegebenes Desktop-Bereitstellungsmodell konfiguriert werden soll. Setzen Sie diese Variable für HDX 3D Pro-Umgebungen auf Y. Diese Variable ist standardmäßig auf N festgelegt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf eine lokale Site zu beschränken, geben Sie einen DNS-Sitenamen an. Diese Variable ist standardmäßig auf **\<none\>** festgelegt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Beispiel: ad1.mycompany.com:389. Diese Variable ist standardmäßig auf **\<none\>** festgelegt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne festgelegt ist (z. B. DC=mycompany,DC=com). Um die Suchleistung zu verbessern, können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** festgelegt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt keine AD-Gruppenrichtlinie, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss mit der in der AD-Gruppenrichtlinie konfigurierten übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – Der Pfad zur Installation der .NET Core Runtime 3.1 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.

- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Gibt die GNOME- oder MATE-Desktopumgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

> **Hinweis:**
>
> Sie können die Desktopumgebung für einen Ziel-Sitzungsbenutzer auch ändern, indem Sie die folgenden Schritte ausführen:
>
> a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.
> b. Bearbeiten Sie die `.xsession`-Datei, um eine Desktopumgebung basierend auf den Distributionen anzugeben.
>
> **Für MATE-Desktop unter CentOS, Ubuntu und Debian**
>
> MSESSION="$(type -p mate-session)"
>
> \> if ; then
>
> ```
> exec mate-session
> ```
>
> \> fi
>
> ```
> **Für GNOME-Desktop unter CentOS**
>
>
>
>    GSESSION="$(type -p gnome-session)"
> ```
>
> \> if ; then

```
    export GNOME_SHELL_SESSION_MODE=classic
```

\> exec gnome-session --session=gnome-classic

```
    fi

**Für GNOME-Desktop unter Ubuntu und Debian**



    GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    exec gnome-session
```

\> fi

a. Teilen Sie die Dateiberechtigung 700 mit dem Ziel-Sitzungsbenutzer.

- **CTX_XDL_START_SERVICE=Y \| N** – Ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Standardmäßig auf Y festgelegt.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Abhören von 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:

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

```
export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
```

```
export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

Wenn Sie den sudo-Befehl ausführen, geben Sie die Option **-E** ein, um die vorhandenen Umgebungsvariablen an die neue Shell zu übergeben, die erstellt wird. Wir empfehlen, dass Sie aus den vorhergehenden Befehlen eine Shell-Skriptdatei mit **#\!/bin/bash** als erster Zeile erstellen.

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST='list-ddc-fqdns' \

CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \
```

```
CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
```

```
CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Konfigurationsänderungen entfernen

In einigen Szenarien müssen Sie möglicherweise die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernen, ohne das Linux VDA-Paket zu deinstallieren.

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

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

So entfernen Sie Konfigurationsänderungen:

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

Wichtig:

Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank und macht den Linux VDA unbrauchbar.

Konfigurationsprotokolle

Die Skripte **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an, wobei zusätzliche Informationen in die Konfigurationsprotokolldatei **/tmp/xdl.configure.log** geschrieben werden.

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

Schritt 9: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um häufige Konfigurationsprobleme in einer Linux VDA-Umgebung zu überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 10: Linux VDA ausführen

Nachdem Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, können Sie die folgenden Befehle ausführen, um den Linux VDA zu steuern.

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Linux VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

> **Hinweis:**

> Bevor Sie die Dienste `ctxvda` und `ctxhdx` beenden, führen Sie den Befehl `service ctxmonitorservice stop` aus, um den Überwachungsdienst-Daemon zu beenden. Andernfalls startet der Überwachungsdienst-Daemon die von Ihnen beendeten Dienste neu.

> **Linux VDA neu starten:**

So starten Sie die Linux VDA-Dienste neu:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart



sudo /sbin/service ctxvda start
```

Status des Linux VDA überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

Schritt 11: Maschinenkatalog in Citrix Virtual Apps oder Citrix Virtual Desktops™ erstellen

Das Erstellen von Maschinenkatalogen und das Hinzufügen von Linux VDA-Maschinen ähnelt dem traditionellen Windows VDA-Ansatz. Eine detailliertere Beschreibung zum Ausführen dieser Aufgaben finden Sie unter Maschinenkataloge erstellen und Maschinenkataloge verwalten.

Für das Erstellen von Maschinenkatalogen, die Linux VDA-Maschinen enthalten, gibt es einige Einschränkungen, die den Prozess von der Erstellung von Maschinenkatalogen für Windows VDA-Maschinen unterscheiden:

- Wählen Sie für das Betriebssystem Folgendes aus:
  - Die Option **Multi-session OS** für ein Bereitstellungsmodell mit gehosteten Shared Desktops.
  - Die Option **Single-session OS** für ein VDI-Bereitstellungsmodell mit dedizierten Desktops.
- Mischen Sie keine Linux- und Windows-VDA-Maschinen im selben Maschinenkatalog.

> **Hinweis:**

> Frühere Versionen von Citrix Studio unterstützten den Begriff „Linux OS“ nicht. Die Auswahl der Option **Windows Server OS** oder **Server OS** impliziert jedoch ein äquivalentes Bereitstellungsmodell für gehostete Shared Desktops. Die Auswahl der Option **Windows Desktop OS** oder **Desktop OS** impliziert ein Bereitstellungsmodell mit einem Benutzer pro Maschine.

> **Tipp:**

> Wenn Sie eine Maschine aus der Active Directory-Domäne entfernen und wieder hinzufügen, müssen Sie die Maschine erneut aus dem Maschinenkatalog entfernen und hinzufügen.

Schritt 12: Bereitstellungsgruppe in Citrix Virtual Apps™ oder Citrix Virtual Desktops erstellen

Das Erstellen einer Bereitstellungsgruppe und das Hinzufügen von Maschinenkatalogen, die Linux VDA-Maschinen enthalten, ist nahezu identisch mit Windows VDA-Maschinen. Eine detailliertere Beschreibung zum Ausführen dieser Aufgaben finden Sie unter Bereitstellungsgruppen erstellen.

Für das Erstellen von Bereitstellungsgruppen, die Linux VDA-Maschinenkataloge enthalten, gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die von Ihnen ausgewählten AD-Benutzer und -Gruppen ordnungsgemäß für die Anmeldung an den Linux VDA-Maschinen konfiguriert wurden.
- Lassen Sie die Anmeldung nicht authentifizierter (anonymer) Benutzer nicht zu.
- Mischen Sie die Bereitstellungsgruppe nicht mit Maschinenkatalogen, die Windows-Maschinen enthalten.

> **Wichtig:**

> Das Veröffentlichen von Anwendungen wird ab Linux VDA Version 1.4 unterstützt. Der Linux VDA unterstützt jedoch nicht die Bereitstellung von Desktops und Apps auf derselben Maschine.

> Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2106.

Linux Virtual Delivery Agent für SUSE manuell installieren

> **Wichtig:**

> Für Neuinstallationen empfehlen wir die Verwendung von Easy Install für eine schnelle Installation. Easy Install spart Zeit und Arbeitsaufwand und ist weniger fehleranfällig als die in diesem Artikel beschriebene manuelle Installation.

Schritt 1: Vorbereitung der Installation

Schritt 1a: YaST-Tool starten

Das SUSE Linux Enterprise YaST-Tool wird zur Konfiguration aller Aspekte des Betriebssystems verwendet.

So starten Sie das textbasierte YaST-Tool:

```
su -


yast
```

So starten Sie das UI-basierte YaST-Tool:

```
su -


yast2 &
```

Schritt 1b: Netzwerkkonfiguration

Die folgenden Abschnitte enthalten Informationen zur Konfiguration der verschiedenen Netzwerkeinstellungen und -dienste, die vom Linux VDA verwendet werden. Die Netzwerkkonfiguration erfolgt über das YaST-Tool, nicht über andere Methoden wie den Network Manager. Diese Anweisungen basieren auf der Verwendung des UI-basierten YaST-Tools. Das textbasierte YaST-Tool kann verwendet werden, hat aber eine andere Navigationsmethode, die hier nicht dokumentiert ist.

Hostnamen und DNS konfigurieren

1. YaST-Netzwerkeinstellungen öffnen.
2. Nur SLED 12: Wählen Sie auf der Registerkarte **Globale Optionen** die **Netzwerkeinrichtungsmethode Wicked Service**.
3. Öffnen Sie die Registerkarte **Hostname/DNS**.
4. Deaktivieren Sie **Hostnamen über DHCP ändern**.
5. Aktivieren Sie **Hostnamen der Loopback-IP zuweisen**.
6. Bearbeiten Sie Folgendes, um Ihre Netzwerkkonfiguration widerzuspiegeln:
    - Hostname – Fügen Sie den DNS-Hostnamen des Computers hinzu.
    - Domänenname – Fügen Sie den DNS-Domänennamen des Computers hinzu.
    - Nameserver – Fügen Sie die IP-Adresse des DNS-Servers hinzu. Dies ist in der Regel die IP-Adresse des AD-Domänencontrollers.
    - Domänensuchliste – Fügen Sie den DNS-Domänennamen hinzu.

> **Hinweis:**

> Der Linux VDA unterstützt derzeit keine NetBIOS-Namenskürzung. Daher darf der Hostname 15 Zeichen nicht überschreiten. **Tipp:**

> Verwenden Sie nur die Zeichen a–z, A–Z, 0–9 und Bindestrich (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Beginnen Sie einen Hostnamen nicht mit einer Zahl und beenden Sie ihn nicht mit einem Bindestrich. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Multicast-DNS deaktivieren

Nur unter SLED sind die Standardeinstellungen für Multicast-DNS (mDNS) aktiviert, was zu inkonsistenten Namensauflösungsergebnissen führen kann. mDNS ist unter SLES standardmäßig nicht aktiviert, daher ist keine Aktion erforderlich.

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

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

In:

`hosts: files dns`

Hostnamen überprüfen

Überprüfen Sie, ob der Hostname korrekt eingestellt ist:

```
hostname
```

Dieser Befehl gibt nur den Hostnamen des Computers und nicht seinen vollqualifizierten Domänennamen (FQDN) zurück.

Überprüfen Sie, ob der FQDN korrekt eingestellt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN des Computers zurück.

Überprüfen der Namensauflösung und Dienstverfügbarkeit

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

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

Wenn Sie den FQDN nicht auflösen oder keine der Maschinen anpingen können, überprüfen Sie die Schritte, bevor Sie fortfahren.

Schritt 1c: Konfigurieren des NTP-Diensts

Es ist entscheidend, eine genaue Zeitsynchronisierung zwischen den VDAs, Delivery Controllern und Domänencontrollern aufrechtzuerhalten. Das Hosten des Linux VDA als virtuelle Maschine kann zu Problemen mit der Zeitverschiebung führen. Aus diesem Grund wird die Zeitverwaltung über einen Remote-NTP-Dienst bevorzugt. Möglicherweise sind einige Änderungen an den Standard-NTP-Einstellungen erforderlich:

1. Öffnen Sie die YaST NTP-Konfiguration und wählen Sie die Registerkarte **Allgemeine Einstellungen**.
2. Aktivieren Sie im Abschnitt „NTP-Daemon starten“ die Option **Jetzt und beim Start**.
3. Wählen Sie, falls vorhanden, das Element **Undisciplined Local Clock (LOCAL)** aus und klicken Sie auf **Löschen**.
4. Fügen Sie einen Eintrag für einen NTP-Server hinzu, indem Sie auf **Hinzufügen** klicken.
5. Wählen Sie den **Servertyp** aus und klicken Sie auf **Weiter**.
6. Geben Sie den DNS-Namen des NTP-Servers in das Feld „Adresse“ ein. Dieser Dienst wird normalerweise auf dem Active Directory-Domänencontroller gehostet.
7. Lassen Sie das Feld „Optionen“ unverändert.
8. Klicken Sie auf **Testen**, um zu überprüfen, ob der NTP-Dienst erreichbar ist.
9. Klicken Sie in den Fenstern auf **OK**, um die Änderungen zu speichern.

> **Hinweis:**
>
> Bei SLES 12-Implementierungen kann der NTP-Daemon aufgrund eines bekannten SUSE-Problems mit AppArmor-Richtlinien nicht gestartet werden. Befolgen Sie die Lösung für weitere Informationen.

Schritt 1d: Linux VDA-abhängige Pakete installieren

Die Linux VDA-Software für SUSE Linux Enterprise hängt von den folgenden Paketen ab:

- Postgresql10-server 10.12 oder höher
- OpenJDK 11
- OpenMotif Runtime Environment 2.3.1 oder höher
- Cups 1.6.0 oder höher
- Foomatic-Filter 3.0.0 oder höher

- ImageMagick 6.8 oder höher

Repositorys hinzufügen

Einige erforderliche Pakete, wie PostgreSQL und ImageMagick, erhalten Sie über das SUSE Linux Enterprise Software Development Kit (SDK). Um die Pakete zu erhalten, fügen Sie das SDK-Repository mit YaST hinzu oder laden Sie die SDK-Image-Datei herunter und mounten Sie sie dann lokal mit den folgenden Befehlen:

```
sudo mkdir -p /mnt/sdk



sudo mount -t iso9660 path-to-iso/SLE-12-SP5-SDK-DVD-x86_64-GM-DVD1.iso /
mnt/sdk



sudo zypper ar -f /mnt/sdk sdk
```

Kerberos-Client installieren

Installieren Sie den Kerberos-Client für die gegenseitige Authentifizierung zwischen dem Linux VDA und den Delivery Controllern:

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

Die Konfiguration des Kerberos-Clients hängt davon ab, welcher Active Directory-Integrationsansatz verwendet wird. Siehe die folgende Beschreibung.

OpenJDK 11 installieren

Für den Linux VDA ist OpenJDK 11 erforderlich.

Um OpenJDK 11 zu installieren, führen Sie den folgenden Befehl aus:

```
sudo zypper install java-11-openjdk
```

PostgreSQL installieren

Installieren Sie unter SLED/SLES 12 die Pakete:

```
sudo zypper install postgresql-init


sudo zypper install postgresql10-server


sudo zypper install postgresql-jdbc
```

Nach der Installation sind Schritte erforderlich, um den Datenbankdienst zu initialisieren und sicherzustellen, dass PostgreSQL beim Start des Computers gestartet wird:

```
sudo systemctl enable postgresql


sudo systemctl restart postgresql
```

Datenbankdateien befinden sich unter /var/lib/pgsql/data.

Repositorys entfernen

Nachdem die abhängigen Pakete installiert wurden, führen Sie die folgenden Befehle aus, um das zuvor eingerichtete SDK-Repository und die gemounteten Medien zu entfernen:

```
sudo zypper rr sdk


sudo umount /mnt/sdk


sudo rmdir /mnt/sdk
```

Schritt 2: Linux-VM für Hypervisor vorbereiten

Einige Änderungen sind erforderlich, wenn der Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausgeführt wird. Nehmen Sie die folgenden Änderungen entsprechend

der verwendeten Hypervisor-Plattform vor. Es sind keine Änderungen erforderlich, wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen.

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

Wenn die Citrix Hypervisor-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme auf, da NTP und Citrix Hypervisor beide versuchen, die Systemuhr zu verwalten. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, muss die Systemuhr in jedem Linux-Gast mit NTP synchronisiert werden. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen können Sie, wenn Sie einen paravirtualisierten Linux-Kernel mit installierten Citrix VM Tools ausführen, innerhalb der Linux-VM überprüfen, ob die Citrix Hypervisor-Zeitsynchronisierungsfunktion vorhanden und aktiviert ist:

```
su -



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

Dieser Befehl gibt 0 oder 1 zurück:

- 0 – Die Zeitsynchronisierungsfunktion ist aktiviert und muss deaktiviert werden.
- 1 – Die Zeitsynchronisierungsfunktion ist deaktiviert, und es sind keine weiteren Maßnahmen erforderlich.

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

Falls aktiviert, deaktivieren Sie die Zeitsynchronisierungsfunktion, indem Sie **1** in die Datei schreiben:

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

Um diese Änderung dauerhaft und nach einem Neustart beizubehalten, bearbeiten Sie die Datei **/etc/sysctl.conf** und fügen Sie die Zeile hinzu:

`xen.independent_wallclock = 1`

Um diese Änderungen zu überprüfen, starten Sie das System neu:

```
reboot
```

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

```
su -



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

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

Linux-VMs mit installierten Hyper-V Linux Integration Services können die Hyper-V-Zeitsynchronisierungsfunktion verwenden, um die Zeit des Hostbetriebssystems zu nutzen. Um sicherzustellen, dass die Systemuhr genau bleibt, aktivieren Sie diese Funktion zusammen mit den NTP-Diensten.

Vom Verwaltungsbetriebssystem aus:

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:

Dieser Ansatz unterscheidet sich von VMware und Citrix Hypervisor, wo die Host-Zeitsynchronisierung deaktiviert ist, um Konflikte mit NTP zu vermeiden. Die Hyper-V-Zeitsynchronisierung kann mit der NTP-Zeitsynchronisierung koexistieren und diese ergänzen.

Zeitsynchronisierung auf ESX und ESXi beheben

Wenn die VMware-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme auf, da NTP und der Hypervisor beide versuchen, die Systemuhr zu synchronisieren. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist,

synchronisieren Sie die Systemuhr in jedem Linux-Gast mit NTP. In diesem Fall muss die Host-Zeitsynchronisierung 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 **Eigenschaften der virtuellen Maschine** die Registerkarte **Optionen**.
4. Wählen Sie **VMware Tools** aus.
5. Deaktivieren Sie im Feld **Erweitert** die Option **Gastzeit mit Host synchronisieren**.

Schritt 3: Hinzufügen der Linux-VM (virtuelle Maschine) zur Windows-Domäne

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

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

Befolgen Sie die Anweisungen entsprechend der von Ihnen gewählten Methode.

> **Hinweis:**

> Sitzungsstarts können fehlschlagen, wenn derselbe Benutzername für das lokale Konto im Linux VDA und das Konto in AD verwendet wird.

Samba Winbind

Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

1. Öffnen Sie YaST Windows-Domänenmitgliedschaft.

2. Nehmen Sie die folgenden Änderungen vor:
    - Legen Sie **Domäne oder Arbeitsgruppe** auf den Namen Ihrer Active Directory-Domäne oder die IP-Adresse des Domänencontrollers fest. Stellen Sie sicher, dass der Domänenname in Großbuchstaben geschrieben ist.
    - Aktivieren Sie **SMB-Informationen auch für Linux-Authentifizierung verwenden**.
    - Aktivieren Sie **Home-Verzeichnis bei Anmeldung erstellen**.
    - Aktivieren Sie **Single Sign-on für SSH**.
    - Stellen Sie sicher, dass **Offline-Authentifizierung** nicht aktiviert ist. Diese Option ist nicht mit dem Linux VDA kompatibel.
3. Klicken Sie auf **OK**. Wenn Sie aufgefordert werden, Pakete zu installieren, klicken Sie auf **Installieren**.
4. Wenn ein Domänencontroller gefunden wird, werden Sie gefragt, ob Sie der Domäne beitreten möchten. Klicken Sie auf **Ja**.
5. Geben Sie bei Aufforderung die Anmeldeinformationen eines Domänenbenutzers mit Berechtigung zum Hinzufügen von Computern zur Domäne ein und klicken Sie auf **OK**.
6. Eine Erfolgsmeldung wird angezeigt.
7. Wenn Sie aufgefordert werden, Samba- und krb5-Pakete zu installieren, klicken Sie auf **Installieren**.

YaST hat möglicherweise darauf hingewiesen, dass diese Änderungen einen Neustart einiger Dienste oder der Maschine erfordern. Wir empfehlen Ihnen, die Maschine neu zu starten:

```
su -



reboot
```

Nur SUSE 12: Kerberos-Anmeldeinformations-Cache-Namen patchen

SUSE 12 hat die Standard-Spezifikation für den Kerberos-Anmeldeinformations-Cache-Namen von der üblichen **FILE:/tmp/krb5cc_%{uid}** in **DIR:/run/user/%{uid}/krb5cc** geändert. Diese neue DIR-Caching-Methode ist nicht mit dem Linux VDA kompatibel und muss manuell geändert werden. Bearbeiten Sie als Root-Benutzer die Datei **/etc/krb5.conf** und fügen Sie die folgende Einstellung unter dem Abschnitt **\[libdefaults\]** hinzu, falls sie nicht vorhanden ist:

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben.

Führen Sie den Samba-Befehl **net ads** aus, um zu überprüfen, ob die Maschine einer Domäne beigetreten ist:

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

Kerberos-Konfiguration überprüfen

Um sicherzustellen, dass Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, überprüfen Sie, ob die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist –ke
```

Dieser Befehl zeigt die Liste der verfügbaren Schlüssel für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten an. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Die Maschinen- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Maschinenkonto mit folgendem Befehl zwischengespeichert wurde:

```
sudo klist
```

Überprüfen Sie die Details des Maschinenkontos mit:

```
sudo net ads status
```

Benutzerauthentifizierung überprüfen

Verwenden Sie das `wbinfo` Tool, um zu überprüfen, ob Domänenbenutzer sich bei der Domäne authentifizieren können:

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

Die hier angegebene Domäne ist der AD-Domänenname, nicht der Kerberos-Realm-Name. Für die Bash-Shell muss der Backslash (\\) mit einem weiteren Backslash maskiert werden. Dieser Befehl gibt eine Meldung zurück, die den Erfolg oder Misserfolg anzeigt.

Um zu überprüfen, ob das Winbind PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username

id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die UID erstellt wurde, die vom Befehl **id -u** zurückgegeben wird:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

Ein ähnlicher Test kann durchgeführt werden, indem 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-Authentifizierungsdienst

Quest auf Domänencontroller konfigurieren

Gehen Sie davon aus, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und Ihnen administrative Berechtigungen zum Erstellen von Computerobjekten in Active Directory erteilt wurden.

Domänenbenutzern die Anmeldung an Linux VDA-Maschinen ermöglichen

Um Domänenbenutzern das Herstellen von HDX™-Sitzungen auf einer Linux VDA-Maschine zu ermöglichen:

1. In der Verwaltungskonsole „Active Directory-Benutzer und -Computer“ öffnen Sie die Active Directory-Benutzereigenschaften für dieses Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix-Konto** aus.
3. Aktivieren Sie **Unix-aktiviert**.
4. Legen Sie die **primäre GID-Nummer** auf die Gruppen-ID einer tatsächlichen Domänenbenutzergruppe fest.

> **Hinweis:**
>
> Diese Anweisungen sind gleichwertig für die Einrichtung von Domänenbenutzern zur Anmeldung über die Konsole, RDP, SSH oder jedes andere Remote-Protokoll.

Quest auf Linux-VDA konfigurieren

VAS-DAEMON KONFIGURIEREN

Die automatische Verlängerung von Kerberos-Tickets muss aktiviert und getrennt werden. Die Authentifizierung (Offline-Anmeldung) muss deaktiviert sein:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400
```

```
sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Dieser Befehl setzt das Verlängerungsintervall auf neun Stunden (32.400 Sekunden), was eine Stunde weniger ist als die standardmäßige Ticket-Lebensdauer von 10 Stunden. Setzen Sie diesen Parameter auf Systemen mit einer kürzeren Ticket-Lebensdauer auf einen niedrigeren Wert.

PAM UND NSS KONFIGURIEREN

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

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



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

Windows-Domäne beitreten

Fügen Sie die Linux-Maschine mit dem Quest-Befehl `vastool` der Active Directory-Domäne hinzu:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

Der **Benutzer** ist ein beliebiger Domänenbenutzer, der über Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne verfügt. Der **Domänenname** ist der DNS-Name der Domäne, z. B. example.com.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine mit Quest verbundene Linux-Maschine in der Domäne ist:

```
sudo /opt/quest/bin/vastool info domain
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl den Domänennamen zurück. Wenn die Maschine keiner Domäne beigetreten ist, wird der folgende Fehler 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 zu überprüfen, ob Quest Domänenbenutzer über PAM authentifizieren kann, melden Sie sich mit einem Domänenbenutzerkonto, das noch nicht verwendet wurde, am Linux-VDA an.

```
ssh localhost -l domain\\username

id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die von dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

```
exit
```

Ein ähnlicher Test kann durchgeführt werden, indem Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit (/de-de/linux-virtual-delivery-agent/2107/installation-overview/suse.html#step-6-install-the-linux-vda) fort.

Centrify DirectControl

Windows-Domäne beitreten

Nach der Installation des Centrify DirectControl Agent fügen Sie die Linux-Maschine der Active Directory-Domäne mit dem Centrify-Befehl **adjoin** hinzu:

```
su –

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

Der **Benutzer** ist ein beliebiger Active Directory-Domänenbenutzer, der über Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne verfügt. Der **Domänenname** ist der Name der Domäne, der die Linux-Maschine beitreten soll.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine mit Centrify verbundene Linux-Maschine in der Domäne ist:

```
su –


adinfo
```

Überprüfen Sie, ob der Wert **Joined to domain** gültig ist und der **CentrifyDC-Modus connected** zurückgibt. Wenn der Modus im Startzustand hängen bleibt, hat der Centrify-Client Probleme mit der Serververbindung oder Authentifizierung.

Umfassendere System- und Diagnoseinformationen sind verfügbar unter:

```
adinfo --sysinfo all


adinfo –diag
```

Testen Sie die Konnektivität zu den verschiedenen Active Directory- und Kerberos-Diensten.

```
adinfo --test
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit (/de-de/linux-virtual-delivery-agent/2107/installation-overview/suse.html#step-6-install-the-linux-vda) fort.

SSSD

Wenn Sie SSSD unter SUSE verwenden, befolgen Sie die Anweisungen in diesem Abschnitt. Dieser Abschnitt enthält Anweisungen zum Beitreten einer Linux-VDA-Maschine zu einer Windows-Domäne und bietet Anleitungen zur Konfiguration der Kerberos-Authentifizierung.

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

1. Der Domäne beitreten und Host-Keytabs erstellen
2. PAM für SSSD konfigurieren
3. SSSD einrichten
4. SSSD aktivieren
5. Domänenmitgliedschaft überprüfen
6. Kerberos-Konfiguration überprüfen
7. Benutzerauthentifizierung überprüfen

Der Domäne beitreten und Host-Keytab erstellen

SSSD bietet keine Active Directory-Clientfunktionen zum Beitreten der Domäne und zur Verwaltung der System-Keytab-Datei. Sie können stattdessen den `Samba`-Ansatz verwenden. Führen Sie die folgenden Schritte aus, bevor Sie SSSD konfigurieren.

1. Den Name Service Cache Daemon (NSCD)-Dienst beenden und deaktivieren.

```
sudo systemctl stop nscd



sudo systemctl disable nscd
```

2. Die erforderlichen Pakete installieren oder aktualisieren:

```
sudo zypper install krb5-client



sudo zypper install samba-client
```

3. Bearbeiten Sie die Datei /etc/krb5.conf als Root-Benutzer, um dem Dienstprogramm `kinit` die Kommunikation mit der Zieldomäne zu ermöglichen. Fügen Sie die folgenden Einträge unter den Abschnitten , und hinzu:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Einzeldomänen-, Einzelforst-Modell vorgesehen.

```
[libdefaults]

    dns_canonicalize_hostname = false

    rdns = false

    default_realm = REALM

    forwardable = true

[realms]

    REALM = {

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

```
        default_domain = realm


        admin_server =     fqdn-of-domain-controller
    }
[domain_realm]


    .realm = REALM


    realm = REALM
```

realm ist der Kerberos-Realm-Name, z. B. example.com. **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM. **fqdn-of-domain-controller** ist der FQDN des Domänencontrollers.

4. Bearbeiten Sie /etc/samba/smb.conf als Root-Benutzer, um dem Dienstprogramm **net** die Kommunikation mit der Zieldomäne zu ermöglichen. Fügen Sie die folgenden Einträge unter dem Abschnitt hinzu:

```
[global]
    workgroup = domain


    realm = REALM


    security = ADS


    kerberos method = secrets and keytab
```

```
    client signing = yes


    client use spnego = yes
```

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

5. Ändern Sie die Einträge **passwd** und **group** in der Datei /etc/nsswitch.conf, um SSSD beim Auflösen von Benutzern und Gruppen zu referenzieren.

```
passwd: compat sss


group: compat sss
```

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

```
sudo realm join REALM -U user
```

user ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Domäne besitzt.

PAM für SSSD konfigurieren

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

```
sudo zypper install sssd sssd-ad
```

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

```
sudo pam-config --add  --sss

sudo pam-config --add --mkhomedir
```

SSSD einrichten

1. Bearbeiten Sie /etc/sssd/sssd.conf als Root-Benutzer, um dem SSSD-Daemon die Kommunikation mit der Zieldomäne zu ermöglichen. Eine Beispielkonfiguration für sssd.conf (zusätzliche Optionen können bei Bedarf hinzugefügt werden):

```
[sssd]

    config_file_version = 2

    services = nss,pam

    domains = domain-dns-name



[domain/domain-dns-name]

    id_provider = ad

    auth_provider = ad

    access_provider = ad

    ad_domain = domain-dns-name

    ad_server = fqdn-of-domain-controller

    ldap_id_mapping = true

    ldap_schema = ad



# Kerberos settings

    krb5_ccachedir = /tmp
```

```
    krb5_ccname_template = FILE:%d/krb5cc_%U



# Comment out if the users have the shell and home dir set on the AD
side



    fallback_homedir = /home/%d/%u

    default_shell = /bin/bash



# Uncomment and adjust if the default principal SHORTNAME$@REALM is not
available



# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM



    ad_gpo_access_control = permissive
```

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

> **Hinweis:**
>
> **ldap_id_mapping** ist auf true gesetzt, damit SSSD selbst die Zuordnung von Windows-SIDs zu Unix-UIDs übernimmt. Andernfalls muss das Active Directory in der Lage sein, POSIX-Erweiterungen bereitzustellen. **ad_gpo_access_control** ist auf **permissive** gesetzt, um einen Fehler bei der ungültigen Anmeldung für Linux-Sitzungen zu verhindern. Siehe die Manpages für sssd.conf und sssd-ad.

2. Legen Sie den Dateibesitz und die Berechtigungen für sssd.conf fest:

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

SSSD aktivieren

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

```
sudo systemctl enable sssd

sudo systemctl start sssd
```

Domänenmitgliedschaft überprüfen

1. Führen Sie den Befehl net ads von Samba aus, um zu überprüfen, ob der Computer einer Domäne beigetreten ist:

   ```
   sudo net ads testjoin
   ```

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

   ```
   sudo net ads info
   ```

Kerberos-Konfiguration überprüfen

Um zu überprüfen, ob Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, vergewissern Sie sich, dass die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der verfügbaren Schlüssel für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten an. Führen Sie den Kerberos-Befehl `kinit` aus, um den Computer mit diesen Schlüsseln beim Domänencontroller zu authentifizieren:

```
sudo kinit –k MACHINE\$@REALM
```

Die Computer- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen (**$**) muss mit einem Backslash (****) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname

vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Computerkonto zwischengespeichert wurde, indem Sie Folgendes verwenden:

```
sudo klist
```

Benutzerauthentifizierung überprüfen

SSSD bietet kein Befehlszeilentool zum direkten Testen der Authentifizierung mit dem Daemon, dies kann nur über PAM erfolgen.

Um zu überprüfen, ob das SSSD PAM-Modul korrekt konfiguriert ist, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u



klist



exit
```

Überprüfen Sie, ob die vom Befehl `klist` zurückgegebenen Kerberos-Tickets für diesen Benutzer korrekt sind und nicht abgelaufen sind.

Überprüfen Sie als Root-Benutzer, ob eine entsprechende Ticket-Cache-Datei für die vom vorherigen Befehl `id -u` zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Ein ähnlicher Test kann durch direktes Anmelden an der Gnome- oder KDE-Konsole durchgeführt werden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

Herunterladen des erforderlichen PBIS-Pakets

Zum Beispiel:

```
wget https://github.com/BeyondTrust/pbis-open/releases/download/8.8.0/
pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Das PBIS-Installationsskript ausführbar machen

Zum Beispiel:

```
chmod +x pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Ausführen des PBIS-Installationsskripts

Zum Beispiel:

```
sh pbis-open-8.8.0.506.linux.x86_64.rpm.sh
```

Einer Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
/opt/pbis/bin/domainjoin-cli join domain-name user
```

Der **Benutzer** ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne besitzt. Der **Domänenname** ist der DNS-Name der Domäne, z. B. example.com.

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine PBIS-verbundene Linux-Maschine in der Domäne ist:

```
/opt/pbis/bin/domainjoin-cli query
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl Informationen über die aktuell beigetretene AD-Domäne und OU zurück. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen

Um zu überprüfen, ob PBIS Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\user



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die UID erstellt wurde, die vom Befehl **id -u** zurückgegeben wird:

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Schritt 4: Installieren Sie .NET Core Runtime 3.1 als Voraussetzung

Bevor Sie den Linux VDA installieren, installieren Sie .NET Core Runtime 3.1 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

Nach der Installation von .NET Core Runtime 3.1 führen Sie den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Basierend auf der Befehlsausgabe legen Sie den Binärpfad der .NET Core-Laufzeit fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Laden Sie das Linux VDA-Paket herunter

Gehen Sie zur Downloadseite von Citrix Virtual Apps and Desktops™. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das Linux VDA-Paket herunterzuladen, das Ihrer Linux-Distribution entspricht.

Schritt 6: Installieren des Linux VDA

Schritt 6a: Deinstallieren der alten Version

Wenn Sie eine frühere Version als die beiden vorherigen und eine LTSR-Version installiert haben, deinstallieren Sie diese, bevor Sie die neue Version installieren.

1. Beenden Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

> **Hinweis:**
>
> Bevor Sie die Dienste `ctxvda` und `ctxhdx` beenden, führen Sie den Befehl `service ctxmonitorservice stop` aus, um den Überwachungsdienst-Daemon zu stoppen. Andernfalls startet der Überwachungsdienst-Daemon die von Ihnen gestoppten Dienste neu.

2. Deinstallieren Sie das Paket:

```
sudo rpm -e XenDesktopVDA
```

> **Wichtig:**
>
> Ein Upgrade von den letzten beiden Versionen wird unterstützt.

> **Hinweis:**

> Installationskomponenten befinden sich in **/opt/Citrix/VDA/**.

> Um einen Befehl auszuführen, ist der vollständige Pfad erforderlich; alternativ können Sie **/opt/Citrix/VDA/sbin** und **/opt/Citrix/VDA/bin** zum Systempfad hinzufügen.

Schritt 6b: Installieren des Linux VDA

Installieren Sie die Linux VDA-Software mit Zypper:

Für SUSE 12:

```
sudo zypper install XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Installieren Sie die Linux VDA-Software mit dem RPM-Paketmanager. Lösen Sie zuvor die folgenden Abhängigkeiten auf:

Für SUSE 12:

```
sudo rpm -i XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Schritt 6c: Aktualisieren des Linux VDA (optional)

Sie können eine vorhandene Installation von den beiden vorherigen Versionen und von einer LTSR-Version aktualisieren.

> **Hinweis:**

> Das Aktualisieren einer vorhandenen Installation überschreibt die Konfigurationsdateien unter /etc/xdl. Sichern Sie die Dateien, bevor Sie ein Upgrade durchführen.

> **Für SUSE 12:**

```
sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

RPM-Abhängigkeitsliste für SUSE 12:

```
mozilla-nss-tools >= 3.47.1

postgresql-server >= 10.12

postgresql-jdbc >= 9.2

java-11-openjdk >= 11

ImageMagick >= 6.8

dbus-1 >= 1.8.8

dbus-1-x11 >= 1.8.8

libXpm4 >= 3.5.11

libXrandr2 >= 1.4.2

libXtst6 >= 1.2.2

motif >= 2.3
```

```
pam >= 1.1.8

bash >= 4.2

findutils >= 4.5

gawk >= 4.1

sed >= 4.2

cups >= 1.6.0

cups-filters-foomatic-rip >= 1.0.0

openldap2 >= 2.4

cyrus-sasl >= 2.1

cyrus-sasl-gssapi >= 2.1

libxml2 >= 2.9
```

```
libmspack0 >= 0.4

python-requests >= 2.8.1

rpmlib(PayloadFilesHavePrefix) <= 4.0-1

rpmlib(CompressedFileNames) <= 3.0.4-1

rpmlib(PayloadIsLzma) <= 4.4.6-1

libtcmalloc4 >= 2.5

libcap-progs >= 2.22

xorg-x11-server >= 7.6_1.18.3-76.15

ibus >= 1.5

xorg- x11-server = 7.6_1.19.6

xorg-x11 = 7.6_1
```

```
postgresql10-server >= 10.12

libgtk-2_0-0 >= 2.24

libgthread-2_0-0 >= 2.48

pulseaudio-utils >= 5.0

lsb-release >= 2.0
```

Wichtig:

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

Schritt 7: Konfigurieren des Linux VDA

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Bevor Änderungen vorgenommen werden, überprüft das Skript die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Bei Bedarf können Sie das Skript jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell mit Eingabeaufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript, bevor Sie fortfahren:

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

Konfiguration mit Eingabeaufforderung

Führen Sie eine manuelle Konfiguration mit Eingabeaufforderungen durch:

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

Automatisierte Konfiguration

Für eine automatisierte Installation geben Sie die vom Setup-Skript benötigten Optionen über Umgebungsvariablen an. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript keine Informationen an.

Unterstützte Umgebungsvariablen umfassen:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens über einen DNS-CNAME-Eintrag. Standardmäßig auf N gesetzt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA benötigt eine durch Leerzeichen getrennte Liste von FQDNs (Fully Qualified Domain Names) der Delivery Controller, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. 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, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux Virtual Desktop-Dienste werden nach dem Start der Maschine gestartet. Der Wert ist standardmäßig auf Y gesetzt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux Virtual Desktop-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) automatisch in der System-Firewall für den Linux Virtual Desktop öffnen. Standardmäßig auf Y gesetzt.
- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4** – Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird vom installierten und konfigurierten Active Directory-Integrationstool auf dem System bestimmt. Geben Sie die zu verwendende unterstützte Active Directory-Integrationsmethode an:
  - 1 – Samba Winbind
  - 2 – Quest Authentication Service
  - 3 – Centrify DirectControl
  - 4 – SSSD

- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung von grafikintensiven Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für den VDI-Desktop-Modus (Einzelsitzung) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Gibt an, ob die Maschine als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie diese Variable auf Y. Diese Variable ist standardmäßig auf N gesetzt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf einen lokalen Standort zu beschränken, geben Sie einen DNS-Standortnamen an. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Beispiel: ad1.mycompany.com:389. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne gesetzt ist (z. B. DC=mycompany,DC=com). Um die Suchleistung zu verbessern, können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – Der Pfad zur Installation der .NET Core Runtime 3.1 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Gibt die GNOME- oder MATE-Desktopumgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

Hinweis:

Sie können die Desktopumgebung für einen Ziel-Sitzungsbenutzer auch ändern, indem Sie die folgenden Schritte ausführen:

a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.
b. Bearbeiten Sie die `.xsession`-Datei, um eine Desktopumgebung basierend auf den Distributionen anzugeben.

Für MATE-Desktop unter CentOS, Ubuntu und Debian:

```
MSESSION="$(type -p mate-session)"

if [ -n "$MSESSION" ]; then

  exec mate-session

fi
```

Für GNOME-Desktop unter CentOS:

```
GSESSION="$(type -p gnome-session)"

if [ -n "$GSESSION" ]; then

    export GNOME_SHELL_SESSION_MODE=classic

    exec gnome-session --session=gnome-classic

fi
```

Für GNOME-Desktop unter Ubuntu und Debian:

```
GSESSION="$(type -p gnome-session)"

if [ -n "$GSESSION" ]; then

    exec gnome-session

fi
```

a. Teilen Sie die Dateiberechtigung 700 mit dem Ziel-Sitzungsbenutzer.

- **CTX_XDL_START_SERVICE=Y \| N** – Ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Standardmäßig auf Y gesetzt.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Abhören von 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:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N


export CTX_XDL_DDC_LIST='list-ddc-fqdns'


export CTX_XDL_VDA_PORT=port-number


export CTX_XDL_REGISTER_SERVICE=Y|N


export CTX_XDL_ADD_FIREWALL_RULES=Y|N
```

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

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

export CTX_XDL_FAS_LIST=‘list-fas-servers’ | '<none>'

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

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number
```

```
export CTX_XDL_START_SERVICE=Y|N


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

Wenn Sie den sudo-Befehl ausführen, geben Sie die Option **-E** ein, um die vorhandenen Umgebungsvariablen an die neue Shell zu übergeben, die erstellt wird. Wir empfehlen, dass Sie aus den vorhergehenden Befehlen eine Shell-Skriptdatei mit **#\!/bin/bash** als erster Zeile erstellen.

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \


CTX_XDL_REGISTER_SERVICE=Y|N \


CTX_XDL_ADD_FIREWALL_RULES=Y|N \


CTX_XDL_AD_INTEGRATION=1|2|3|4 \


CTX_XDL_HDX_3D_PRO=Y|N \


CTX_XDL_VDI_MODE=Y|N \
```

```
CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=‘list-ldap-servers’ \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST=‘list-fas-servers’ \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Konfigurationsänderungen entfernen

In einigen Szenarien müssen Sie möglicherweise die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernen, ohne das Linux VDA-Paket zu deinstallieren.

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

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

So entfernen Sie Konfigurationsänderungen:

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

Wichtig:

Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank und macht den Linux VDA unbrauchbar.

Konfigurationsprotokolle

Die Skripte **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an, wobei zusätzliche Informationen in eine Konfigurationsprotokolldatei geschrieben werden:

`/tmp/xdl.configure.log`

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

Schritt 8: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um häufige Konfigurationsprobleme in einer Linux VDA-Umgebung zu überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 9: Linux VDA ausführen

Nachdem Sie den Linux VDA mithilfe des Skripts **ctxsetup.sh** konfiguriert haben, können Sie die folgenden Befehle ausführen, um den Linux VDA zu steuern.

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Linux VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

Hinweis:

Bevor Sie die Dienste `ctxvda` und `ctxhdx` beenden, führen Sie den Befehl `service ctxmonitorservice stop` aus, um den Überwachungsdienst-Daemon zu beenden. Andernfalls startet der Überwachungsdienst-Daemon die von Ihnen beendeten Dienste neu.

Linux VDA neu starten:

So starten Sie die Linux VDA-Dienste neu:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart



sudo /sbin/service ctxvda start
```

Linux VDA-Status überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

Schritt 10: Maschinenkatalog in Citrix Virtual Apps oder Citrix Virtual Desktops™ erstellen

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt dem traditionellen Windows VDA-Ansatz. Eine detailliertere Beschreibung zur Ausführung dieser Aufgaben finden Sie unter Maschinenkataloge erstellen und Maschinenkataloge verwalten.

Für die Erstellung von Maschinenkatalogen, die Linux-VDA-Maschinen enthalten, gibt es einige Einschränkungen, die den Prozess von der Erstellung von Maschinenkatalogen für Windows-VDA-Maschinen unterscheiden:

- Wählen Sie für das Betriebssystem:
  - Die Option **Multi-session OS** für ein Bereitstellungsmodell mit gehosteten Shared Desktops.
  - Die Option **Single-session OS** für ein VDI-Bereitstellungsmodell mit dedizierten Desktops.
- Mischen Sie keine Linux- und Windows-VDA-Maschinen im selben Maschinenkatalog.

Hinweis:

Frühere Versionen von Citrix Studio unterstützten den Begriff „Linux-Betriebssystem“ nicht. Die Auswahl der Option **Windows Server OS** oder **Server OS** impliziert jedoch ein äquivalentes Bereitstellungsmodell für gehostete Shared Desktops. Die Auswahl der Option **Windows Desktop OS** oder **Desktop OS** impliziert ein Bereitstellungsmodell mit einem einzelnen Benutzer pro Maschine.

Tipp:

Wenn Sie eine Maschine aus der Active Directory-Domäne entfernen und wieder hinzufügen, müssen Sie die Maschine erneut aus dem Maschinenkatalog entfernen und hinzufügen.

Schritt 11: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps™ oder Citrix Virtual Desktops

Der Prozess zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen, die Linux-VDA-Maschinen enthalten, ist nahezu identisch mit dem für Windows-VDA-Maschinen. Eine detailliertere Beschreibung zum Ausführen dieser Aufgaben finden Sie unter Bereitstellungsgruppen erstellen.

Für die Erstellung von Bereitstellungsgruppen, die Linux-VDA-Maschinenkataloge enthalten, gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die von Ihnen ausgewählten AD-Benutzer und -Gruppen ordnungsgemäß für die Anmeldung an den Linux-VDA-Maschinen konfiguriert wurden.
- Lassen Sie die Anmeldung von nicht authentifizierten (anonymen) Benutzern nicht zu.
- Mischen Sie die Bereitstellungsgruppe nicht mit Maschinenkatalogen, die Windows-Maschinen enthalten.

> **Wichtig:**

> Das Veröffentlichen von Anwendungen wird ab Linux VDA Version 1.4 unterstützt. Der Linux VDA unterstützt jedoch nicht die Bereitstellung von Desktops und Anwendungen auf derselben Maschine.

> Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2106.

Manuelle Installation des Linux Virtual Delivery Agent für Ubuntu

> **Wichtig:**

> Für Neuinstallationen empfehlen wir Ihnen, Easy Install für eine schnelle Installation zu verwenden. Easy Install spart Zeit und Arbeitsaufwand und ist weniger fehleranfällig als die in diesem Artikel beschriebene manuelle Installation.

Schritt 1: Ubuntu für die VDA-Installation vorbereiten

Schritt 1a: Netzwerkkonfiguration überprüfen

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

Wenn Sie einen Ubuntu 18.04 Live Server verwenden, nehmen Sie die folgende Änderung in der Konfigurationsdatei **/etc/cloud/cloud.cfg** vor, bevor Sie den Hostnamen festlegen:

```
preserve_hostname: true
```

Schritt 1b: Hostnamen festlegen

Um sicherzustellen, dass der Hostname des Computers korrekt gemeldet wird, ändern Sie die Datei **/etc/hostname** so, dass sie nur den Hostnamen des Computers enthält.

```
hostname
```

Schritt 1c: Dem Hostnamen eine Loopback-Adresse zuweisen

Stellen Sie sicher, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) des Computers korrekt zurückgemeldet werden. Dazu ändern Sie die folgende Zeile der Datei **/etc/hosts**, um den FQDN und den Hostnamen als die ersten beiden Einträge aufzunehmen:

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

Zum 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 keine NetBIOS-Namenskürzung. Daher darf der Hostname 15 Zeichen nicht überschreiten.

> **Tipp:**

> Verwenden Sie nur die Zeichen a–z, A–Z, 0–9 und Bindestrich (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Beginnen Sie einen Hostnamen nicht mit einer Zahl und beenden Sie ihn nicht mit einem Bindestrich. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Schritt 1d: Hostnamen überprüfen

Überprüfen Sie, ob der Hostname korrekt festgelegt ist:

```
hostname
```

Dieser Befehl gibt nur den Hostnamen des Computers und nicht dessen FQDN zurück.

Überprüfen Sie, ob der FQDN korrekt eingestellt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN des Computers zurück.

Schritt 1e: Multicast-DNS deaktivieren

Die Standardeinstellungen haben Multicast-DNS (**mDNS**) aktiviert, was zu inkonsistenten Namensauflösungsergebnissen führen kann.

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

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

In:

`hosts: files dns`

Schritt 1f: Namensauflösung und Dienstverfügbarkeit prüfen

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

```
nslookup domain-controller-fqdn
```

```
ping domain-controller-fqdn



nslookup delivery-controller-fqdn



ping delivery-controller-fqdn
```

Wenn Sie den FQDN nicht auflösen oder keine dieser Maschinen anpingen können, überprüfen Sie die Schritte, bevor Sie fortfahren.

Schritt 1g: Taktsynchronisierung konfigurieren (chrony)

Eine genaue Taktsynchronisierung zwischen den VDAs, Delivery Controllern und Domänencontrollern ist entscheidend. Das Hosten des Linux VDA als virtuelle Maschine kann zu Problemen mit der Taktverschiebung führen. Aus diesem Grund wird die Synchronisierung der Zeit mit einem entfernten Zeitdienst bevorzugt.

chrony installieren:

```
apt-get install chrony
```

Bearbeiten Sie als Root-Benutzer **/etc/chrony/chrony.conf** und fügen Sie einen Servereintrag für jeden entfernten Zeitserver 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-Pool-Servern. Fügen Sie einen Servereintrag für jeden Active Directory-Domänencontroller in der Domäne hinzu.

Entfernen Sie alle anderen **Server**- oder **Pool**-Einträge, einschließlich Loopback-IP-Adresse, Localhost und öffentliche Server-Einträge ***.pool.ntp.org**.

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

```
sudo systemctl restart chrony
```

Schritt 1h: OpenJDK 11 installieren

Der Linux VDA erfordert die Anwesenheit von OpenJDK 11.

Installieren Sie unter Ubuntu 16.04 OpenJDK 11, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das neueste OpenJDK 11 von `<https://jdk.java.net/archive/>` herunter.
2. Führen Sie den Befehl `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` aus, um das heruntergeladene Paket zu entpacken.
3. (Optional) Führen Sie den Befehl `mv jdk-11.0.2/ <target directory>` aus, um OpenJDK in einem Zielverzeichnis zu speichern.
4. Führen Sie den Befehl `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` aus, um die Java-Laufzeitumgebung einzurichten.
5. Führen Sie den Befehl `java -version` aus, um die Java-Version zu überprüfen.

Installieren Sie unter Ubuntu 20.04 und Ubuntu 18.04 OpenJDK 11 mit:

```
sudo apt-get install -y openjdk-11-jdk
```

Schritt 1i: PostgreSQL installieren

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

```
sudo apt-get install -y postgresql



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

Schritt 1j: Motif installieren

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

Schritt 1k: Andere Pakete installieren

```
sudo apt-get install -y libsasl2-2



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

```
sudo apt-get install -y libldap-2.4-2
```

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

```
sudo apt-get install -y libgtk2.0-0
```

Schritt 2: Hypervisor vorbereiten

Einige Änderungen sind erforderlich, wenn der Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausgeführt wird. Nehmen Sie die folgenden Änderungen entsprechend der verwendeten Hypervisor-Plattform vor. Es sind keine Änderungen erforderlich, wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen.

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

Wenn die Citrix Hypervisor-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und Citrix Hypervisor auf, da beide versuchen, die Systemuhr zu verwalten. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit dem NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen können Sie, wenn Sie einen paravirtualisierten Linux-Kernel mit installierten Citrix VM Tools ausführen, innerhalb der Linux-VM überprüfen, ob die Citrix Hypervisor-Zeitsynchronisierungsfunktion vorhanden und aktiviert ist:

```
su -
```

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

Dieser Befehl gibt 0 oder 1 zurück:

- 0 – Die Zeitsynchronisierungsfunktion ist aktiviert und muss deaktiviert werden.

- 1 – Die Zeitsynchronisierungsfunktion ist deaktiviert, und es sind keine weiteren Maßnahmen erforderlich.

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

Wenn aktiviert, deaktivieren Sie die Zeitsynchronisierungsfunktion, indem Sie 1 in die Datei schreiben:

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

Um diese Änderung dauerhaft und nach einem Neustart persistent zu machen, bearbeiten Sie die Datei **/etc/sysctl.conf** und fügen Sie die Zeile hinzu:

`xen.independent_wallclock = 1`

Um diese Änderungen zu überprüfen, starten Sie das System neu:

```
su -



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

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

Linux-VMs mit installierten Hyper-V Linux Integration Services können die Hyper-V-Zeitsynchronisierungsfunktion verwenden, um die Zeit des Hostbetriebssystems zu nutzen. Um sicherzustellen, dass die Systemuhr genau bleibt, aktivieren Sie diese Funktion zusammen mit den NTP-Diensten.

Vom Verwaltungsbetriebssystem aus:

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

> **Hinweis:**

> Dieser Ansatz unterscheidet sich von VMware und Citrix Hypervisor, wo die Host-Zeitsynchronisierung deaktiviert ist, um Konflikte mit NTP zu vermeiden. Die Hyper-V-Zeitsynchronisierung kann mit der NTP-Zeitsynchronisierung koexistieren und diese ergänzen.

Zeitsynchronisierung auf ESX und ESXi beheben

Wenn die VMware-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und dem Hypervisor auf, da beide versuchen, die Systemuhr zu synchronisieren. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel mit installierten VMware Tools ausführen:

1. Öffnen Sie den vSphere Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Eigenschaften der virtuellen Maschine** die Registerkarte **Optionen**.
4. Wählen Sie **VMware Tools** aus.
5. Deaktivieren Sie im Feld **Erweitert** die Option **Gastzeit mit Host synchronisieren**.

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

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

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

Befolgen Sie die Anweisungen basierend auf der von Ihnen gewählten Methode.

> **Hinweis:**

> Sitzungsstarts können fehlschlagen, wenn derselbe Benutzername für das lokale Konto im Linux VDA und das Konto in AD verwendet wird.

Samba Winbind

Erforderliche Pakete installieren oder aktualisieren

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

Winbind-Daemon für den Start beim Systemstart aktivieren

Der Winbind-Daemon muss so konfiguriert werden, dass er beim Systemstart gestartet wird:

```
sudo systemctl enable winbind
```

> **Hinweis:**
>
> Stellen Sie sicher, dass sich das `winbind`-Skript unter `/etc/init.d` befindet.

Kerberos konfigurieren

Öffnen Sie **/etc/krb5.conf** als Root-Benutzer, und nehmen Sie die folgenden Einstellungen vor:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Einzeldomänen-, Einzelforst-Modell 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**. Der **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. **EXAMPLE.COM**.

Winbind-Authentifizierung konfigurieren

Konfigurieren Sie Winbind manuell, da Ubuntu kein Tool wie `authconfig` in RHEL und yast2 in SUSE besitzt.

Öffnen Sie **/etc/samba/smb.conf** und nehmen Sie die folgenden 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-Realm-Name in Großbuchstaben.

`nsswitch` konfigurieren

Öffnen Sie **/etc/nsswitch.conf** und fügen Sie `winbind` an die folgenden Zeilen an:

`passwd: compat winbind`

`group: compat winbind`

Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

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

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

`winbind` neu starten

```
sudo systemctl restart winbind
```

PAM für Winbind konfigurieren

Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass die Optionen **Winbind NT/Active Directory-Authentifizierung** und **Home-Verzeichnis bei Anmeldung erstellen** ausgewählt sind:

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

> **Tipp:**
>
> Der `winbind`-Daemon bleibt nur aktiv, wenn der Computer einer Domäne beigetreten ist.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in Active Directory haben.

Führen Sie den **net ads**-Befehl von Samba aus, um zu überprüfen, ob der Computer einer Domäne beigetreten ist:

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

Kerberos-Konfiguration überprüfen

Um zu überprüfen, ob Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, stellen Sie sicher, dass die Systemdatei **keytab** erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der Schlüssel an, die für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um den Computer mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Die Computer- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie mit Folgendem, ob das TGT-Ticket für das Computerkonto zwischengespeichert wurde:

```
sudo klist
```

Überprüfen Sie die Kontodetails des Computers mit:

```
sudo net ads status
```

Benutzerauthentifizierung überprüfen

Verwenden Sie das Tool **wbinfo**, um zu überprüfen, ob Domänenbenutzer sich bei der Domäne authentifizieren können:

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

Die hier angegebene Domäne ist der AD-Domänenname, nicht der Kerberos-Realm-Name. Für die Bash-Shell muss der Backslash (\\) mit einem weiteren Backslash maskiert werden. Dieser Befehl gibt eine Meldung über Erfolg oder Misserfolg zurück.

Um zu überprüfen, ob das Winbind PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u
```

Hinweis:

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

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die von dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

Ein ähnlicher Test kann durch direkte Anmeldung an der Gnome- oder KDE-Konsole durchgeführt werden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Linux VDA installieren fort.

Tipp:

Wenn die Benutzerauthentifizierung erfolgreich ist, Sie aber Ihren Desktop beim Anmelden mit einem Domänenkonto nicht anzeigen können, starten Sie den Computer neu und versuchen Sie es dann erneut.

Quest-Authentifizierungsdienst

Quest auf Domänencontroller konfigurieren

Gehen Sie davon aus, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und über administrative Berechtigungen zum Erstellen von Computerobjekten in Active Directory verfügen.

Domänenbenutzer zur Anmeldung an Linux VDA-Maschinen aktivieren

Um Domänenbenutzern das Herstellen von HDX™-Sitzungen auf einer Linux VDA-Maschine zu ermöglichen:

1. Öffnen Sie in der Verwaltungskonsole „Active Directory-Benutzer und -Computer“ die Active Directory-Benutzereigenschaften für dieses Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix-Konto**.
3. Aktivieren Sie **Unix-aktiviert**.
4. Legen Sie die **Primäre GID-Nummer** auf die Gruppen-ID einer tatsächlichen Domänenbenutzergruppe fest.

Hinweis:

Diese Anweisungen sind äquivalent für die Einrichtung von Domänenbenutzern zur Anmeldung über die Konsole, RDP, SSH oder jedes andere Remoting-Protokoll.

Quest auf Linux VDA konfigurieren

UMGEHUNG DER SELINUX-RICHTLINIENERZWINGUNG

Die Standard-RHEL-Umgebung hat SELinux vollständig erzwungen. Diese Erzwingung stört die von Quest verwendeten Unix-Domain-Socket-IPC-Mechanismen und verhindert, dass Domänenbenutzer sich anmelden können.

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

`SELINUX=disabled`

Diese Änderung erfordert einen Neustart der Maschine:

```
reboot
```

> **Wichtig:**
>
> Verwenden Sie diese Einstellung mit Vorsicht. Das erneute Aktivieren der SELinux-Richtlinienerzwingung nach der Deaktivierung kann zu einer vollständigen Sperrung führen, selbst für den Root-Benutzer und andere lokale Benutzer.

VAS-DAEMON KONFIGURIEREN

Die automatische Verlängerung von Kerberos-Tickets muss aktiviert und getrennt werden. Die Authentifizierung (Offline-Anmeldung) muss deaktiviert werden:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Dieser Befehl legt das Verlängerungsintervall auf neun Stunden (32.400 Sekunden) fest, was eine Stunde weniger ist als die standardmäßige Ticket-Lebensdauer von 10 Stunden. Legen Sie diesen Parameter auf einen niedrigeren Wert fest, wenn Systeme eine kürzere Ticket-Lebensdauer haben.

PAM UND NSS KONFIGURIEREN

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

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



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

Windows-Domäne beitreten

Fügen Sie die Linux-Maschine der Active Directory-Domäne mit dem Quest-Befehl `vastool` hinzu:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

Der Benutzer ist ein beliebiger Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne. Der Domänenname ist der DNS-Name der Domäne, z. B. example.com.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in Active Directory haben. So überprüfen Sie, ob eine mit Quest verbundene Linux-Maschine in der Domäne ist:

```
sudo /opt/quest/bin/vastool info domain
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl den Domänennamen zurück. Wenn die Maschine keiner Domäne beigetreten ist, wird der folgende Fehler 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 zu überprüfen, ob Quest Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die vom Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Linux VDA installieren fort.

Centrify DirectControl

Windows-Domäne beitreten

Nach der Installation des Centrify DirectControl Agent fügen Sie die Linux-Maschine der Active Directory-Domäne mit dem Centrify-Befehl `adjoin` hinzu:

```
su –

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

Der Parameter **user** ist ein beliebiger Active Directory-Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne. Der Parameter **domain-name** ist der Name der Domäne, der die Linux-Maschine hinzugefügt werden soll.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine mit Centrify verbundene Linux-Maschine in der Domäne ist:

```
su -


adinfo
```

Vergewissern Sie sich, dass der Wert **Joined to domain** gültig ist und der **CentrifyDC mode** den Status **connected** zurückgibt. Bleibt der Modus im Startzustand hängen, hat der Centrify-Client Probleme mit der Serververbindung oder Authentifizierung.

Umfassendere System- und Diagnoseinformationen sind verfügbar mit:

```
adinfo --sysinfo all


adinfo --diag
```

Testen Sie die Konnektivität zu den verschiedenen Active Directory- und Kerberos-Diensten.

```
adinfo --test
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

SSSD

Kerberos konfigurieren

Führen Sie den folgenden Befehl aus, um Kerberos zu installieren:

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

Um Kerberos zu konfigurieren, öffnen Sie **/etc/krb5.conf** als Root und legen Sie die Parameter fest:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Einzeldomänen-, Einzelforst-Modell 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 `domain-dns-name`-Parameter in diesem Kontext ist der DNS-Domänenname, z. B. example.com. Das *REALM* ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM.

Der Domäne beitreten

SSSD muss so konfiguriert werden, dass es Active Directory als Identitätsanbieter und Kerberos zur Authentifizierung verwendet. SSSD bietet jedoch keine AD-Client-Funktionen zum Beitreten zur Domäne und zur Verwaltung der System-Keytab-Datei. Stattdessen können Sie `adcli`, `realmd` oder `Samba` verwenden.

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

- **Wenn Sie `adcli` verwenden, um der Domäne beizutreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie `adcli`.

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

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

   Entfernen Sie die alte System-Keytab-Datei und treten Sie der Domäne bei mit:

   ```
   su -



   rm -rf /etc/krb5.keytab



   adcli join domain-dns-name -U user -H hostname-fqdn
   ```

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

   Die Option **-H** ist erforderlich, damit `adcli` SPN im Format host/hostname-fqdn@REALM generiert, was der Linux VDA benötigt.

3. System-Keytab überprüfen.

   Führen Sie für eine Ubuntu 20.04-Maschine den Befehl `adcli testjoin` aus, um zu testen, ob sie der Domäne beigetreten ist.

   Führen Sie für eine Ubuntu 18.04- oder Ubuntu 16.04-Maschine den Befehl `sudo klist -ket` aus, um sicherzustellen, dass die System-Keytab-Datei erstellt wurde.

   Überprüfen Sie, ob der Zeitstempel für jeden Schlüssel mit der Zeit übereinstimmt, zu der die Maschine der Domäne beigetreten ist.

- **Wenn Sie `Samba` verwenden, um der Domäne beizutreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.

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

2. Konfigurieren Sie `Samba`.

   Öffnen Sie **/etc/samba/smb.conf**, und nehmen Sie die folgenden 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-Realm-Name in Großbuchstaben.

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

   Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Windows-Konto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen.

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

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

SSSD einrichten

Erforderliche Pakete installieren oder aktualisieren:

Installieren Sie die erforderlichen SSSD- und Konfigurationspakete, falls noch nicht geschehen:

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

Wenn die Pakete bereits installiert sind, wird ein Update empfohlen:

```
sudo apt-get install --only-upgrade sssd
```

Hinweis:

Standardmäßig konfiguriert der Installationsprozess in Ubuntu **nsswitch.conf** und das PAM-Anmeldemodul automatisch.

SSSD konfigurieren

SSSD-Konfigurationsänderungen sind erforderlich, bevor der SSSD-Daemon gestartet wird. Bei einigen SSSD-Versionen ist die Konfigurationsdatei **/etc/sssd/sssd.conf** standardmäßig nicht installiert und muss manuell erstellt werden. Erstellen oder öffnen Sie als Root **/etc/sssd/sssd.conf** und nehmen Sie die folgenden Einstellungen vor:

`[sssd]`

`services = nss, pam`

`config_file_version = 2`

`domains =` *`domain-dns-name`*

`[domain/` *`domain-dns-name`* `]`

`id_provider = ad`

`access_provider = ad`

`auth_provider = krb5`

`krb5_realm =` *`REALM`*

`# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days`

`krb5_renewable_lifetime = 14d`

`# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours`

`krb5_renew_interval = 1h`

```
krb5_ccachedir = /tmp
```

```
krb5_ccname_template = FILE:%d/krb5cc_%U
```

```
# This ldap_id_mapping setting is also the default value
```

```
ldap_id_mapping = true
```

```
override_homedir = /home/%d/%u
```

```
default_shell = /bin/bash
```

```
ad_gpo_map_remote_interactive = +ctxhdx
```

> **Hinweis:**

> ldap_id_mapping ist auf **true** gesetzt, damit SSSD selbst die Zuordnung von Windows-SIDs zu Unix-UIDs übernimmt. Andernfalls muss das Active Directory POSIX-Erweiterungen bereitstellen können. Der PAM-Dienst `ctxhdx` wird zu ad_gpo_map_remote_interactive hinzugefügt.

> Der Parameter **domain-dns-name** in diesem Kontext ist der DNS-Domänenname, z. B. example.com. Der **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM. Es ist nicht erforderlich, den NetBIOS-Domänennamen zu konfigurieren.

> Informationen zu den Konfigurationseinstellungen finden Sie in den Manpages für sssd.conf und `sssd-ad`.

> Der SSSD-Daemon erfordert, dass die Konfigurationsdatei nur Leseberechtigungen für den Eigentümer hat:

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

SSSD-Daemon starten

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

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

PAM-Konfiguration

Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass die Optionen **SSS-Authentifizierung** und **Home-Verzeichnis bei Anmeldung erstellen** ausgewählt sind:

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben.

- Wenn Sie `adcli` zur Überprüfung der Domänenmitgliedschaft verwenden, führen Sie den Befehl `sudo adcli info domain-dns-name` aus, um die Domäneninformationen anzuzeigen.
- Wenn Sie `Samba` zur Überprüfung der Domänenmitgliedschaft verwenden, führen Sie den Befehl `sudo net ads testjoin` aus, um zu überprüfen, ob die Maschine einer Domäne beigetreten ist, und den Befehl `sudo net ads info`, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen.

Kerberos-Konfiguration überprüfen

Um zu überprüfen, ob Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, stellen Sie sicher, dass die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der Schlüssel an, die für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Die Maschinen- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT für das Maschinenkonto zwischengespeichert wurde, indem Sie Folgendes verwenden:

```
sudo klist
```

Benutzerauthentifizierung überprüfen

SSSD bietet kein Befehlszeilentool zum direkten Testen der Authentifizierung mit dem Daemon und kann nur über PAM erfolgen.

Um zu überprüfen, ob das SSSD PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u



klist



exit
```

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

Als Root-Benutzer überprüfen Sie, ob eine entsprechende Ticket-Cache-Datei für die UID erstellt wurde, die vom vorherigen Befehl **id -u** zurückgegeben wurde:

```
ls /tmp/krb5cc_uid
```

Ein ähnlicher Test kann durch Anmelden bei KDE oder Gnome Display Manager durchgeführt werden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

Erforderliches PBIS-Paket herunterladen

Zum Beispiel:

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

PBIS-Installationsskript ausführbar machen

Zum Beispiel:

```
sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

PBIS-Installationsskript ausführen

Zum Beispiel:

```
sudo sh pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
```

Der **Benutzer** ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne besitzt. Der **Domänenname** ist der DNS-Name der Domäne, z. B. example.com.

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine PBIS-verbundene Linux-Maschine in der Domäne ist:

```
/opt/pbis/bin/domainjoin-cli query
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl die Informationen über die aktuell beigetretene AD-Domäne und OU zurück. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen

Um zu überprüfen, dass PBIS Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

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



id -u
```

Vergewissern Sie sich, dass eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die vom Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Schritt 4: Installieren von .NET Core Runtime 3.1 als Voraussetzung

Bevor Sie den Linux VDA installieren, installieren Sie .NET Core Runtime 3.1 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

Nach der Installation von .NET Core Runtime 3.1 führen Sie den Befehl **which dotnet** aus, um Ihren Runtime-Pfad zu finden.

Basierend auf der Befehlsausgabe legen Sie den binären Pfad der .NET Core-Runtime fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als binären .NET-Pfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

Gehen Sie zur Downloadseite von Citrix Virtual Apps and Desktops™. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das Linux VDA-Paket herunterzuladen, das Ihrer Linux-Distribution entspricht.

Schritt 6: Installieren des Linux VDA

Schritt 6a: Installieren des Linux VDA

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

Für Ubuntu 20.04:

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

Für Ubuntu 18.04:

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

Für Ubuntu 16.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu16.04_amd64.deb
```

Debian-Abhängigkeitsliste für Ubuntu 20.04:

```
ibus >= 1.5



libsasl2-modules-gssapi-mit >= 2.1.~
```

```
postgresql >= 12

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

ufw >= 0.36

ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34

gtk3-nocsd >= 3
```

```
bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

libgoogle-perftools4 >= 2.7~

libpython2.7 >= 2.7~
```

Debian-Abhängigkeitsliste für Ubuntu 18.04:

```
libmspack0 >= 0.6

ibus >= 1.5

libnss3-tools >= 2:3.35

postgresql >= 9.5
```

```
libpostgresql-jdbc-java >= 9.2

openjdk-11-jdk >= 11

gtk3-nocsd >=3

imagemagick >= 8:6.8.9.9

ufw >= 0.35

ubuntu-desktop >= 1.361

libxrandr2 >= 2:1.5.0

libxtst6 >= 2:1.2.2

libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3
```

```
findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42

libsasl2-modules-gssapi-mit >= 2.1.~

python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~

xserver-xorg-core >= 2:1.18

xserver-xorg-core << 2:1.19

x11vnc>=0.9.13
```

```
python-websockify >= 0.6.1
```

Debian-Abhängigkeitsliste für Ubuntu 16.04:

```
libmspack0 >=  0.5


python-pkg-resources >= 20.7.0


libnss3-tools >= 2:3.28


postgresql >= 9.5


libpostgresql-jdbc-java >= 9.2


imagemagick >= 8:6.8.9.9


ufw >= 0.35


ubuntu-desktop >= 1.361


libxrandr2 >= 2:1.5.0


libxtst6 >= 2:1.2.2
```

```
libxm4 >= 2.3.4

util-linux >= 2.27.1

bash >= 4.3

findutils >= 4.6.0

sed >= 4.2.2

cups >= 2.1

libldap-2.4-2 >= 2.4.42

libsasl2-modules-gssapi-mit >= 2.1.~

python-requests >= 2.9.1

libgoogle-perftools4 >= 2.4~

xserver-xorg-core >= 2:1.18
```

```
xserver-xorg-core << 2:1.19


x11vnc>=0.9.13


python-websockify >= 0.6.1
```

Hinweis:

Eine Matrix der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden, finden Sie unter Systemanforderungen.

Schritt 6b: Linux VDA aktualisieren (optional)

Sie können eine vorhandene Installation von den beiden vorherigen Versionen und von einem LTSR-Release aktualisieren.

```
sudo dpkg -i <PATH>/<Linux VDA deb>
```

Hinweis:

Beim Upgrade einer vorhandenen Installation werden die Konfigurationsdateien unter /etc/xdl überschrieben. Sichern Sie die Dateien, bevor Sie ein Upgrade durchführen.

Schritt 7: Linux VDA konfigurieren

Nach der Installation des Pakets müssen Sie den Linux VDA durch Ausführen des Skripts ctxsetup.sh konfigurieren. Bevor das Skript Änderungen vornimmt, überprüft es die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Bei Bedarf können Sie das Skript jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell mit Eingabeaufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript, bevor Sie fortfahren:

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

Konfiguration mit Eingabeaufforderung

Führen Sie eine manuelle Konfiguration mit Fragen aus:

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

Automatisierte Konfiguration

Für eine automatisierte Installation können die vom Setup-Skript benötigten Optionen über Umgebungsvariablen bereitgestellt werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript den Benutzer nicht zur Eingabe von Informationen auf, was einen skriptgesteuerten Installationsprozess ermöglicht.

Unterstützte Umgebungsvariablen sind:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags. Standardmäßig auf N festgelegt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste von FQDNs (Fully Qualified Domain Names) der Delivery Controller, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. 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, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux Virtual Desktop-Dienste werden nach dem Start der Maschine gestartet. Standardmäßig auf Y festgelegt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux Virtual Desktop-Dienste erfordern, dass eingehende Netzwerkverbindungen über die Systemfirewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Ports 80 und 1494) automatisch in der Systemfirewall für den Linux Virtual Desktop öffnen. Standardmäßig auf Y festgelegt.
- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4 \|5** – Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird vom installierten und konfigurierten Active Directory-Integrationstool auf dem

System bestimmt. Geben Sie die zu verwendende unterstützte Active Directory-Integrationsmethode an:

  - 1 – Samba Winbind
  - 2 – Quest Authentication Service
  - 3 – Centrify DirectControl
  - 4 – SSSD
  - 5 – PBIS

- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung von grafikintensiven Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für den VDI-Desktop-Modus (Einzelsitzung) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Gibt an, ob die Maschine als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie diese Variable auf Y. Diese Variable ist standardmäßig auf N festgelegt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA erkennt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf einen lokalen Standort zu beschränken, geben Sie einen DNS-Standortnamen an. Diese Variable ist standardmäßig auf **\<none\>** festgelegt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum Beispiel, ad1.mycompany.com:389. Diese Variable ist standardmäßig auf **\<none\>** eingestellt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com) festgelegt ist. Um jedoch die Suchleistung zu verbessern, können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** eingestellt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein, wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit dem Text **\<none\>** aus und ändern Sie nicht die Reihenfolge der Serveradressen.

- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – Der Pfad zur Installation der .NET Core Runtime 3.1 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Gibt die GNOME- oder MATE-Desktop-Umgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

> **Hinweis:**
>
> Sie können die Desktop-Umgebung für einen Ziel-Sitzungsbenutzer auch ändern, indem Sie die folgenden Schritte ausführen:
>
> a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.
>
> b. Bearbeiten Sie die `.xsession`-Datei, um eine Desktop-Umgebung basierend auf den Distributionen anzugeben.
>
> **Für MATE-Desktop unter CentOS, Ubuntu und Debian**
>
> MSESSION="$(type -p mate-session)"
>
> \> wenn ; dann
>
> ```
> exec mate-session
> ```
>
> \> fi
>
> ```
> **Für GNOME-Desktop unter CentOS**
>
>
>
>    GSESSION="$(type -p gnome-session)"
> ```

\> if ; then

```
    export GNOME_SHELL_SESSION_MODE=classic
```

\> exec gnome-session --session=gnome-classic

```
    fi

**Für GNOME-Desktop unter Ubuntu und Debian**



    GSESSION="$(type -p gnome-session)"
```

\> wenn ; dann

```
    exec gnome-session
```

\> fi

a. Teilen Sie die Dateiberechtigung 700 mit dem Ziel-Sitzungsbenutzer.

- **CTX_XDL_START_SERVICE=Y \| N** – Gibt an, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Standardmäßig auf Y gesetzt.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Abhören von 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:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

```
export CTX_XDL_FAS_LIST=‘list-fas-servers’ | '<none>'

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

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

Geben Sie beim Ausführen des sudo-Befehls die Option **-E** ein, um die vorhandenen Umgebungsvariablen an die neue Shell zu übergeben, die erstellt wird. Wir empfehlen, aus den vorhergehenden Befehlen eine Shell-Skriptdatei mit **#\!/bin/bash** als erster Zeile zu erstellen.

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=‘list-ddc-fqdns’ \

CTX_XDL_VDA_PORT=port-number \
```

```
CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST=‘list-ldap-servers’ \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST=‘list-fas-servers’ \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \
```

```
CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Konfigurationsänderungen entfernen

In einigen Szenarien müssen Sie möglicherweise die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernen, ohne das Linux-VDA-Paket zu deinstallieren.

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

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

So entfernen Sie Konfigurationsänderungen:

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

Wichtig:

Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank und macht den Linux-VDA unbrauchbar.

Konfigurationsprotokolle

Die Skripte **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an, wobei zusätzliche Informationen in die Konfigurationsprotokolldatei **/tmp/xdl.configure.log** geschrieben werden.

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

Linux-VDA-Software deinstallieren

So überprüfen Sie, ob der Linux-VDA installiert ist, und um die Version des installierten Pakets anzuzeigen:

```
dpkg -l xendesktopvda
```

Um detailliertere Informationen anzuzeigen:

```
apt-cache show xendesktopvda
```

So deinstallieren Sie die Linux VDA-Software:

```
dpkg -r xendesktopvda
```

Hinweis:

Durch die Deinstallation der Linux VDA-Software werden die zugehörigen PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden jedoch nicht gelöscht.

Tipp:

Die Informationen in diesem Abschnitt behandeln nicht die Entfernung abhängiger Pakete, einschließlich PostgreSQL.

Schritt 8: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um häufige Konfigurationsprobleme in einer Linux VDA-Umgebung zu überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 9: Linux VDA ausführen

Nachdem Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, verwenden Sie die folgenden Befehle, um den Linux VDA zu steuern.

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Linux VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

> **Hinweis:**
>
> Bevor Sie die Dienste `ctxvda` und `ctxhdx` beenden, führen Sie den Befehl `service ctxmonitorservice stop` aus, um den Überwachungsdienst-Daemon zu beenden. Andernfalls startet der Überwachungsdienst-Daemon die von Ihnen beendeten Dienste neu.

Linux VDA neu starten:

So starten Sie die Linux VDA-Dienste neu:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx



sudo systemctl restart ctxvda
```

Überprüfen Sie den Status des Linux VDA:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda



sudo systemctl status ctxhdx
```

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 dem traditionellen Windows VDA-Ansatz. Eine detailliertere Beschreibung zur Durchführung dieser Aufgaben finden Sie unter Maschinenkataloge erstellen und Maschinenkataloge verwalten.

Für die Erstellung von Maschinenkatalogen, die Linux VDA-Maschinen enthalten, gibt es einige Einschränkungen, die den Prozess von der Erstellung von Maschinenkatalogen für Windows VDA-Maschinen unterscheiden:

- Wählen Sie für das Betriebssystem:
  - Die Option **Multi-session OS** für ein Bereitstellungsmodell mit gehosteten Shared Desktops.
  - Die Option **Single-session OS** für ein VDI-Bereitstellungsmodell mit dedizierten Desktops.
- Mischen Sie keine Linux- und Windows VDA-Maschinen im selben Maschinenkatalog.

Hinweis:

Frühere Versionen von Citrix Studio unterstützten den Begriff „Linux OS“ nicht. Die Auswahl der Option **Windows Server OS** oder **Server OS** impliziert jedoch ein äquivalentes Bereitstellungsmodell für gehostete Shared Desktops. Die Auswahl der Option **Windows Desktop OS** oder **Desktop OS** impliziert ein Bereitstellungsmodell mit einem Benutzer pro Maschine.

Tipp:

> Wenn Sie eine Maschine aus der Active Directory-Domäne entfernen und wieder hinzufügen, müssen Sie die Maschine aus dem Maschinenkatalog entfernen und erneut hinzufügen.

Schritt 11: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps™ oder Citrix Virtual Desktops

Der Prozess zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen, die Linux VDA-Maschinen enthalten, ist nahezu identisch mit dem für Windows VDA-Maschinen. Eine detailliertere Beschreibung zur Durchführung dieser Aufgaben finden Sie unter Bereitstellungsgruppen erstellen.

Für die Erstellung von Bereitstellungsgruppen, die Linux VDA-Maschinenkataloge enthalten, gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die von Ihnen ausgewählten AD-Benutzer und -Gruppen ordnungsgemäß für die Anmeldung an den Linux VDA-Maschinen konfiguriert wurden.
- Lassen Sie die Anmeldung nicht authentifizierter (anonymer) Benutzer nicht zu.
- Mischen Sie die Bereitstellungsgruppe nicht mit Maschinenkatalogen, die Windows-Maschinen enthalten.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2106.

Linux Virtual Delivery Agent für Debian manuell installieren

> **Wichtig:**

> Für Neuinstallationen empfehlen wir die Verwendung von Easy Install für eine schnelle Installation. Easy Install spart Zeit und Arbeit und ist weniger fehleranfällig als die in diesem Artikel beschriebene manuelle Installation.

Schritt 1: Debian für die VDA-Installation vorbereiten

Schritt 1a: Netzwerkkonfiguration überprüfen

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

Schritt 1b: Hostnamen festlegen

Um sicherzustellen, dass der Hostname des Computers korrekt gemeldet wird, ändern Sie die Datei **/etc/hostname** so, dass sie nur den Hostnamen des Computers enthält.

```
hostname
```

Schritt 1c: Loopback-Adresse dem Hostnamen zuweisen

Stellen Sie sicher, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) des Computers korrekt zurückgemeldet werden. Dazu ändern Sie die folgende Zeile der Datei **/etc/hosts** so, dass sie den FQDN und den Hostnamen als erste zwei Einträge enthält:

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

Zum 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 keine NetBIOS-Namenskürzung. Daher darf der Hostname 15 Zeichen nicht überschreiten.

> **Tipp:**

> Verwenden Sie nur die Zeichen a–z, A–Z, 0–9 und Bindestrich (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Beginnen Sie einen Hostnamen nicht mit einer Zahl und beenden Sie ihn nicht mit einem Bindestrich. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Schritt 1d: Hostnamen überprüfen

Überprüfen Sie, ob der Hostname korrekt festgelegt ist:

```
hostname
```

Dieser Befehl gibt nur den Hostnamen des Computers und nicht dessen FQDN zurück.

Überprüfen Sie, ob der FQDN korrekt eingestellt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN des Computers zurück.

Schritt 1e: Multicast-DNS deaktivieren

Die Standardeinstellungen haben Multicast-DNS (**mDNS**) aktiviert, was zu inkonsistenten Namensauflösungsergebnissen führen kann.

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

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

In:

`hosts: files dns`

Schritt 1f: Namensauflösung und Dienstverfügbarkeit prüfen

Vergewissern Sie sich, dass Sie den FQDN auflösen und den Domänencontroller und Delivery Controller™ anpingen können:

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

Wenn Sie den FQDN nicht auflösen oder keine dieser Maschinen anpingen können, überprüfen Sie die Schritte, bevor Sie fortfahren.

Schritt 1g: Taktsynchronisierung konfigurieren (chrony)

Die Aufrechterhaltung einer genauen Taktsynchronisierung zwischen den VDAs, Delivery Controllern und Domänencontrollern ist entscheidend. Das Hosten des Linux VDA als virtuelle Maschine kann zu Problemen mit der Taktverschiebung führen. Aus diesem Grund wird die Zeitsynchronisierung mit einem Remote-Zeitdienst bevorzugt.

Chrony installieren:

```
apt-get install chrony
```

Bearbeiten Sie als Root-Benutzer **/etc/chrony/chrony.conf** und fügen Sie einen Servereintrag für jeden Remote-Zeitserver 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-Pool-Servern. Fügen Sie einen Servereintrag für jeden Active Directory-Domänencontroller in der Domäne hinzu.

Entfernen Sie alle anderen aufgeführten **server**- oder **pool**-Einträge, einschließlich Loopback-IP-Adresse, localhost und öffentliche Server-Einträge ***.pool.ntp.org**.

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

```
sudo systemctl restart chrony
```

Schritt 1h: Pakete installieren

```
sudo apt-get install -y libsasl2-2



sudo apt-get install -y libgtk2.0-0
```

Schritt 1i: Das oldstable-Repository hinzufügen

Um die erforderlichen Abhängigkeiten für eine Debian-Distribution zu installieren, fügen Sie die Zeile `deb http://deb.debian.org/debian/ oldstable main` zur Datei `/etc/apt/sources.list` hinzu.

Schritt 2: Den Hypervisor vorbereiten

Einige Änderungen sind erforderlich, wenn der Linux VDA als virtuelle Maschine auf einem unterstützten Hypervisor ausgeführt wird. Nehmen Sie die folgenden Änderungen entsprechend der verwendeten Hypervisor-Plattform vor. Es sind keine Änderungen erforderlich, wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen.

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

Wenn die Citrix Hypervisor-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und Citrix Hypervisor auf, da beide versuchen, die Systemuhr zu verwalten. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit dem NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Auf einigen Linux-Distributionen können Sie, wenn Sie einen paravirtualisierten Linux-Kernel mit installierten Citrix VM Tools ausführen, innerhalb der Linux-VM überprüfen, ob die Citrix Hypervisor-Zeitsynchronisierungsfunktion vorhanden und aktiviert ist:

```
su -



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

Dieser Befehl gibt 0 oder 1 zurück:

- 0 – Die Zeitsynchronisierungsfunktion ist aktiviert und muss deaktiviert werden.
- 1 – Die Zeitsynchronisierungsfunktion ist deaktiviert, und es sind keine weiteren Maßnahmen erforderlich.

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

Falls aktiviert, deaktivieren Sie die Zeitsynchronisierungsfunktion, indem Sie 1 in die Datei schreiben:

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

Um diese Änderung nach einem Neustart dauerhaft zu machen, bearbeiten Sie die Datei **/etc/sysctl.conf** und fügen Sie die Zeile hinzu:

`xen.independent_wallclock = 1`

Um diese Änderungen zu überprüfen, starten Sie das System neu:

```
su -



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

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

Linux-VMs mit installierten Hyper-V Linux Integration Services können die Hyper-V-Zeitsynchronisierungsfunktion verwenden, um die Zeit des Hostbetriebssystems zu nutzen. Um sicherzustellen, dass die Systemuhr genau bleibt, aktivieren Sie diese Funktion zusammen mit den NTP-Diensten.

Vom Verwaltungsbetriebssystem aus:

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

> **Hinweis:**

> Dieser Ansatz unterscheidet sich von VMware und Citrix Hypervisor, wo die Host-Zeitsynchronisierung deaktiviert ist, um Konflikte mit NTP zu vermeiden. Die Hyper-V-Zeitsynchronisierung kann mit der NTP-Zeitsynchronisierung koexistieren und diese ergänzen.

Zeitsynchronisierung auf ESX und ESXi beheben

Wenn die VMware-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und dem Hypervisor auf, die beide versuchen, die Systemuhr zu synchronisieren. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel mit installierten VMware Tools ausführen:

1. Öffnen Sie den vSphere Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Eigenschaften der virtuellen Maschine** die Registerkarte **Optionen**.
4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Erweitert** die Option **Gastzeit mit Host synchronisieren**.

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

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

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

Befolgen Sie die Anweisungen entsprechend der von Ihnen gewählten Methode.

> **Hinweis:**

> Sitzungsstarts können fehlschlagen, wenn derselbe Benutzername für das lokale Konto im Linux VDA und das Konto in AD verwendet wird.

Samba Winbind

Erforderliche Pakete installieren oder aktualisieren

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

Winbind-Daemon für den Start beim Maschinenstart aktivieren

Der Winbind-Daemon muss so konfiguriert werden, dass er beim Maschinenstart gestartet wird:

```
sudo systemctl enable winbind
```

> **Hinweis:**
>
> Stellen Sie sicher, dass sich das Winbind-Skript unter `/etc/init.d` befindet.

Kerberos konfigurieren

Öffnen Sie **/etc/krb5.conf** als Root-Benutzer, und nehmen Sie die folgenden Einstellungen vor:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Einzeldomänen-, Einzelforst-Modell 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**. Der **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. **EXAMPLE.COM**.

Winbind-Authentifizierung konfigurieren

Öffnen Sie **/etc/samba/smb.conf**, und nehmen Sie die folgenden 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-Realm-Name in Großbuchstaben.

nsswitch konfigurieren

Öffnen Sie **/etc/nsswitch.conf**, und fügen Sie `winbind` zu den folgenden Zeilen hinzu:

```
passwd: systemd winbind
```

```
group: systemd winbind
```

Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

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

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

Winbind neu starten

```
sudo systemctl restart winbind
```

PAM für Winbind konfigurieren

Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass die Optionen **Winbind NT/Active Directory-Authentifizierung** und **Home-Verzeichnis bei Anmeldung erstellen** ausgewählt sind:

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

Tipp:

Der `winbind`-Daemon läuft nur, wenn die Maschine einer Domäne beigetreten ist.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in Active Directory haben.

Führen Sie den Befehl **net ads** von Samba aus, um zu überprüfen, ob die Maschine einer Domäne beigetreten ist:

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

Kerberos-Konfiguration überprüfen

Um zu überprüfen, ob Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, vergewissern Sie sich, dass die Systemdatei **keytab** erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der Schlüssel an, die für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um den Computer mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Der Computer- und Realmname muss in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Computerkonto zwischengespeichert wurde, mit:

```
sudo klist
```

Überprüfen Sie die Kontodetails des Computers mit:

```
sudo net ads status
```

Benutzerauthentifizierung überprüfen

Verwenden Sie das Tool **wbinfo**, um zu überprüfen, ob Domänenbenutzer sich bei der Domäne authentifizieren können:

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

Die hier angegebene Domäne ist der AD-Domänenname, nicht der Kerberos-Realm-Name. Für die Bash-Shell muss der Backslash (\\) mit einem weiteren Backslash maskiert werden. Dieser Befehl gibt eine Meldung zurück, die den Erfolg oder Misserfolg anzeigt.

Um zu überprüfen, ob das Winbind PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u
```

Hinweis:

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

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die von dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

Ein ähnlicher Test kann durchgeführt werden, indem 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, Sie aber Ihren Desktop nicht anzeigen können, wenn Sie sich mit einem Domänenkonto anmelden, starten Sie den Computer neu und versuchen Sie es dann erneut.

Quest-Authentifizierungsdienst

Quest auf dem Domänencontroller konfigurieren

Gehen Sie davon aus, dass Sie die Quest-Software auf den Active Directory-Domänencontrollern installiert und konfiguriert haben und über administrative Berechtigungen zum Erstellen von Computerobjekten in Active Directory verfügen.

Domänenbenutzern die Anmeldung an Linux-VDA-Maschinen ermöglichen

Um Domänenbenutzern das Herstellen von HDX™-Sitzungen auf einer Linux-VDA-Maschine zu ermöglichen:

1. Öffnen Sie in der Verwaltungskonsole „Active Directory-Benutzer und -Computer“ die Active Directory-Benutzereigenschaften für dieses Benutzerkonto.
2. Wählen Sie die Registerkarte **Unix-Konto** aus.
3. Aktivieren Sie **Unix-fähig**.
4. Legen Sie die **Primäre GID-Nummer** auf die Gruppen-ID einer tatsächlichen Domänenbenutzergruppe fest.

Hinweis:

Diese Anweisungen sind gleichwertig für die Einrichtung von Domänenbenutzern zur Anmeldung über die Konsole, RDP, SSH oder jedes andere Remoting-Protokoll.

Quest auf Linux-VDA konfigurieren

UMGEHUNG DER SELINUX-RICHTLINIENDURCHSETZUNG

Die Standard-RHEL-Umgebung hat SELinux vollständig erzwungen. Diese Erzwingung stört die von Quest verwendeten IPC-Mechanismen für Unix-Domänensockets und verhindert, dass Domänenbenutzer sich anmelden können.

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

`SELINUX=disabled`

Diese Änderung erfordert einen Neustart der Maschine:

```
reboot
```

Wichtig:

Verwenden Sie diese Einstellung mit Vorsicht. Das erneute Aktivieren der SELinux-Richtlinienerzwingung nach der Deaktivierung kann zu einer vollständigen Sperrung führen, selbst für den Root-Benutzer und andere lokale Benutzer.

VAS-DAEMON KONFIGURIEREN

Die automatische Verlängerung von Kerberos-Tickets muss aktiviert und getrennt werden. Die Authentifizierung (Offline-Anmeldung) muss deaktiviert werden:

```
sudo /opt/quest/bin/vastool configure vas vasd auto-ticket-renew-interval
32400



sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth
false
```

Dieser Befehl setzt das Verlängerungsintervall auf neun Stunden (32.400 Sekunden), was eine Stunde weniger ist als die standardmäßige Ticket-Lebensdauer von 10 Stunden. Legen Sie diesen Parameter auf Systemen mit einer kürzeren Ticket-Lebensdauer auf einen niedrigeren Wert fest.

PAM UND NSS KONFIGURIEREN

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

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

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

Windows-Domäne beitreten

Fügen Sie die Linux-Maschine mit dem Quest-Befehl `vastool` der Active Directory-Domäne hinzu:

```
sudo /opt/quest/bin/vastool -u user join domain-name
```

Der Benutzer ist ein beliebiger Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne. Der Domänenname ist der DNS-Name der Domäne, z. B. example.com.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in Active Directory haben. So überprüfen Sie, ob eine mit Quest verbundene Linux-Maschine in der Domäne ist:

```
sudo /opt/quest/bin/vastool info domain
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl den Domänennamen zurück. Wenn die Maschine keiner Domäne beigetreten ist, wird der folgende Fehler 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 zu überprüfen, ob Quest Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux-VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die UID erstellt wurde, die vom Befehl **id -u** zurückgegeben wird:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache gültig und nicht abgelaufen sind:

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

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Centrify DirectControl

Windows-Domäne beitreten

Nach der Installation des Centrify DirectControl Agents fügen Sie die Linux-Maschine der Active Directory-Domäne mithilfe des Centrify-Befehls `adjoin` hinzu:

```
su –

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

Der Parameter **user** ist ein beliebiger Active Directory-Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne. Der Parameter **domain-name** ist der Name der Domäne, der die Linux-Maschine hinzugefügt werden soll.

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine mit Centrify verbundene Linux-Maschine in der Domäne ist:

```
su –



adinfo
```

Überprüfen Sie, ob der Wert **Joined to domain** gültig ist und der **CentrifyDC mode** den Status **connected** zurückgibt. Wenn der Modus im Startzustand hängen bleibt, treten beim Centrify-Client Probleme mit der Serververbindung oder Authentifizierung auf.

Umfassendere System- und Diagnoseinformationen sind verfügbar mit:

```
adinfo --sysinfo all



adinfo --diag
```

Testen Sie die Konnektivität zu den verschiedenen Active Directory- und Kerberos-Diensten.

```
adinfo --test
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

SSSD

Kerberos konfigurieren

Führen Sie den folgenden Befehl aus, um Kerberos zu installieren:

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

Um Kerberos zu konfigurieren, öffnen Sie **/etc/krb5.conf** als Root und legen Sie die Parameter fest:

> **Hinweis:**

> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Einzeldomänen-, Einzelforst-Modell 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. Der *REALM* ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM.

Der Domäne beitreten

SSSD muss so konfiguriert werden, dass es Active Directory als Identitätsanbieter und Kerberos zur Authentifizierung verwendet. SSSD bietet jedoch keine AD-Client-Funktionen zum Beitreten zur Domäne und zur Verwaltung der System-Keytab-Datei. Stattdessen können Sie `adcli`, `realmd` oder `Samba` verwenden.

> **Hinweis:**

> Dieser Abschnitt enthält nur Informationen für `adcli` und `Samba`.

- **Wenn Sie adcli verwenden, um der Domäne beizutreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie `adcli`.

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

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

   Entfernen Sie die alte System-Keytab-Datei und treten Sie der Domäne bei mit:

```
su -



rm -rf /etc/krb5.keytab



adcli join domain-dns-name -U user -H hostname-fqdn
```

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

   Die Option **-H** ist erforderlich, damit `adcli` SPN im Format host/hostname-fqdn@REALM generiert, was der Linux VDA benötigt.

3. System-Keytab überprüfen.

   Führen Sie den Befehl `sudo klist -ket` aus, um sicherzustellen, dass die System-Keytab-Datei erstellt wurde.

   Überprüfen Sie, ob der Zeitstempel für jeden Schlüssel mit dem Zeitpunkt übereinstimmt, zu dem die Maschine der Domäne beigetreten ist.

- **Wenn Sie `Samba` verwenden, um der Domäne beizutreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.

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

2. Konfigurieren Sie `Samba`.

   Öffnen Sie **/etc/samba/smb.conf**, und nehmen Sie die folgenden 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-Realm-Name in Großbuchstaben.

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

   Ihr Domänencontroller muss erreichbar sein und Sie müssen über ein Windows-Konto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen.

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

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

SSSD einrichten

Erforderliche Pakete installieren oder aktualisieren:

Installieren Sie die erforderlichen SSSD- und Konfigurationspakete, falls noch nicht geschehen:

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

Sind die Pakete bereits installiert, wird ein Update empfohlen:

```
sudo apt-get install --only-upgrade sssd
```

Hinweis:

> Standardmäßig konfiguriert der Installationsprozess in Ubuntu automatisch **nsswitch.conf** und das PAM-Anmeldemodul.

SSSD konfigurieren

SSSD-Konfigurationsänderungen sind erforderlich, bevor der SSSD-Daemon gestartet wird. Bei einigen SSSD-Versionen ist die Konfigurationsdatei **/etc/sssd/sssd.conf** standardmäßig nicht installiert und muss manuell erstellt werden. Erstellen oder öffnen Sie als Root **/etc/sssd/sssd.conf** und nehmen Sie die folgenden Einstellungen vor:

```
[sssd]
```

```
services = nss, pam
```

```
config_file_version = 2
```

```
domains = domain-dns-name
```

```
[domain/domain-dns-name]
```

```
id_provider = ad
```

```
access_provider = ad
```

```
auth_provider = krb5
```

```
krb5_realm = REALM
```

```
# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days
```

```
krb5_renewable_lifetime = 14d
```

```
# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours
```

```
krb5_renew_interval = 1h
```

```
krb5_ccachedir = /tmp
```

```
krb5_ccname_template = FILE:%d/krb5cc_%U
```

```
# This ldap_id_mapping setting is also the default value
```

```
ldap_id_mapping = true
```

`override_homedir = /home/%d/%u`

`default_shell = /bin/bash`

`ad_gpo_map_remote_interactive = +ctxhdx`

> **Hinweis:**

> ldap_id_mapping ist auf **true** gesetzt, damit SSSD selbst die Zuordnung von Windows-SIDs zu Unix-UIDs übernimmt. Andernfalls muss das Active Directory POSIX-Erweiterungen bereitstellen können. Der PAM-Dienst `ctxhdx` wird zu ad_gpo_map_remote_interactive hinzugefügt.

> Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. example.com. Der **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM. Es ist nicht erforderlich, den NetBIOS-Domänennamen zu konfigurieren.

> Informationen zu den Konfigurationseinstellungen finden Sie in den Manpages für sssd.conf und `sssd-ad`.

> Der SSSD-Daemon erfordert, dass die Konfigurationsdatei nur Leseberechtigungen für den Eigentümer haben darf:

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

SSSD-Daemon starten

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

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

PAM-Konfiguration

Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass die Optionen **SSS-Authentifizierung** und **Home-Verzeichnis bei Anmeldung erstellen** ausgewählt sind:

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben.

- Wenn Sie `adcli` verwenden, um die Domänenmitgliedschaft zu überprüfen, führen Sie den Befehl `sudo adcli info domain-dns-name` aus, um die Domäneninformationen anzuzeigen.
- Wenn Sie `Samba` verwenden, um die Domänenmitgliedschaft zu überprüfen, führen Sie den Befehl `sudo net ads testjoin` aus, um zu überprüfen, ob die Maschine einer Domäne beigetreten ist, und den Befehl `sudo net ads info`, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen.

Kerberos-Konfiguration überprüfen

Um zu überprüfen, ob Kerberos korrekt für die Verwendung mit dem Linux VDA konfiguriert ist, überprüfen Sie, ob die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der Schlüssel an, die für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Die Maschinen- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT für das Maschinenkonto mit Hilfe von: zwischengespeichert wurde.

```
sudo klist
```

Benutzerauthentifizierung überprüfen

SSSD bietet kein Befehlszeilentool zum direkten Testen der Authentifizierung mit dem Daemon, und dies kann nur über PAM erfolgen.

Um zu überprüfen, ob das SSSD PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u



klist



exit
```

Überprüfen Sie, ob die vom Befehl **klist** zurückgegebenen Kerberos-Tickets für diesen Benutzer korrekt sind und nicht abgelaufen sind.

Als Root-Benutzer überprüfen Sie, ob eine entsprechende Ticket-Cache-Datei für die UID erstellt wurde, die vom vorherigen Befehl **id -u** zurückgegeben wurde:

```
ls /tmp/krb5cc_uid
```

Ein ähnlicher Test kann durch Anmelden am KDE oder Gnome Display Manager durchgeführt werden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

Erforderliches PBIS-Paket herunterladen

Zum Beispiel:

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
8.8.0/pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

PBIS-Installationsskript ausführbar machen

Zum Beispiel:

```
sudo chmod +x pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

PBIS-Installationsskript ausführen

Zum Beispiel:

```
sudo sh pbis-open-8.8.0.506.linux.x86_64.deb.sh
```

Windows-Domäne beitreten

Ihr Domänencontroller muss erreichbar sein und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
```

Der **Benutzer** ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne besitzt. Der **Domänenname** ist der DNS-Name der Domäne, zum Beispiel example.com.

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

Domänenmitgliedschaft überprüfen

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine PBIS-verbundene Linux-Maschine in der Domäne ist:

```
/opt/pbis/bin/domainjoin-cli query
```

Wenn der Computer einer Domäne beigetreten ist, gibt dieser Befehl die Informationen über die aktuell beigetretene AD-Domäne und OU zurück. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen

Um zu überprüfen, ob PBIS Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

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



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die UID erstellt wurde, die vom Befehl **id -u** zurückgegeben wird:

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Schritt 4: Installieren von .NET Core Runtime 3.1 als Voraussetzung

Bevor Sie den Linux VDA installieren, installieren Sie .NET Core Runtime 3.1 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

Nach der Installation von .NET Core Runtime 3.1 führen Sie den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Basierend auf der Befehlsausgabe legen Sie den Binärpfad der .NET Core-Laufzeit fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

Gehen Sie zur Downloadseite von Citrix Virtual Apps and Desktops™. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um das Linux VDA-Paket herunterzuladen, das Ihrer Linux-Distribution entspricht.

Schritt 6: Installieren des Linux VDA

Schritt 6a: Installieren des Linux VDA

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

```
sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
```

Debian-Abhängigkeitsliste für Debian 10.7:

```
ibus                    >= 1.5

postgresql              >= 11

libpostgresql-jdbc-java >= 42.2

openjdk-11-jdk           >= 11

imagemagick             >= 8:6.9.10

ufw                     >= 0.36

desktop-base            >= 10.0.2

libxrandr2              >= 2:1.5.1

libxtst6                >= 2:1.2.3

libxm4                  >= 2.3.8

util-linux              >= 2.33

gtk3-nocsd              >= 3

bash                    >= 5.0

findutils               >= 4.6.0
```

```
sed                     >= 4.7

cups                    >= 2.2

ghostscript             >= 9.27~

libmspack0              >= 0.10

libgoogle-perftools4    >= 2.7~

libpython2.7            >= 2.7~

libsasl2-modules-gssapi-mit >= 2.1.~
```

Hinweis:

Eine Matrix der Linux-Distributionen und Xorg-Versionen, die diese Version des Linux VDA unterstützt, finden Sie unter Systemanforderungen.

Schritt 6b: Linux VDA aktualisieren (optional)

Sie können eine vorhandene Installation von den beiden vorherigen Versionen und von einer LTSR-Version aktualisieren.

```
sudo dpkg -i <PATH>/<Linux VDA deb>
```

Hinweis:

Beim Upgrade einer vorhandenen Installation werden die Konfigurationsdateien unter /etc/xdl überschrieben. Sichern Sie die Dateien, bevor Sie ein Upgrade durchführen.

Schritt 7: Linux VDA konfigurieren

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Bevor Änderungen vorgenommen werden, überprüft das Skript die

Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Bei Bedarf können Sie das Skript jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell mit Eingabeaufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript, bevor Sie fortfahren:

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

Konfiguration mit Eingabeaufforderungen

Führen Sie eine manuelle Konfiguration mit Fragen durch:

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

Automatisierte Konfiguration

Für eine automatisierte Installation können die vom Setup-Skript benötigten Optionen über Umgebungsvariablen bereitgestellt werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript den Benutzer nicht zur Eingabe von Informationen auf, was einen skriptgesteuerten Installationsprozess ermöglicht.

Unterstützte Umgebungsvariablen sind:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags. Standardmäßig auf N festgelegt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste von Delivery Controller-FQDNs (Fully Qualified Domain Names) zur 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, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux Virtual Desktop-Dienste werden nach dem Start der Maschine gestartet. Standardmäßig auf Y eingestellt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux Virtual Desktop-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) automatisch in der System-Firewall für den Linux Virtual Desktop öffnen. Standardmäßig auf Y eingestellt.

- **CTX_XDL_AD_INTEGRATION=1 \| 2 \| 3 \| 4 \|5** – Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das installierte und konfigurierte Active Directory-Integrationstool auf dem System bestimmt. Geben Sie die zu verwendende unterstützte Active Directory-Integrationsmethode an:
  - 1 – Samba Winbind
  - 2 – Quest Authentication Service
  - 3 – Centrify DirectControl
  - 4 – SSSD
  - 5 – PBIS
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung von grafikintensiven Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für den VDI-Desktop-Modus (Einzelsitzung) konfiguriert – (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Ob die Maschine als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie diese Variable auf Y. Diese Variable ist standardmäßig auf N eingestellt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf einen lokalen Standort zu beschränken, geben Sie einen DNS-Standortnamen an. Diese Variable ist standardmäßig auf **\<none\>** eingestellt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum Beispiel ad1.mycompany.com:389. Diese Variable ist standardmäßig auf **\<none\>** eingestellt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com) gesetzt ist. Um die Suchleistung zu verbessern, können Sie jedoch eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** eingestellt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, aber Sie können stattdessen eine durch Semikolons getrennte Liste

von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen.

- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – Der Pfad zur Installation der .NET Core Runtime 3.1 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/mate** – Gibt die GNOME- oder MATE-Desktop-Umgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

> **Hinweis:**
>
> Sie können die Desktop-Umgebung für einen Ziel-Sitzungsbenutzer auch ändern, indem Sie die folgenden Schritte ausführen:
>
> a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.
> b. Bearbeiten Sie die `.xsession`-Datei, um eine Desktop-Umgebung basierend auf den Distributionen anzugeben.
>
> **Für MATE-Desktop unter CentOS, Ubuntu und Debian**
>
> MSESSION="$(type -p mate-session)"
>
> \> wenn ; dann
>
> ```
> exec mate-session
> ```
>
> \> fi
>
> ```
> **Für GNOME-Desktop unter CentOS**
> ```

```
    GSESSION="$(type -p gnome-session)"
```

\> if ; then

```
    export GNOME_SHELL_SESSION_MODE=classic
```

\> exec gnome-session --session=gnome-classic

```
    fi

**Für GNOME-Desktop unter Ubuntu und Debian**



    GSESSION="$(type -p gnome-session)"
```

\> wenn ; dann

```
    exec gnome-session
```

\> fi

a. Teilen Sie die Dateiberechtigung 700 mit dem Ziel-Sitzungsbenutzer.

- **CTX_XDL_START_SERVICE=Y \| N** – Gibt an, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Standardmäßig auf Y gesetzt.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Abhören von 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:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=1|2|3|4|5

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

```
export CTX_XDL_FAS_LIST=‘list-fas-servers’ | '<none>'

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

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | mate | '<none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

Wenn Sie den sudo-Befehl ausführen, geben Sie die Option **-E** ein, um die vorhandenen Umgebungsvariablen an die neue Shell zu übergeben, die er erstellt. Wir empfehlen, dass Sie aus den vorhergehenden Befehlen eine Shell-Skriptdatei mit **#\!/bin/bash** als erster Zeile erstellen.

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

CTX_XDL_DDC_LIST=‘list-ddc-fqdns’ \
```

```
CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=1|2|3|4|5 \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

```
CTX_XDL_DESKTOP_ENVIRONMENT=gnome | mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Konfigurationsänderungen entfernen

In einigen Szenarien müssen Sie möglicherweise die durch das Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernen, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie vor dem Fortfahren die Hilfe zu diesem Skript:

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

So entfernen Sie Konfigurationsänderungen:

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

Wichtig:

Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank und macht den Linux VDA unbrauchbar.

Konfigurationsprotokolle

Die Skripte **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an, wobei zusätzliche Informationen in die Konfigurationsprotokolldatei **/tmp/xdl.configure.log** geschrieben werden.

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

Deinstallieren der Linux VDA-Software

So überprüfen Sie, ob der Linux VDA installiert ist, und um die Version des installierten Pakets anzuzeigen:

```
dpkg -l xendesktopvda
```

So zeigen Sie detailliertere Informationen an:

```
apt-cache show xendesktopvda
```

So deinstallieren Sie die Linux VDA-Software:

```
dpkg -r xendesktopvda
```

Hinweis:

Durch die Deinstallation der Linux VDA-Software werden die zugehörigen PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden jedoch nicht gelöscht.

Tipp:

Die Informationen in diesem Abschnitt behandeln nicht die Entfernung abhängiger Pakete, einschließlich PostgreSQL.

Schritt 8: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um häufige Konfigurationsprobleme in einer Linux-VDA-Umgebung zu überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 9: Linux VDA ausführen

Nachdem Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, verwenden Sie die folgenden Befehle, um den Linux VDA zu steuern.

Linux VDA starten:

So starten Sie die Linux-VDA-Dienste:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Linux VDA beenden:

So beenden Sie die Linux-VDA-Dienste:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

Hinweis:

Bevor Sie die Dienste `ctxvda` und `ctxhdx` beenden, führen Sie den Befehl `service ctxmonitorservice stop` aus, um den Überwachungsdienst-Daemon zu beenden. Andernfalls startet der Überwachungsdienst-Daemon die von Ihnen beendeten Dienste neu.

Linux VDA neu starten:

So starten Sie die Linux-VDA-Dienste neu:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx
```

```
sudo systemctl restart ctxvda
```

Linux-VDA-Status überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux-VDA-Dienste:

```
sudo systemctl status ctxvda
```

```
sudo systemctl status ctxhdx
```

Schritt 10: Maschinenkatalog in Citrix Virtual Apps oder Citrix Virtual Desktops™ erstellen

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux-VDA-Maschinen ähnelt dem traditionellen Windows-VDA-Ansatz. Eine detailliertere Beschreibung zum Ausführen dieser Aufgaben finden Sie unter Maschinenkataloge erstellen und Maschinenkataloge verwalten.

Für die Erstellung von Maschinenkatalogen, die Linux-VDA-Maschinen enthalten, gibt es einige Einschränkungen, die den Prozess von der Erstellung von Maschinenkatalogen für Windows-VDA-Maschinen unterscheiden:

- Wählen Sie für das Betriebssystem Folgendes aus:
  - Die Option **Multi-session OS** für ein Bereitstellungsmodell mit gehosteten, gemeinsam genutzten Desktops.
  - Die Option **Single-session OS** für ein VDI-Bereitstellungsmodell mit dedizierten Desktops.
- Mischen Sie keine Linux- und Windows-VDA-Maschinen im selben Maschinenkatalog.

> **Hinweis:**

> Frühere Versionen von Citrix Studio unterstützten den Begriff „Linux-Betriebssystem“ nicht. Die Auswahl der Option **Windows Server OS** oder **Server OS** impliziert jedoch ein äquivalentes Bereitstellungsmodell für gehostete, gemeinsam genutzte Desktops. Die

> Auswahl der Option **Windows Desktop OS** oder **Desktop OS** impliziert ein Bereitstellungsmodell mit einem Benutzer pro Maschine.

> **Tipp:**
>
> Wenn Sie eine Maschine aus der Active Directory-Domäne entfernen und wieder hinzufügen, müssen Sie die Maschine erneut aus dem Maschinenkatalog entfernen und hinzufügen.

Schritt 11: Erstellen der Bereitstellungsgruppe in Citrix Virtual Apps™ oder Citrix Virtual Desktops

Der Prozess zum Erstellen einer Bereitstellungsgruppe und Hinzufügen von Maschinenkatalogen, die Linux-VDA-Maschinen enthalten, ist nahezu identisch mit dem für Windows-VDA-Maschinen. Eine detailliertere Beschreibung zum Ausführen dieser Aufgaben finden Sie unter Bereitstellungsgruppen erstellen.

Für die Erstellung von Bereitstellungsgruppen, die Linux-VDA-Maschinenkataloge enthalten, gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die von Ihnen ausgewählten AD-Benutzer und -Gruppen ordnungsgemäß für die Anmeldung an den Linux-VDA-Maschinen konfiguriert wurden.
- Lassen Sie die Anmeldung nicht authentifizierter (anonymer) Benutzer nicht zu.
- Mischen Sie die Bereitstellungsgruppe nicht mit Maschinenkatalogen, die Windows-Maschinen enthalten.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2106.

Erstellen von Linux-VDAs in Citrix Virtual Apps and Desktops™ Standard für Azure

Sie können sowohl domänenverbundene als auch nicht domänenverbundene Linux-VDAs in Citrix Virtual Apps and Desktops Standard für Azure erstellen, um virtuelle Apps und Desktops von Microsoft Azure auf jedem Gerät bereitzustellen. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Standard für Azure.

Unterstützte Linux-Distributionen

Die folgenden Linux-Distributionen unterstützen diese Funktion:

- RHEL 8.3
- RHEL 8.2
- RHEL 7.8
- Ubuntu 20.04
- Ubuntu 18.04
- Ubuntu 16.04

Schritte

Führen Sie die folgenden Schritte aus, um Linux-VDAs in Citrix Virtual Apps™ and Desktops Standard für Azure zu erstellen:

1. Bereiten Sie ein Masterimage in Azure vor:

> **Hinweis:**
>
> Sie können auch die Funktion Linux VDA self-update verwenden, um automatische Softwareupdates zu planen. Um dies zu erreichen, fügen Sie Befehlszeilen zur Datei etc/xdl/mcs/mcs_local_setting.reg auf dem Masterimage hinzu. Sie können beispielsweise die folgenden Befehlszeilen hinzufügen:
>
> ```
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"
> -t "REG_DWORD" -v "fEnabled" -d "0x00000001" –force
>
>
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"
> -t "REG_SZ" -v "ScheduledTime" -d "Immediately" –force
>
>
>
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate"
> -t "REG_SZ" -v "Url" -d "<Your-Azure-Container-Url>" –force
>
>
>
> ```

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

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 auf der VM .NET Core Runtime 3.1 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

d. (Nur für Ubuntu) Fügen Sie die Zeile `source /etc/network/interfaces.d/*` zur Datei `/etc/network/interfaces` hinzu.

e. (Nur für Ubuntu) Verweisen Sie `/etc/resolv.conf` auf `/run/systemd/resolve/resolv.conf`, anstatt auf `/run/systemd/resolve/stub-resolv.conf` zu verweisen:

```
unlink /etc/resolv.conf



ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

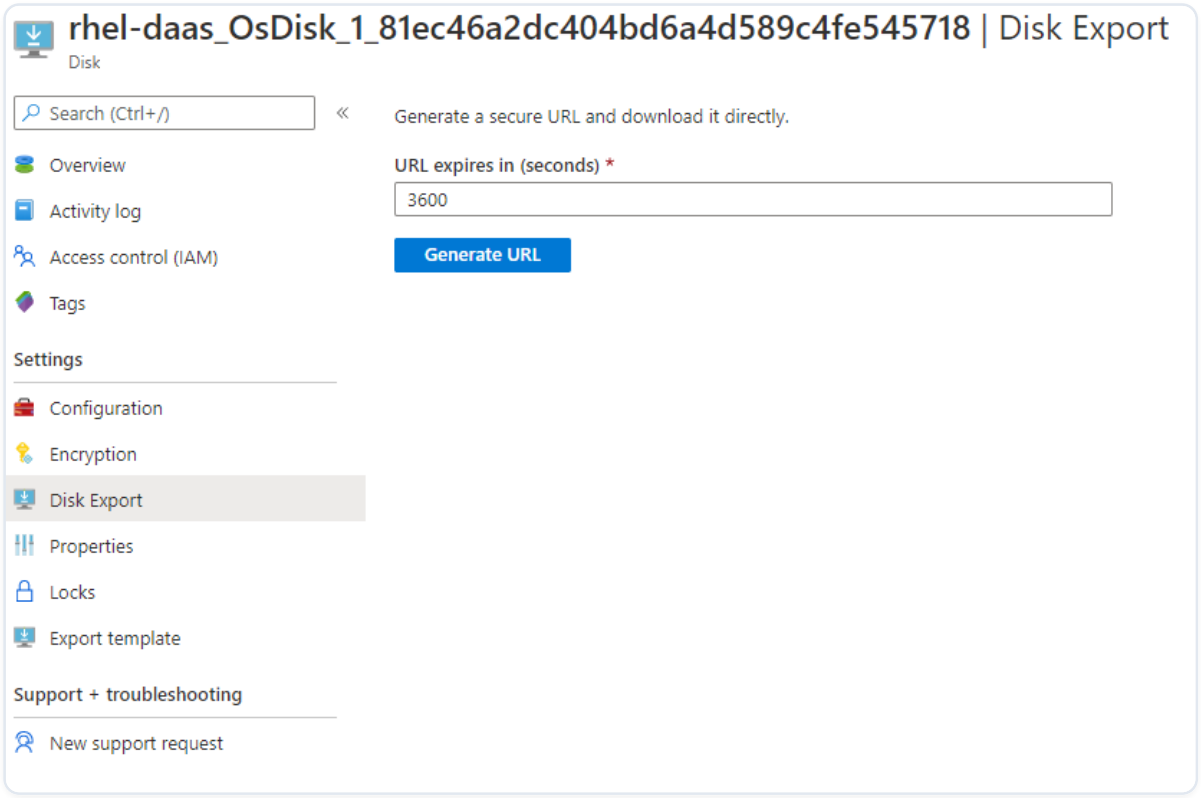
f. Installieren Sie das Linux VDA-Paket.

g. Ändern Sie Variablen in /etc/xdl/mcs/mcs.conf. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Festlegen von MCS und des Linux VDA.

> **Hinweis:**
>
> Lassen Sie die Variable dns unspezifiziert. Wenn Sie beim Erstellen eines Maschinenkatalogs den Typ **Static** oder **Random** auswählen, legen Sie `VDI_MODE=Y` fest.

h. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.

i. Halten Sie in Azure die VM an (oder heben Sie die Zuordnung auf). Klicken Sie auf **Disk Export**, um eine SAS-URL für die VHD-Datei (Virtual Hard Disk) zu generieren, die Sie als Masterimage zum Erstellen weiterer VMs verwenden können.



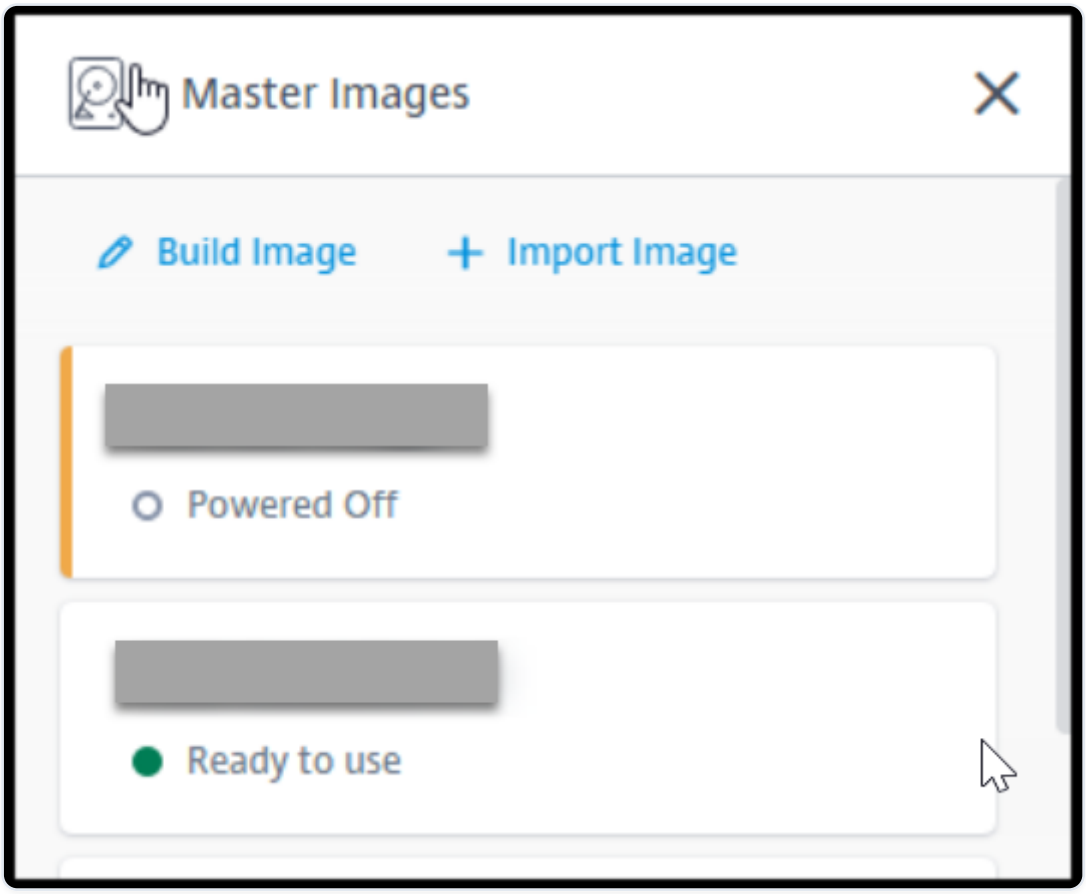
j. (Optional) Nehmen Sie Gruppenrichtlinieneinstellungen am Masterimage vor. Sie können das Tool `ctxreg` verwenden, um Gruppenrichtlinieneinstellungen vorzunehmen. Der folgende Befehl aktiviert beispielsweise die Richtlinie **Auto-create PDF Universal Printer** für den PDF-Druck.

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

2. Importieren Sie das Masterimage aus Azure.

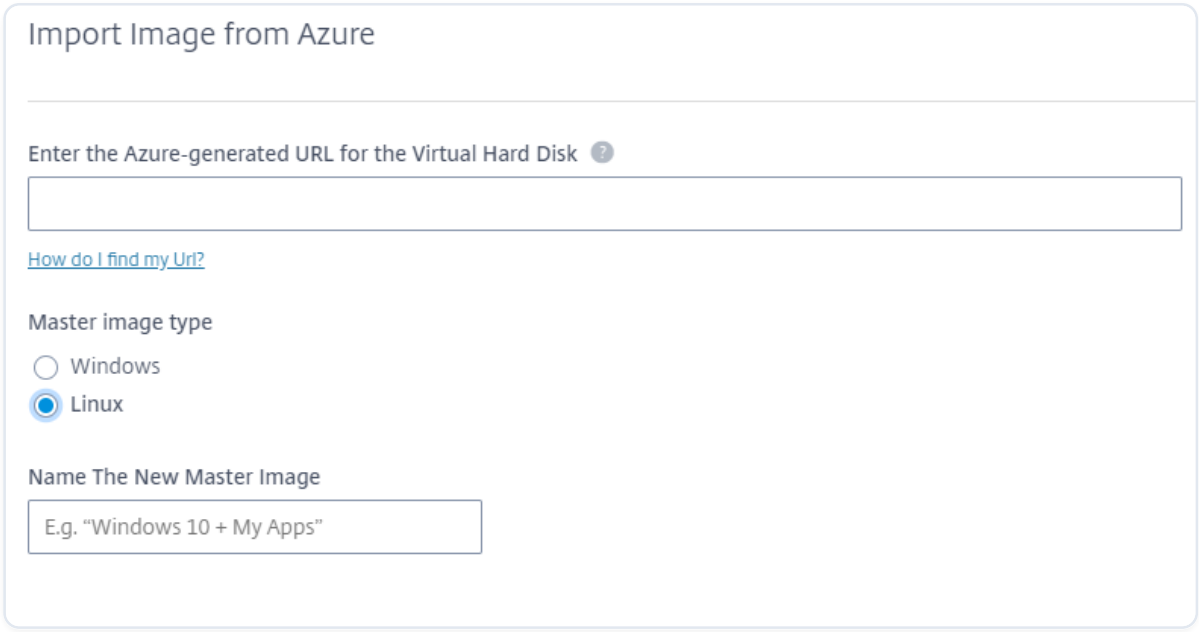
a. Im Verwalten Dashboard, auf der rechten Seite, erweitern Sie **Master Images**. Die Anzeige listet die von Citrix bereitgestellten Master-Images sowie die von Ihnen erstellten und importierten Images auf.

Tipp: Die meisten Administratoraktivitäten für diesen Dienst werden über die Dashboards **Verwalten** und **Überwachen** verwaltet. Nachdem Sie Ihren ersten Katalog erstellt haben, wird das Dashboard **Verwalten** automatisch gestartet, nachdem 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 Masterimage-Typ aus.



d. Befolgen Sie die Anweisungen im Assistenten, um den Import des Master-Images abzuschließen.

3. Erstellen Sie einen Maschinenkatalog.

Greifen Sie auf das Manage-Dashboard zu und klicken Sie auf **Katalog erstellen**. Beim Erstellen des Maschinenkatalogs wählen Sie das zuvor erstellte Master-Image aus.

Hinweis: Sie können nicht in die Domäne eingebundene Linux-Maschinenkataloge nur in einem von Citrix verwalteten Azure-Abonnement erstellen.

Verwenden Sie Machine Creation Services™ (MCS) zum Erstellen von Linux-VMs

Um MCS zum Erstellen von Linux-VMs zu verwenden, bereiten Sie ein Masterimage auf Ihrem Hypervisor vor. Dieser Prozess umfasst die Installation des VDA auf der Vorlagen-VM, das Erstellen eines Maschinenkatalogs in Citrix Studio, das Erstellen einer Bereitstellungsgruppe und die Durchführung bestimmter Konfigurationsaufgaben.

Hinweis:

Unerwartete Ergebnisse können auftreten, wenn Sie versuchen, ein Masterimage auf anderen Hypervisoren als Citrix Hypervisor™, Microsoft Azure, VMware vSphere, AWS, GCP oder Nutanix AHV vorzubereiten.

Microsoft Azure, AWS und GCP werden ab Citrix Virtual Apps and Desktops™ 7 2003 nicht mehr unterstützt. Sie können die Hosts jedoch weiterhin im Citrix Virtual Apps and Desktops-Dienst verwenden.

Unterstützte Distributionen

	WINBIND	SSSD	CENTRIFY	PBIS
RHEL 8.4	Ja	Nein	Ja	Ja
CentOS 8 (2105)	Ja	Nein	Ja	Ja
RHEL 8.3	Ja	Nein	Ja	Ja
CentOS 8.3	Ja	Nein	Ja	Ja
RHEL 8.2	Ja	Nein	Ja	Ja

	WINBIND	SSSD	CENTRIFY	PBIS
CentOS 8.2	Ja	Nein	Ja	Ja
RHEL 8.1	Ja	Nein	Ja	Ja
CentOS 8.1	Ja	Nein	Ja	Ja
RHEL 7.9	Ja	Ja	Ja	Ja
CentOS 7.9	Ja	Ja	Ja	Ja
RHEL 7.8	Ja	Ja	Ja	Ja
CentOS 7.8	Ja	Ja	Ja	Ja
Ubuntu 20.04	Ja	Ja	Nein	Ja
Ubuntu 18.04	Ja	Ja	Nein	Ja
Ubuntu 16.04	Ja	Ja	Nein	Ja
Debian 10.7	Ja	Ja	Nein	Ja
SUSE 12.5	Ja	Ja	Nein	Ja

Hinweis:

Wenn Sie PBIS oder Centrify verwenden, um von MCS erstellte Maschinen Windows-Domänen beizutreten, führen Sie die folgenden Aufgaben aus:

- Konfigurieren Sie auf der Vorlagenmaschine den Downloadpfad des PBIS- oder Centrify-Pakets in der Datei `/etc/xdl/mcs/mcs.conf` oder installieren Sie das PBIS- oder Centrify-Paket direkt.
- Bevor Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` ausführen, erstellen Sie eine Organisationseinheit (OU), die Schreib- und Kennwortrücksetzberechtigungen für alle ihre untergeordneten, von MCS erstellten Maschinen hat.

- Bevor Sie von MCS erstellte Maschinen neu starten, nachdem `/opt/Citrix/VDA/sbin/deploymcs.sh` ausgeführt wurde, führen Sie `klist -li 0x3e4 purge` auf Ihrem Delivery Controller oder auf Ihrem Citrix Cloud Connector aus, basierend auf Ihrer Bereitstellung.

Verwenden Sie MCS zum Erstellen von Linux-VMs auf Citrix Hypervisor

Schritt 1: Masterimage vorbereiten

Ein Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, VDA und andere Software. Gehen Sie wie folgt vor, um ein Masterimage vorzubereiten:

Schritt 1a: Citrix VM Tools installieren

Installieren Sie die Citrix VM Tools auf der Vorlagen-VM, damit jede VM die xe-CLI oder XenCenter verwenden kann. Die VM-Leistung kann langsam sein, wenn Sie die Tools nicht installieren. Ohne die Tools können Sie Folgendes nicht tun:

- Eine VM sauber herunterfahren, neu starten oder anhalten.
- Die VM-Leistungsdaten in XenCenter anzeigen.
- Eine laufende VM migrieren (über `XenMotion`).
- Snapshots oder Snapshots mit Speicher (Checkpoints) erstellen und zu Snapshots zurückkehren.
- Die Anzahl der vCPUs auf einer laufenden Linux-VM anpassen.

1. Führen Sie den folgenden Befehl aus, um die Citrix VM Tools namens guest-tools.iso bereitzustellen.

   ```
   sudo mount /dev/cdrom /mnt
   ```

2. Führen Sie den folgenden Befehl aus, um das `xe-guest-utilities`-Paket basierend auf Ihrer Linux-Distribution zu installieren.

   Für RHEL/CentOS:

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

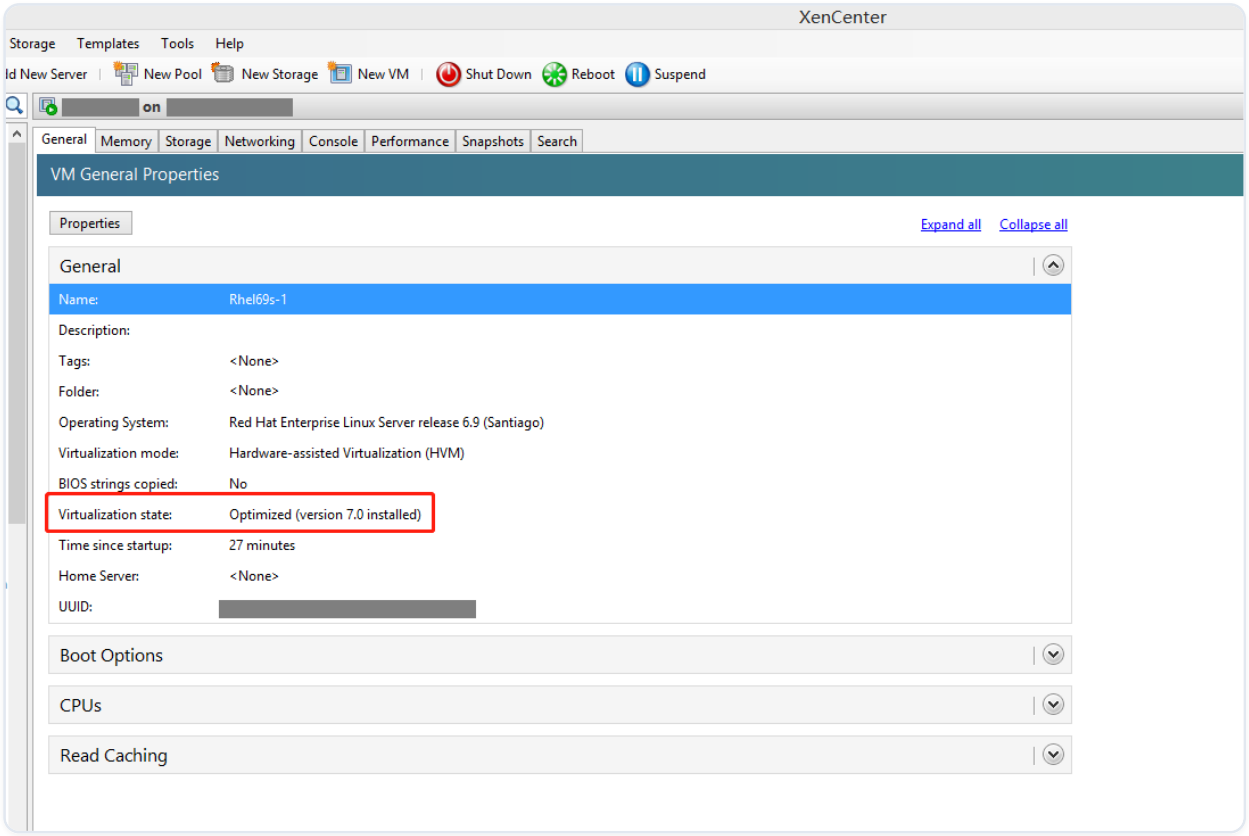
   Für Ubuntu/Debian:

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

Für SUSE 12:

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

3. Überprüfen Sie den Virtualisierungsstatus der Vorlagen-VM auf der Registerkarte **Allgemein** in XenCenter. Wenn die Citrix VM Tools korrekt installiert sind, lautet der Virtualisierungsstatus **Optimiert**:



Schritt 1b: (Nur für Ubuntu 16.04) OpenJDK 11 installieren

Unter Ubuntu 16.04 installieren Sie OpenJDK 11, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das neueste OpenJDK 11 von `<https://jdk.java.net/archive/>` herunter.
2. Führen Sie den Befehl `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` aus, um das heruntergeladene Paket zu entpacken.
3. (Optional) Führen Sie den Befehl `mv jdk-11.0.2/ <target directory>` aus, um OpenJDK in einem Zielverzeichnis zu speichern.
4. Führen Sie den Befehl `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` aus, um die Java-Laufzeitumgebung einzurichten.

5. Führen Sie den Befehl `java -version` aus, um die Java-Version zu überprüfen.

Schritt 1c: Installieren Sie das Linux VDA-Paket auf der Vorlagen-VM

> **Hinweis:**

> Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden möchten, überspringen Sie diesen Schritt.

> Bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Core Runtime 3.1. Weitere Informationen finden Sie unter Installationsübersicht.

> Führen Sie je nach Linux-Distribution den folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

Für RHEL/CentOS:

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

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE 12:

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

Schritt 1d: Repositorys aktivieren, um das tdb-tools-Paket zu installieren

Für RHEL 7-Server:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

Für RHEL 7-Workstation:

```
subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

Schritt 1e: EPEL-Repository installieren, das ntfs-3g bereitstellen kann

Installieren Sie das EPEL-Repository unter RHEL 8/CentOS 8, RHEL 7/CentOS 7, damit bei der späteren Ausführung von deploymcs.sh das im EPEL-Repository verfügbare ntfs-3g-Paket installiert wird.

Schritt 1f: ntfs-3g unter SUSE 12 manuell installieren

Auf der SUSE 12-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC)-Compilersystem und das make-Paket:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

   ```
   ./configure

   make

   make install
   ```

Schritt 1g: Laufzeitumgebung einrichten

Führen Sie vor der Ausführung von `deploymcs.sh` Folgendes aus:

- Ändern Sie Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Festlegen von MCS und des Linux VDA. Die folgenden Variablen können Sie nach Bedarf festlegen:
  - `Use_Existing_Configurations_Of_Current_VDA`: Legt fest, ob die vorhandenen Konfigurationen des aktuell ausgeführten VDA verwendet werden sollen. Wenn auf Y gesetzt, sind die Konfigurationsdateien auf MCS-erstellten Maschinen identisch mit den entsprechenden Dateien auf dem aktuell ausgeführten VDA. Sie müssen jedoch weiterhin die Variablen `dns` und `AD_INTEGRATION` konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsvorlagen auf dem Masterimage die Konfigurationsdateien auf MCS-erstellten Maschinen bestimmen.
  - `dns`: Legt die DNS-IP-Adresse fest.
  - `AD_INTEGRATION`: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der von MSC unterstützten Linux-Distributionen und Domänenbeitrittsmethoden finden Sie unter Unterstützte Distributionen in diesem Artikel.
  - `CENTRIFY_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
  - `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
  - `WORKGROUP`: Legt den Arbeitsgruppennamen (Groß-/Kleinschreibung beachten) fest, wenn Sie ihn in AD konfiguriert haben.
- Fügen Sie auf der Vorlagenmaschine Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` 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 bereitgestellten Maschine.

  Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

  Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 1h: Masterimage erstellen

1. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
2. (Optional) Aktualisieren Sie auf der Vorlagen-VM die Konfigurationsvorlagen, um die relevanten Dateien `/etc/krb5.conf`, `/etc/samba/smb.conf` und `/etc/sssd/sssd.conf` auf allen erstellten VMs anzupassen.

   Aktualisieren Sie für Winbind-Benutzer die Vorlagen `/etc/xdl/mcs/winbind_krb5.conf.tmpl` und `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

   Aktualisieren Sie für SSSD-Benutzer die Vorlagen `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` und `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

   Aktualisieren Sie für Centrify-Benutzer die Vorlagen `/etc/xdl/mcs/centrify_krb5.conf.tmpl` und `/etc/xdl/mcs/centrify_smb.conf.tmpl`.

   Hinweis:

   Behalten Sie das vorhandene Format in den Vorlagendateien bei und verwenden Sie Variablen wie $WORKGROUP, $REALM, $realm, ${new_hostname} und $AD_FQDN.

3. Fahren Sie auf Citrix Hypervisor die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages.

Schritt 2: Maschinenkatalog erstellen

Erstellen Sie in Citrix Studio einen Maschinenkatalog und geben Sie die Anzahl der im Katalog zu erstellenden VMs an. Führen Sie bei Bedarf weitere Konfigurationsaufgaben durch. Weitere Informationen finden Sie unter Maschinenkatalog mit Studio erstellen.

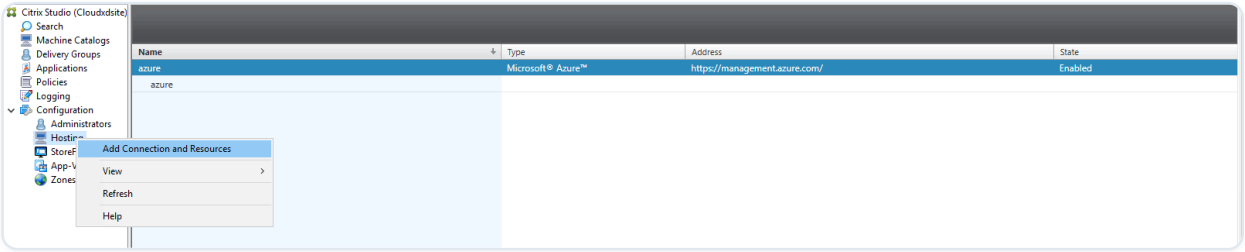
Schritt 3: Eine Bereitstellungsgruppe erstellen

Ein Maschinenkatalog ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Der Maschinenkatalog legt fest, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

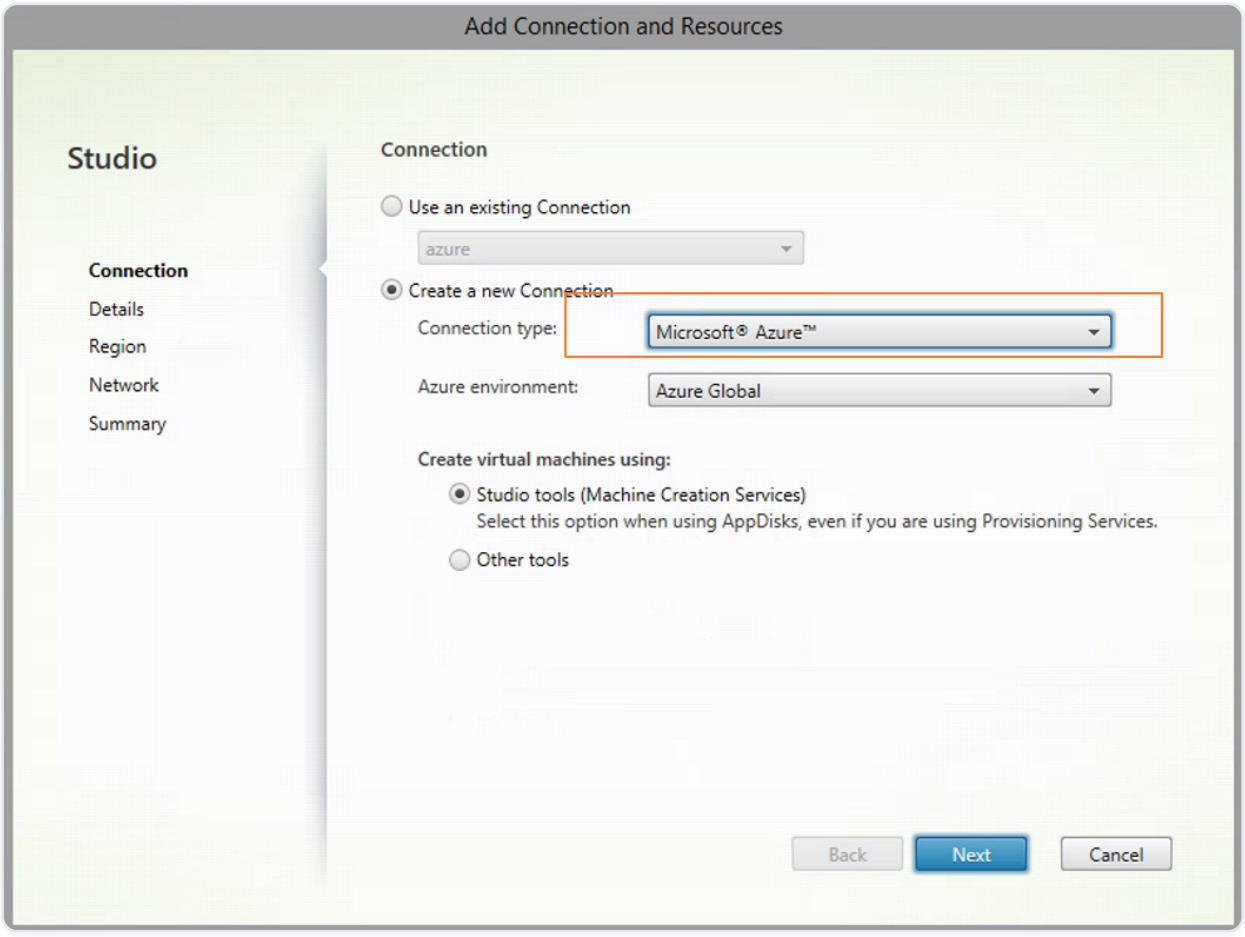
MCS zum Erstellen von Linux-VMs in Azure verwenden

Schritt 1: Eine Hosting-Verbindung zu Azure in Citrix Studio erstellen

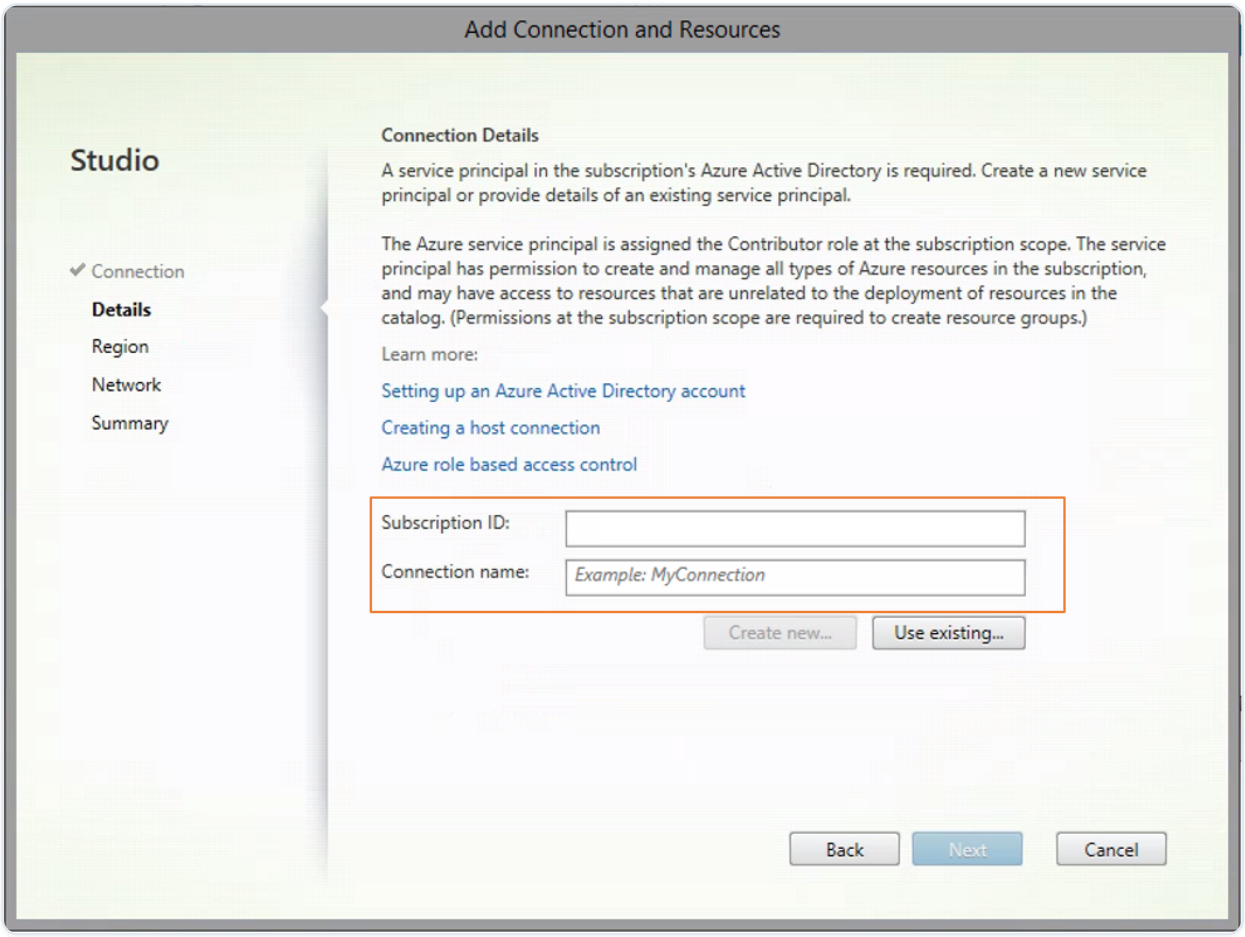
1. Wählen Sie in Citrix Studio in Citrix Cloud™ **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu Azure zu erstellen.



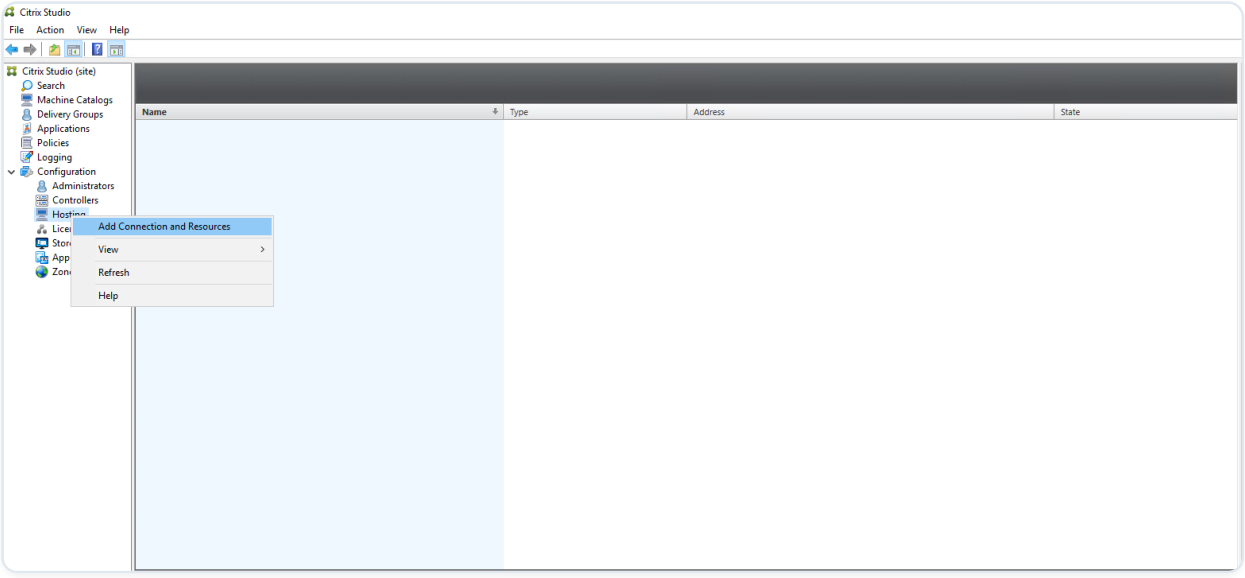
2. Wählen Sie Microsoft Azure als Verbindungstyp.



3. Geben Sie die Abonnement-ID Ihres Azure-Kontos und Ihren Verbindungsnamen ein.



Eine neue Verbindung wird im Hosting-Bereich angezeigt.



Schritt 2: Ein Masterimage auf der Vorlagen-VM vorbereiten

Ein Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, den VDA und andere Software. Gehen Sie wie folgt vor, um ein Masterimage vorzubereiten:

Schritt 2a: cloud-init für Ubuntu 18.04 konfigurieren

Um sicherzustellen, dass ein VDA-Hostname beim Neustart oder Herunterfahren einer VM erhalten bleibt, führen Sie den folgenden Befehl aus.

```
echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
```

Stellen Sie sicher, dass die folgenden Zeilen im Abschnitt **system_info** in der Datei /etc/cloud/cloud.cfg vorhanden sind:

```
system_info:

   network:

       renderers: ['netplan', 'eni', 'sysconfig']
```

Schritt 2b: (Nur für Ubuntu 16.04) OpenJDK 11 installieren

Installieren Sie unter Ubuntu 16.04 OpenJDK 11, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das neueste OpenJDK 11 von `<https://jdk.java.net/archive/>` herunter.
2. Führen Sie den Befehl `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` aus, um das heruntergeladene Paket zu entpacken.
3. (Optional) Führen Sie den Befehl `mv jdk-11.0.2/ <target directory>` aus, um OpenJDK in einem Zielverzeichnis zu speichern.
4. Führen Sie den Befehl `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` aus, um die Java-Laufzeitumgebung einzurichten.
5. Führen Sie den Befehl `java -version` aus, um die Java-Version zu überprüfen.

Schritt 2c: Das Linux VDA-Paket auf der Vorlagen-VM installieren

> **Hinweis:**
>
> Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden möchten, überspringen Sie diesen Schritt.

> Bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Core Runtime 3.1. Weitere Informationen finden Sie unter Installationsübersicht.

> Führen Sie je nach Linux-Distribution den folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

Für RHEL/CentOS:

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

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE 12:

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

Schritt 2d: Installieren Sie das EPEL-Repository, das ntfs-3g bereitstellen kann

Installieren Sie das EPEL-Repository auf RHEL 8/CentOS 8, RHEL 7/CentOS 7, damit deploymcs.sh später das im EPEL-Repository verfügbare ntfs-3g-Paket installiert.

Schritt 2e: ntfs-3g manuell auf SUSE 12 installieren

Auf der SUSE 12-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

1. Installieren Sie das Compiler-System GNU Compiler Collection (GCC) und das make-Paket:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

```
./configure

make

make install
```

Schritt 2f: Die Laufzeitumgebung einrichten

Führen Sie vor dem Ausführen von `deploymcs.sh` Folgendes aus:

- Ändern Sie Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Festlegen von MCS und des Linux VDA. Im Folgenden sind einige der Variablen aufgeführt, von denen `dns` und `AD_INTEGRATION` festgelegt werden müssen:

  Hinweis: Wenn eine Variable mit mehreren Werten festgelegt werden kann, setzen Sie die Werte in einfache Anführungszeichen und trennen Sie sie durch Leerzeichen. Beispiel: LDAP_LIST='aaa.lab:389 bbb.lab:389'.

  - `Use_Existing_Configurations_Of_Current_VDA`: Legt fest, ob die vorhandenen Konfigurationen des aktuell ausgeführten VDA verwendet werden sollen. Wenn auf Y gesetzt, sind die Konfigurationsdateien auf MCS-erstellten Maschinen dieselben wie die entsprechenden Dateien auf dem aktuell ausgeführten VDA. Sie müssen jedoch weiterhin die Variablen `dns` und `AD_INTEGRATION` konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsvorlagen auf dem Masterimage die Konfigurationsdateien auf MCS-erstellten Maschinen bestimmen.
  - `dns`: Legt die DNS-IP-Adresse fest.
  - `AD_INTEGRATION`: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der von MSC unterstützten Linux-Distributionen und Domänenbeitrittsmethoden finden Sie unter Unterstützte Distributionen in diesem Artikel.

  - `CENTRIFY_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
  - `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
  - `WORKGROUP`: Legt den Arbeitsgruppennamen (Groß-/Kleinschreibung beachten) fest, wenn Sie ihn in AD konfiguriert haben.

- Fügen Sie auf der Vorlagenmaschine Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzu, um Registrierungswerte nach Bedarf zu schreiben oder zu aktualisieren. Diese Aktion verhindert den Verlust von Daten und Einstellungen bei jedem Neustart einer MCS-bereitgestellten Maschine.

  Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

  Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 2g: Masterimage erstellen

1. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
2. (Optional) Aktualisieren Sie auf der Vorlagen-VM die Konfigurationsvorlagen, um die relevanten Dateien `/etc/krb5.conf`, `/etc/samba/smb.conf` und `/etc/sssd/sssd.conf` auf allen erstellten VMs anzupassen.

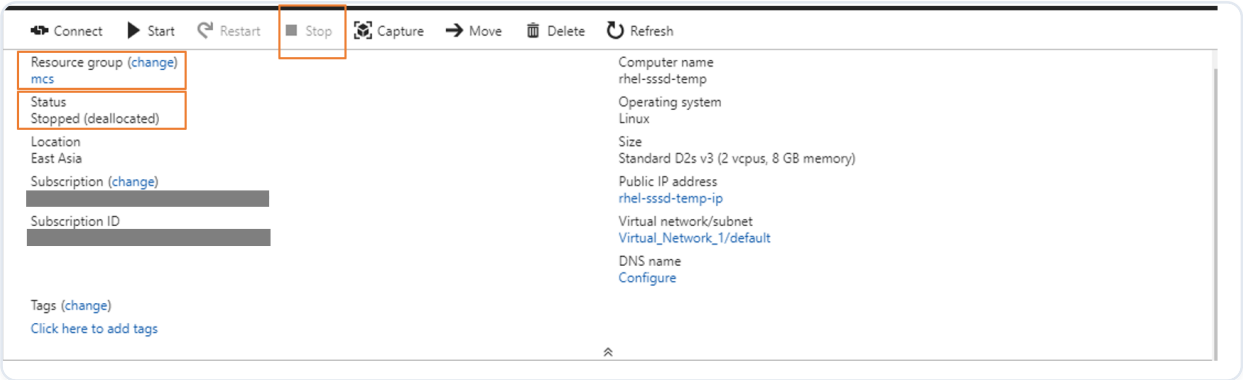
   Für Winbind-Benutzer aktualisieren Sie die Vorlagen `/etc/xdl/mcs/winbind_krb5.conf.tmpl` und `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

Für SSSD-Benutzer aktualisieren Sie die Vorlagen `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` und `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

Aktualisieren Sie für Centrify-Benutzer die `/etc/xdl/mcs/centrify_krb5.conf.tmpl`- und `/etc/xdl/mcs/centrify_smb.conf.tmpl`-Vorlagen.

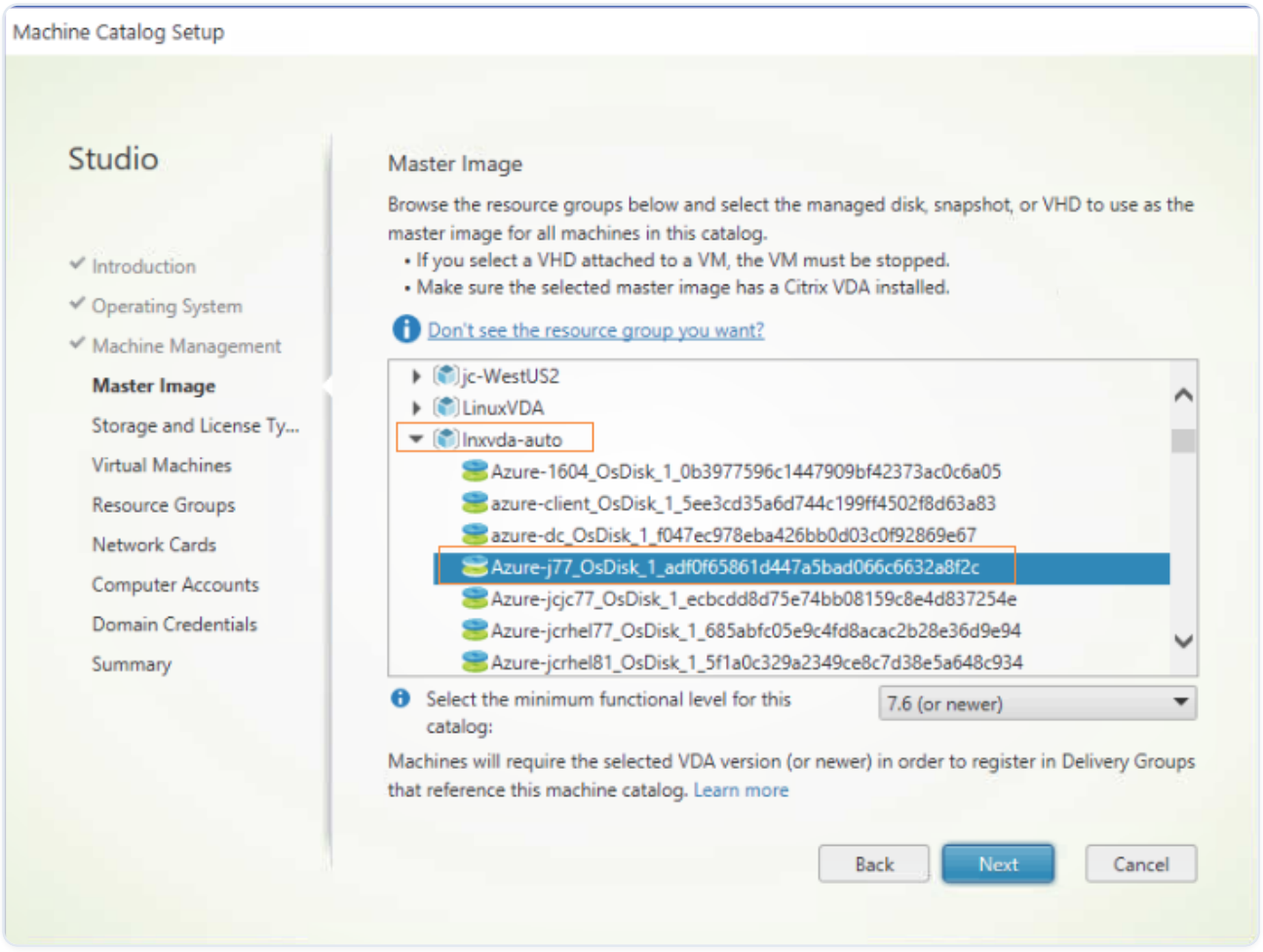
Hinweis: Behalten Sie das vorhandene Format in den Vorlagendateien bei und verwenden Sie Variablen wie $WORKGROUP, $REALM, $realm, ${new_hostname} und $AD_FQDN.

3. Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM über das Azure-Portal herunter. Stellen Sie sicher, dass der Energiestatus der Vorlagen-VM **Beendet (Zuordnung aufgehoben)** ist. Merken Sie sich hier den Namen der Ressourcengruppe. Sie benötigen den Namen, um Ihr Masterimage in Azure zu finden.



Schritt 3: Maschinenkatalog erstellen

Erstellen Sie in Citrix Studio einen Maschinenkatalog und geben Sie die Anzahl der im Katalog zu erstellenden VMs an. Wählen Sie beim Erstellen des Maschinenkatalogs Ihr Masterimage aus der Ressourcengruppe aus, zu der die Vorlagen-VM gehört, und suchen Sie die VHD der Vorlagen-VM.



Führen Sie bei Bedarf weitere Konfigurationsaufgaben aus. Weitere Informationen finden Sie unter Erstellen eines Maschinenkatalogs mit Studio.

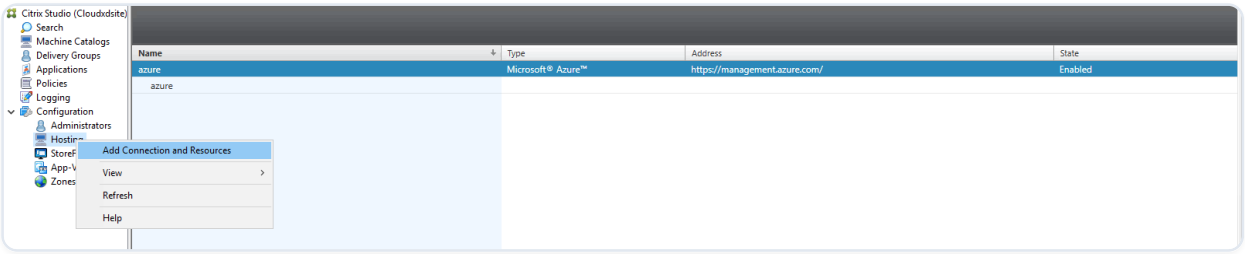
Schritt 4: Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Die Bereitstellungsgruppe gibt an, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

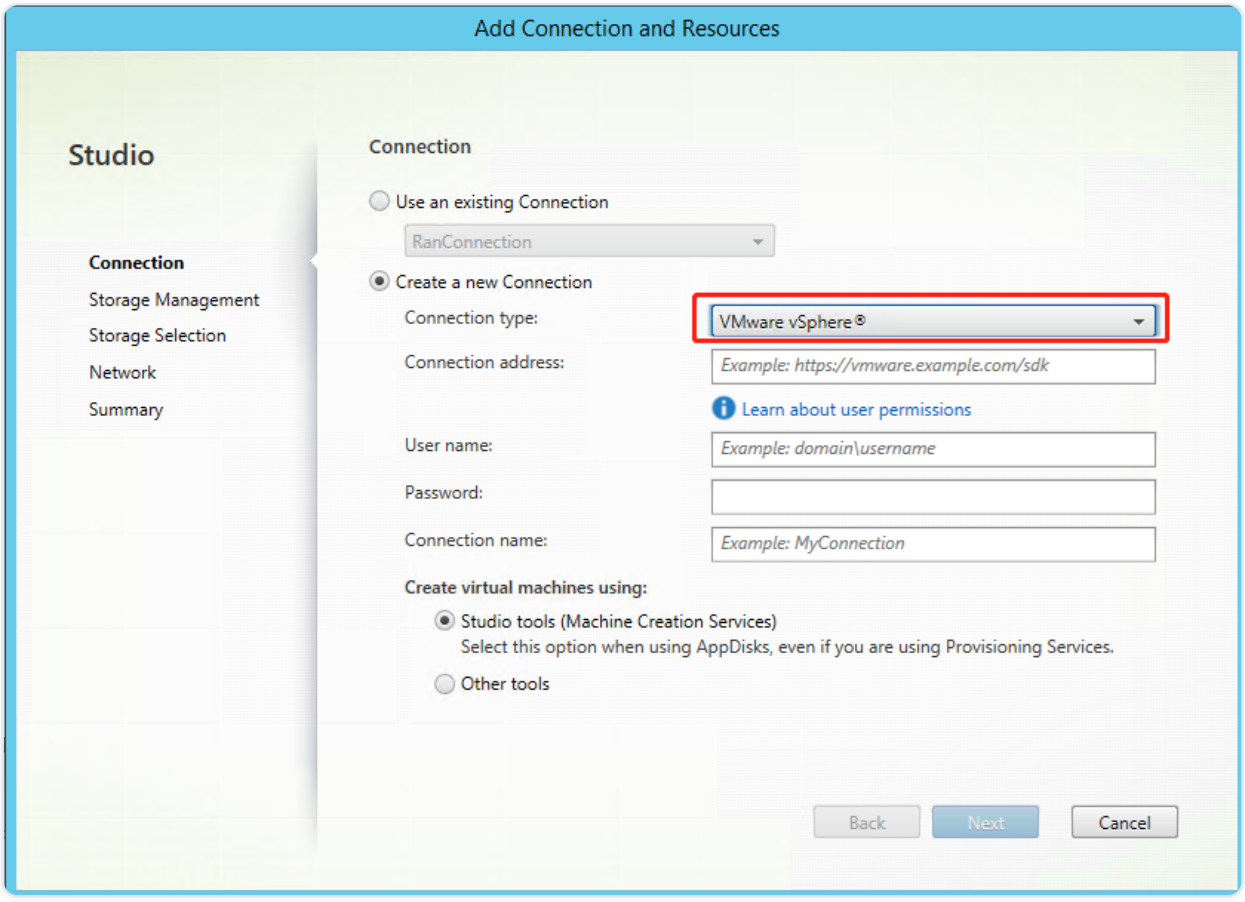
MCS zum Erstellen von Linux-VMs auf VMware vSphere verwenden

Schritt 1: Hostingverbindung zu VMware in Citrix Studio erstellen

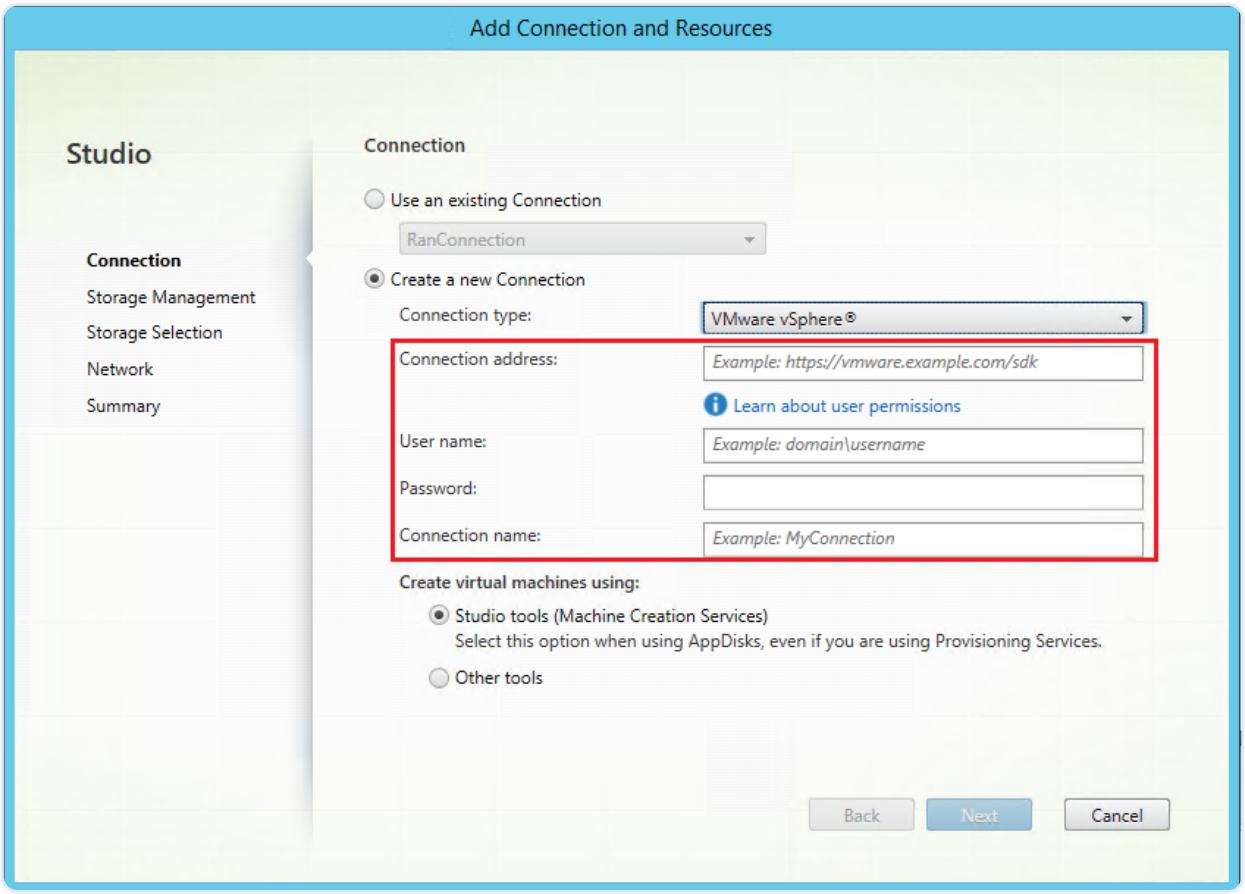
1. Installieren Sie vCenter Server in der vSphere-Umgebung. Weitere Informationen finden Sie unter VMware vSphere.
2. Wählen Sie in Citrix Studio **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu VMware vSphere herzustellen.



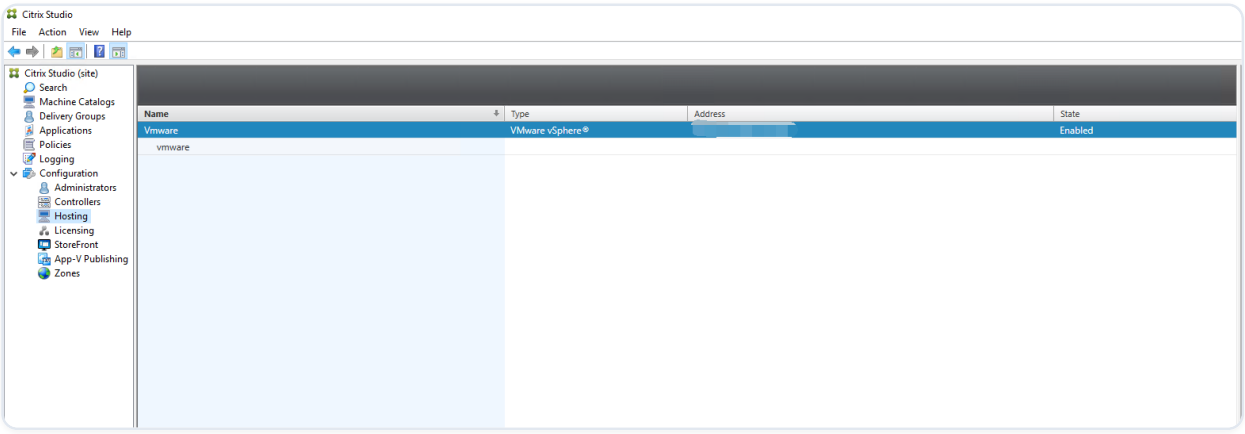
3. Wählen Sie VMware vSphere als Verbindungstyp.



4. Geben Sie die Verbindungsadresse (die vCenter Server-URL) Ihres VMware-Kontos, Ihren Benutzernamen und Ihr Kennwort sowie Ihren Verbindungsnamen ein.



Eine neue Verbindung wird im Hosting-Bereich angezeigt.



Schritt 2: Masterimage vorbereiten

Ein Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, VDA und andere Software. Gehen Sie wie folgt vor, um ein Masterimage vorzubereiten:

Schritt 2a: (Nur für Ubuntu 16.04) OpenJDK 11 installieren

Führen Sie unter Ubuntu 16.04 die folgenden Schritte aus, um OpenJDK 11 zu installieren:

1. Laden Sie das neueste OpenJDK 11 von `<https://jdk.java.net/archive/>` herunter.

2. Führen Sie den Befehl `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` aus, um das heruntergeladene Paket zu entpacken.
3. (Optional) Führen Sie den Befehl `mv jdk-11.0.2/ <target directory>` aus, um OpenJDK in einem Zielverzeichnis zu speichern.
4. Führen Sie den Befehl `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` aus, um die Java-Laufzeitumgebung einzurichten.
5. Führen Sie den Befehl `java -version` aus, um die Java-Version zu überprüfen.

Schritt 2b: Installieren Sie das Linux VDA-Paket auf der Vorlagen-VM

> **Hinweis:**

> Um einen aktuell ausgeführten VDA als Vorlagen-VM zu verwenden, überspringen Sie diesen Schritt.

> Bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Core Runtime 3.1. Weitere Informationen finden Sie unter Installationsübersicht.

> Führen Sie je nach Linux-Distribution den folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

Für RHEL/CentOS:

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

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE 12:

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

Schritt 2c: Installieren Sie das EPEL-Repository, das ntfs-3g bereitstellen kann

Installieren Sie das EPEL-Repository auf RHEL 8/CentOS 8, RHEL 7/CentOS 7, damit deploymcs.sh später das im EPEL-Repository verfügbare ntfs-3g-Paket installiert.

Schritt 2d: ntfs-3g manuell auf SUSE 12 installieren

Auf der SUSE 12-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC)-Compilersystem und das make-Paket:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. ntfs-3g installieren:

   ```
   ./configure

   make

   make install
   ```

Schritt 2e: Laufzeitumgebung einrichten

Führen Sie vor dem Ausführen von `deploymcs.sh` Folgendes aus:

- Ändern Sie Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Festlegen von MCS und des Linux VDA. Im Folgenden sind einige der Variablen aufgeführt, von denen `dns` und `AD_INTEGRATION` festgelegt werden müssen:

Hinweis: Wenn eine Variable mit mehreren Werten festgelegt werden kann, setzen Sie die Werte in einfache Anführungszeichen und trennen Sie sie durch Leerzeichen. Beispiel: LDAP_LIST='aaa.lab:389 bbb.lab:389.'

- `Use_Existing_Configurations_Of_Current_VDA`: Legt fest, ob die vorhandenen Konfigurationen des aktuell ausgeführten VDA verwendet werden sollen. Wenn auf Y gesetzt, sind die Konfigurationsdateien auf MCS-erstellten Maschinen identisch mit den entsprechenden Dateien auf dem aktuell ausgeführten VDA. Sie müssen jedoch weiterhin die Variablen `dns` und `AD_INTEGRATION` konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsvorlagen auf dem Masterimage die Konfigurationsdateien auf MCS-erstellten Maschinen bestimmen.
- `dns`: Legt die DNS-IP-Adresse fest.
- `AD_INTEGRATION`: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der von MSC unterstützten Linux-Distributionen und Domänenbeitrittsmethoden finden Sie unter Unterstützte Distributionen in diesem Artikel.
- `CENTRIFY_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
- `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
- `WORKGROUP`: Legt den Arbeitsgruppennamen (Groß-/Kleinschreibung beachten) fest, wenn Sie ihn in AD konfiguriert haben.

- Fügen Sie auf der Vorlagenmaschine Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzu, um Registrierungswerte nach Bedarf zu schreiben oder zu aktualisieren. Diese Aktion verhindert den Verlust von Daten und Einstellungen bei jedem Neustart einer MCS-bereitgestellten Maschine.

  Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

  Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 2f: Masterimage erstellen

1. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
2. (Optional) Aktualisieren Sie auf der Vorlagen-VM die Konfigurationsvorlagen, um die relevanten Dateien /etc/krb5.conf, /etc/samba/smb.conf und /etc/sssd/sssd.conf auf allen erstellten VMs anzupassen.

   Aktualisieren Sie für Winbind-Benutzer die Vorlagen `/etc/xdl/mcs/winbind_krb5.conf.tmpl` und `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

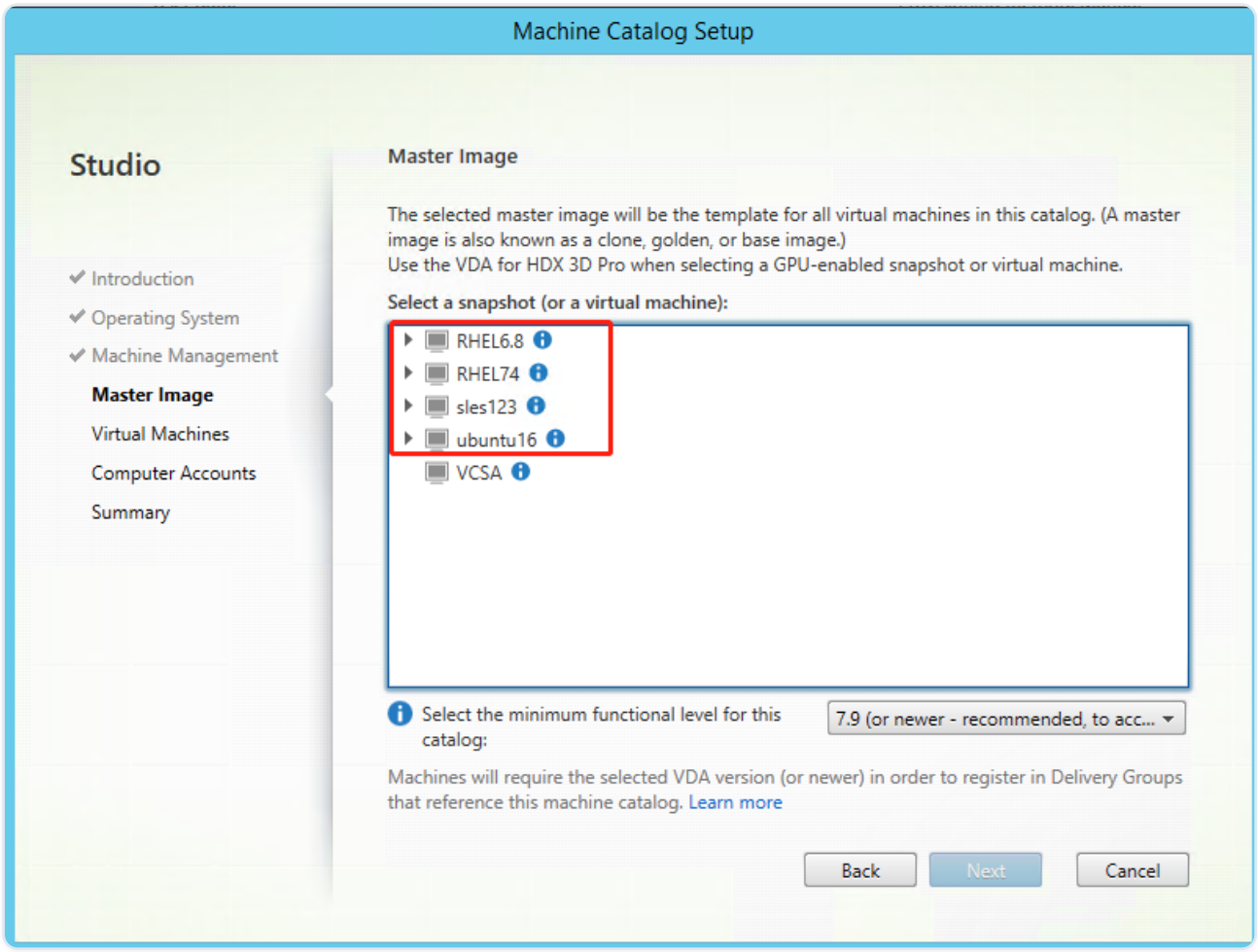
   Aktualisieren Sie für SSSD-Benutzer die Vorlagen `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` und `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

   Aktualisieren Sie für Centrify-Benutzer die Vorlagen `/etc/xdl/mcs/centrify_krb5.conf.tmpl` und `/etc/xdl/mcs/centrify_smb.conf.tmpl`.

   Hinweis: Behalten Sie das vorhandene Format der Vorlagendateien bei und verwenden Sie Variablen wie $WORKGROUP, $REALM, $realm, ${new_hostname} und $AD_FQDN.
3. Nachdem Sie die Installation der Anwendungen auf der Vorlagen-VM abgeschlossen haben, fahren Sie die Vorlagen-VM in VMware herunter. Erstellen Sie einen Snapshot der Vorlagen-VM.

Schritt 3: Maschinenkatalog erstellen

Erstellen Sie in Citrix Studio einen Maschinenkatalog und geben Sie die Anzahl der im Katalog zu erstellenden VMs an. Wählen Sie beim Erstellen des Maschinenkatalogs Ihr Masterimage aus der Snapshot-Liste aus.



Führen Sie bei Bedarf weitere Konfigurationsaufgaben durch. Weitere Informationen finden Sie unter Maschinenkatalog mit Studio erstellen.

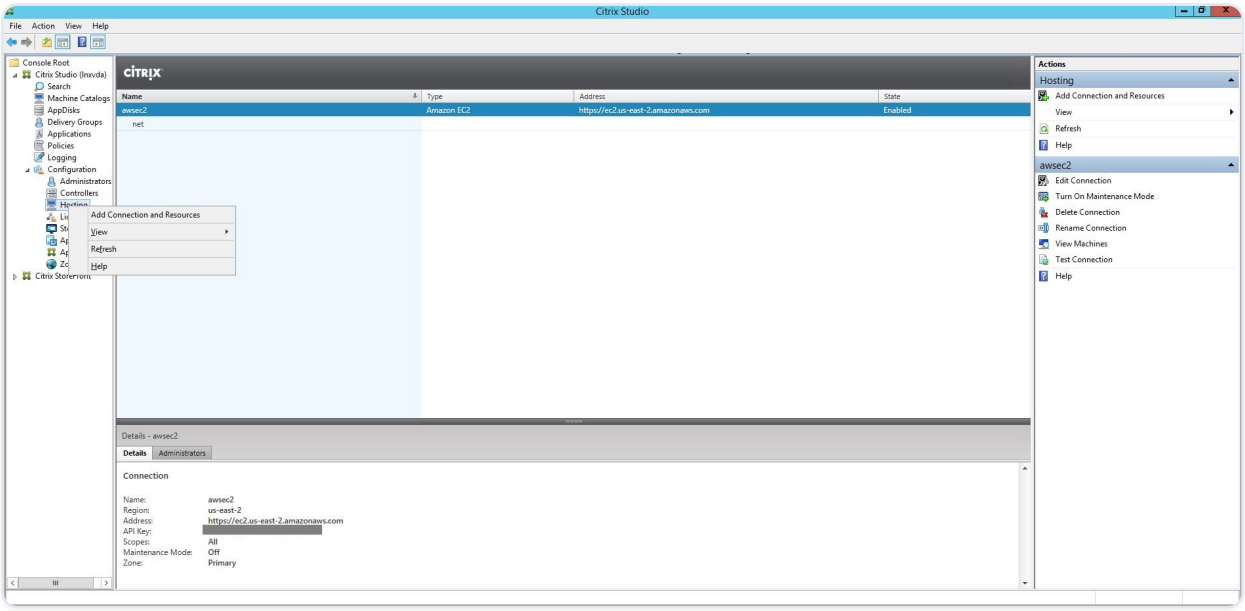
Schritt 4: Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Die Bereitstellungsgruppe gibt an, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

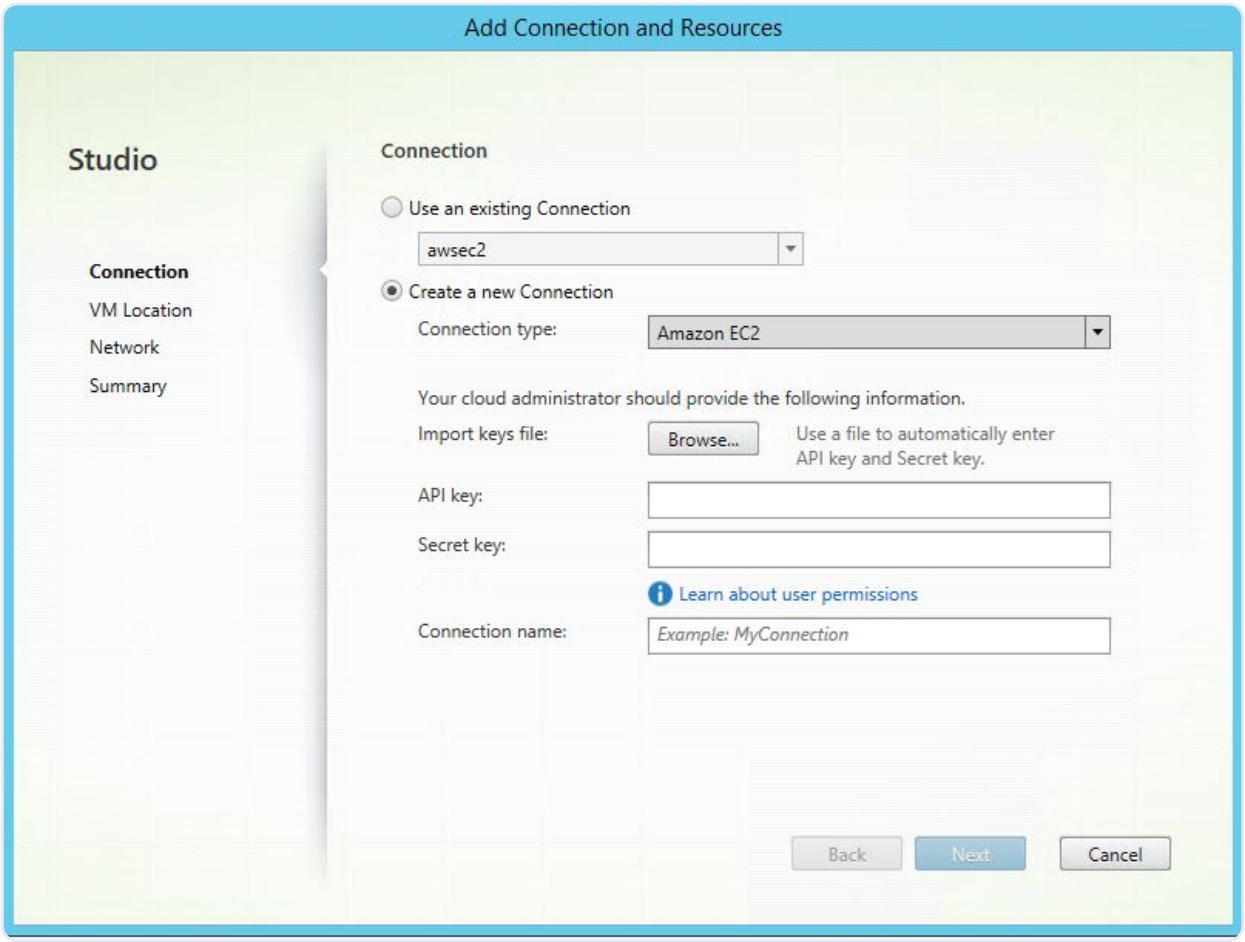
Verwenden Sie MCS zum Erstellen von Linux-VMs in AWS

Schritt 1: Hosting-Verbindung zu AWS in Citrix Studio erstellen

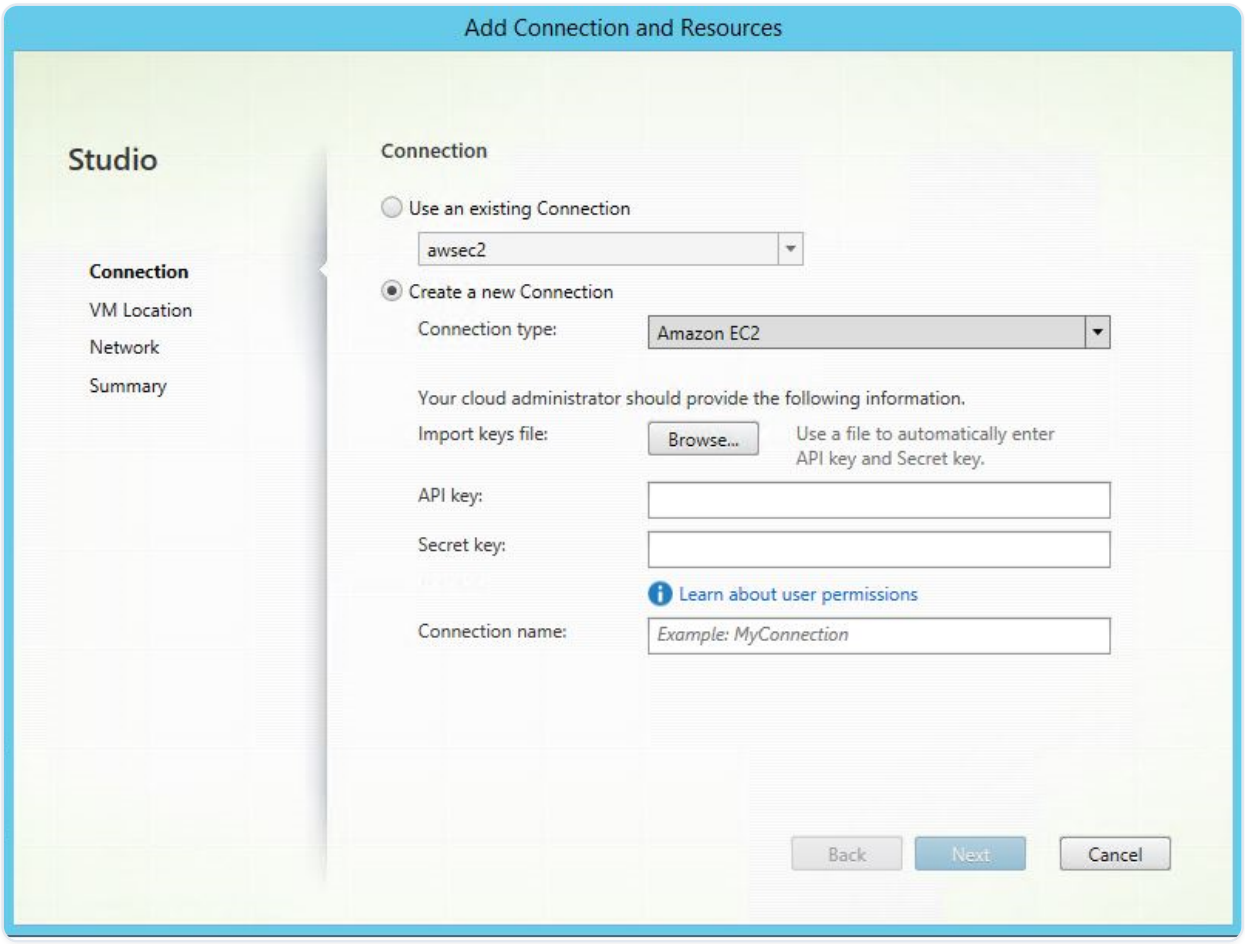
1. Wählen Sie in Citrix Studio in Citrix Cloud **Konfiguration** > **Hosting** > **Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu AWS herzustellen.



2. Wählen Sie **Amazon EC2** als Verbindungstyp.



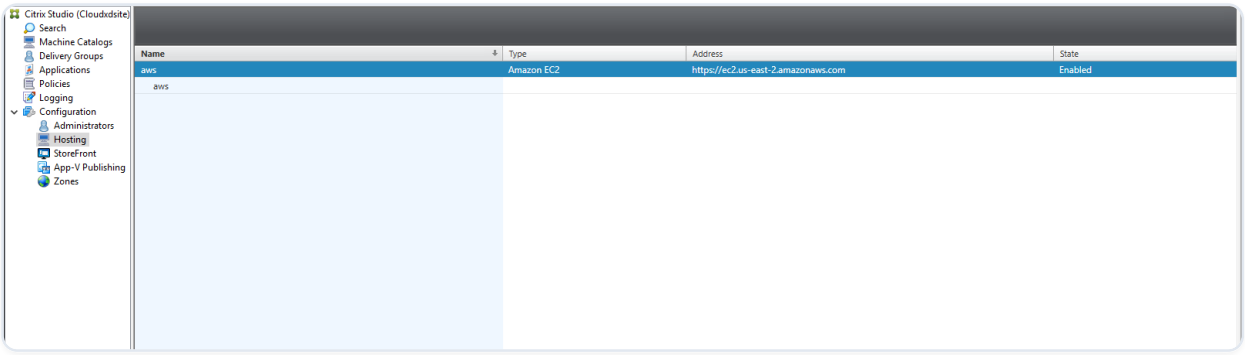
3. Geben Sie den API-Schlüssel und den geheimen Schlüssel Ihres AWS-Kontos sowie den Namen Ihrer Verbindung ein.



Der **API-Schlüssel** ist Ihre Zugriffsschlüssel-ID und der **geheime Schlüssel** ist Ihr geheimer Zugriffsschlüssel. Sie werden als Zugriffsschlüsselpaar betrachtet. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, können Sie den Zugriffsschlüssel löschen und einen neuen erstellen. Gehen Sie wie folgt vor, um einen Zugriffsschlüssel zu erstellen:

a. Melden Sie sich bei den AWS-Diensten an.
b. Navigieren Sie zur Konsole für Identitäts- und Zugriffsverwaltung (IAM).
c. Wählen Sie im linken Navigationsbereich **Benutzer** aus.
d. Wählen Sie den Zielbenutzer aus und scrollen Sie nach unten, um die Registerkarte **Sicherheitsanmeldeinformationen** auszuwählen.
e. Scrollen Sie nach unten und klicken Sie auf **Zugriffsschlüssel erstellen**. Ein neues Fenster wird angezeigt.
f. Klicken Sie auf **.csv-Datei herunterladen** und speichern Sie den Zugriffsschlüssel an einem sicheren Ort.

Eine neue Verbindung wird im Hosting-Bereich angezeigt.



Schritt 2: Masterimage vorbereiten

Ein Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, VDA und andere Software. Gehen Sie wie folgt vor, um ein Masterimage vorzubereiten:

Schritt 2a: cloud-init konfigurieren

1. Um sicherzustellen, dass ein VDA-Hostname beim Neustart oder Beenden einer EC2-Instanz erhalten bleibt, führen Sie den folgenden Befehl aus, um den VDA-Hostnamen beizubehalten.

   ```
   echo "preserve_hostname: true" > /etc/cloud/cloud.cfg.d/99_hostname.cfg
   ```

   Stellen Sie für Ubuntu 18.04 sicher, dass die folgenden Zeilen im Abschnitt system_info in der Datei /etc/cloud/cloud.cfg vorhanden sind:

   ```
   system_info:

       network:

           renderers: ['netplan', 'eni', 'sysconfig']
   ```

2. Um SSH für den Remotezugriff auf mit MCS erstellte VMs in AWS zu verwenden, aktivieren Sie die Kennwortauthentifizierung, da diesen VMs kein Schlüsselname zugeordnet ist. Gehen Sie bei Bedarf wie folgt vor.

   - Bearbeiten Sie die Konfigurationsdatei `cloud-init`, /etc/cloud/cloud.cfg. Stellen Sie sicher, dass die Zeile **ssh_pwauth: true** vorhanden ist. Entfernen oder kommentieren Sie die Zeile **set-password** und die folgenden Zeilen, falls sie vorhanden sind.

     ```
     users:

     - default
     ```

- Wenn Sie den von `cloud-init` erstellten Standardbenutzer `ec2-user` oder `ubuntu` verwenden möchten, können Sie das Benutzerkennwort mit dem Befehl `passwd` ändern. Merken Sie sich das neue Kennwort für die spätere Anmeldung bei den mit MCS erstellten VMs.
- Bearbeiten Sie die Datei `/etc/ssh/sshd_config`, um sicherzustellen, dass die folgende Zeile vorhanden ist:

  ```
  PasswordAuthentication yes
  ```

  Speichern Sie die Datei und führen Sie den Befehl `sudo service sshd restart` aus.

Schritt 2b: (Nur für Ubuntu 16.04) OpenJDK 11 installieren

Installieren Sie unter Ubuntu 16.04 OpenJDK 11, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das neueste OpenJDK 11 von `<https://jdk.java.net/archive/>` herunter.
2. Führen Sie den Befehl `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` aus, um das heruntergeladene Paket zu entpacken.
3. (Optional) Führen Sie den Befehl `mv jdk-11.0.2/ <target directory>` aus, um OpenJDK in einem Zielverzeichnis zu speichern.
4. Führen Sie den Befehl `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` aus, um die Java-Laufzeitumgebung einzurichten.
5. Führen Sie den Befehl `java -version` aus, um die Java-Version zu überprüfen.

Schritt 2c: Installieren des Linux VDA-Pakets auf der Vorlagen-VM

> **Hinweis:**

> Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden möchten, überspringen Sie diesen Schritt.

> Bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Core Runtime 3.1. Weitere Informationen finden Sie unter Installationsübersicht.

> Führen Sie je nach Linux-Distribution den folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

Für RHEL/CentOS:

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

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE 12:

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

Schritt 2d: Installieren des EPEL-Repositorys, das ntfs-3g bereitstellen kann

Installieren Sie das EPEL-Repository auf RHEL 8/CentOS 8, RHEL 7/CentOS 7, damit deploymcs.sh später das im EPEL-Repository verfügbare ntfs-3g-Paket installiert.

Schritt 2e: ntfs-3g manuell auf SUSE 12 installieren

Auf der SUSE 12-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC)-Compilersystem und das make-Paket:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

```
./configure

make

make install
```

Schritt 2f: Einrichten der Laufzeitumgebung

Führen Sie vor dem Ausführen von `deploymcs.sh` Folgendes aus:

- Ändern Sie die Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Festlegen von MCS und des Linux VDA. Im Folgenden sind einige der Variablen aufgeführt, von denen `dns` und `AD_INTEGRATION` festgelegt werden müssen:

  Hinweis: Wenn eine Variable mit mehreren Werten festgelegt werden kann, setzen Sie die Werte in einfache Anführungszeichen und trennen Sie sie durch Leerzeichen. Beispiel: LDAP_LIST='aaa.lab:389 bbb.lab:389.'

  - `Use_Existing_Configurations_Of_Current_VDA`: Legt fest, ob die vorhandenen Konfigurationen des aktuell ausgeführten VDA verwendet werden sollen. Wenn auf Y gesetzt, sind die Konfigurationsdateien auf MCS-erstellten Maschinen identisch mit den entsprechenden Dateien auf dem aktuell ausgeführten VDA. Sie müssen jedoch weiterhin die Variablen `dns` und `AD_INTEGRATION` konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsvorlagen auf dem Masterimage die Konfigurationsdateien auf MCS-erstellten Maschinen bestimmen.
  - `dns`: Legt die DNS-IP-Adresse fest.
  - `AD_INTEGRATION`: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der von MSC unterstützten Linux-Distributionen und Domänenbeitrittsmethoden finden Sie unter Unterstützte Distributionen in diesem Artikel.
  - `CENTRIFY_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
  - `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.

  - `WORKGROUP`: Legt den Arbeitsgruppennamen (Groß-/Kleinschreibung beachten) fest, wenn Sie ihn in AD konfiguriert haben.

- Fügen Sie auf der Vorlagenmaschine Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzu, um Registrierungswerte nach Bedarf zu schreiben oder zu aktualisieren. Diese Aktion verhindert den Verlust von Daten und Einstellungen bei jedem Neustart einer MCS-bereitgestellten Maschine.

  Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

  Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 2g: Master-Image erstellen

1. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
2. (Optional) Aktualisieren Sie auf der Vorlagen-VM die Konfigurationsvorlagen, um die relevanten Dateien `/etc/krb5.conf`, `/etc/samba/smb.conf` und `/etc/sssd/sssd.conf` auf allen erstellten VMs anzupassen.

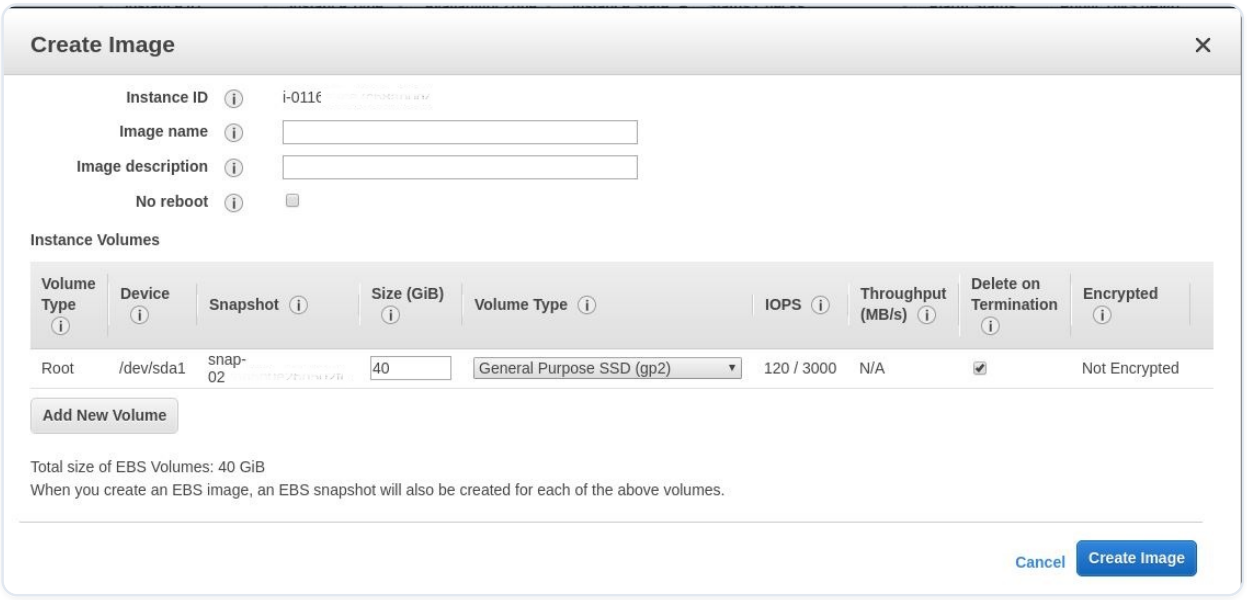
   Für Winbind-Benutzer aktualisieren Sie die Vorlagen `/etc/xdl/mcs/winbind_krb5.conf.tmpl` und `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

   Für SSSD-Benutzer aktualisieren Sie die Vorlagen `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` und `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

   Für Centrify-Benutzer aktualisieren Sie die Vorlagen `/etc/xdl/mcs/centrify_krb5.conf.tmpl` und `/etc/xdl/mcs/centrify_smb.conf.tmpl`.

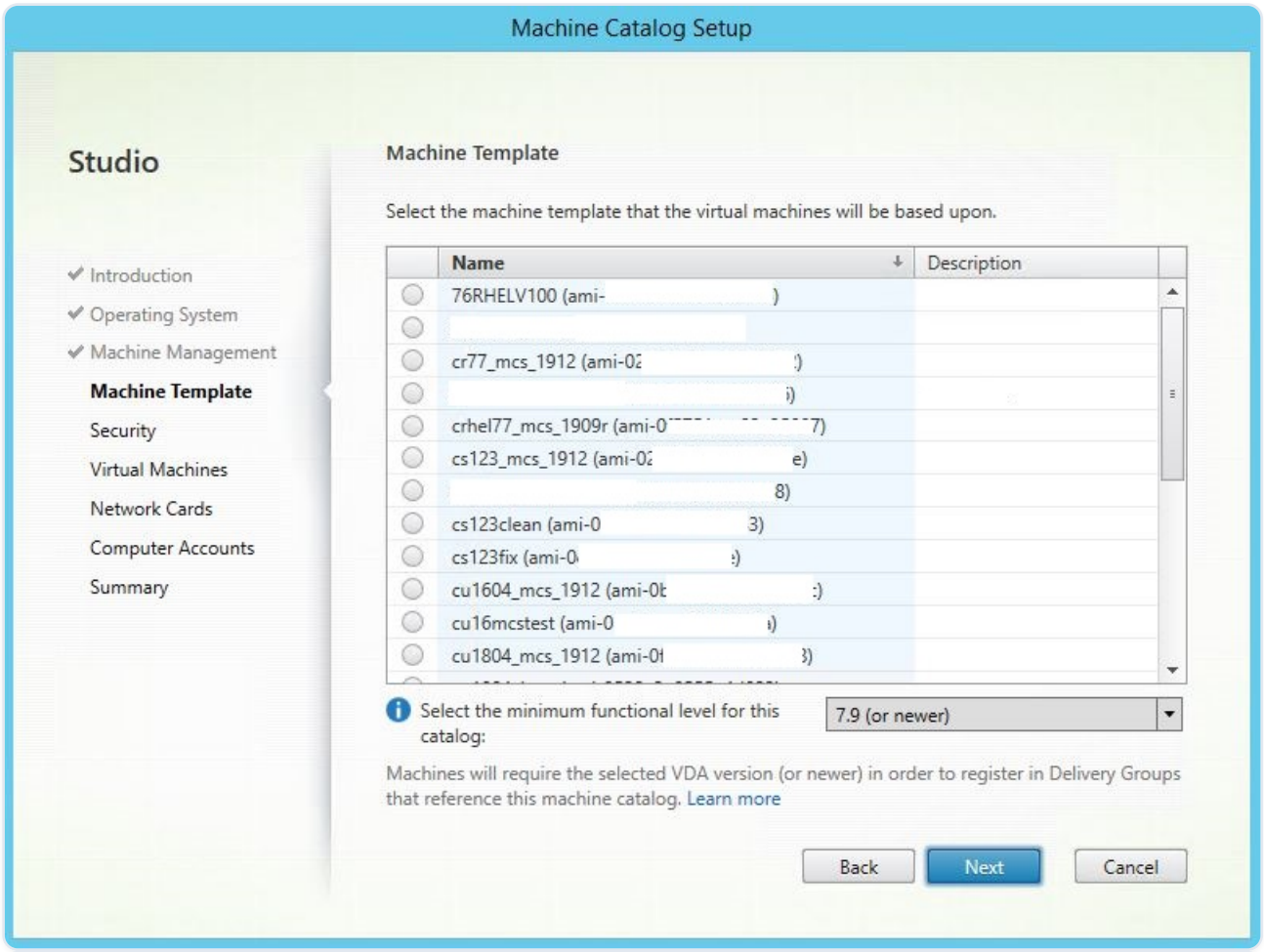
Hinweis: Behalten Sie das in den Vorlagendateien verwendete Format bei und verwenden Sie Variablen wie $WORKGROUP, $REALM, $realm, ${new_hostname} und $AD_FQDN.

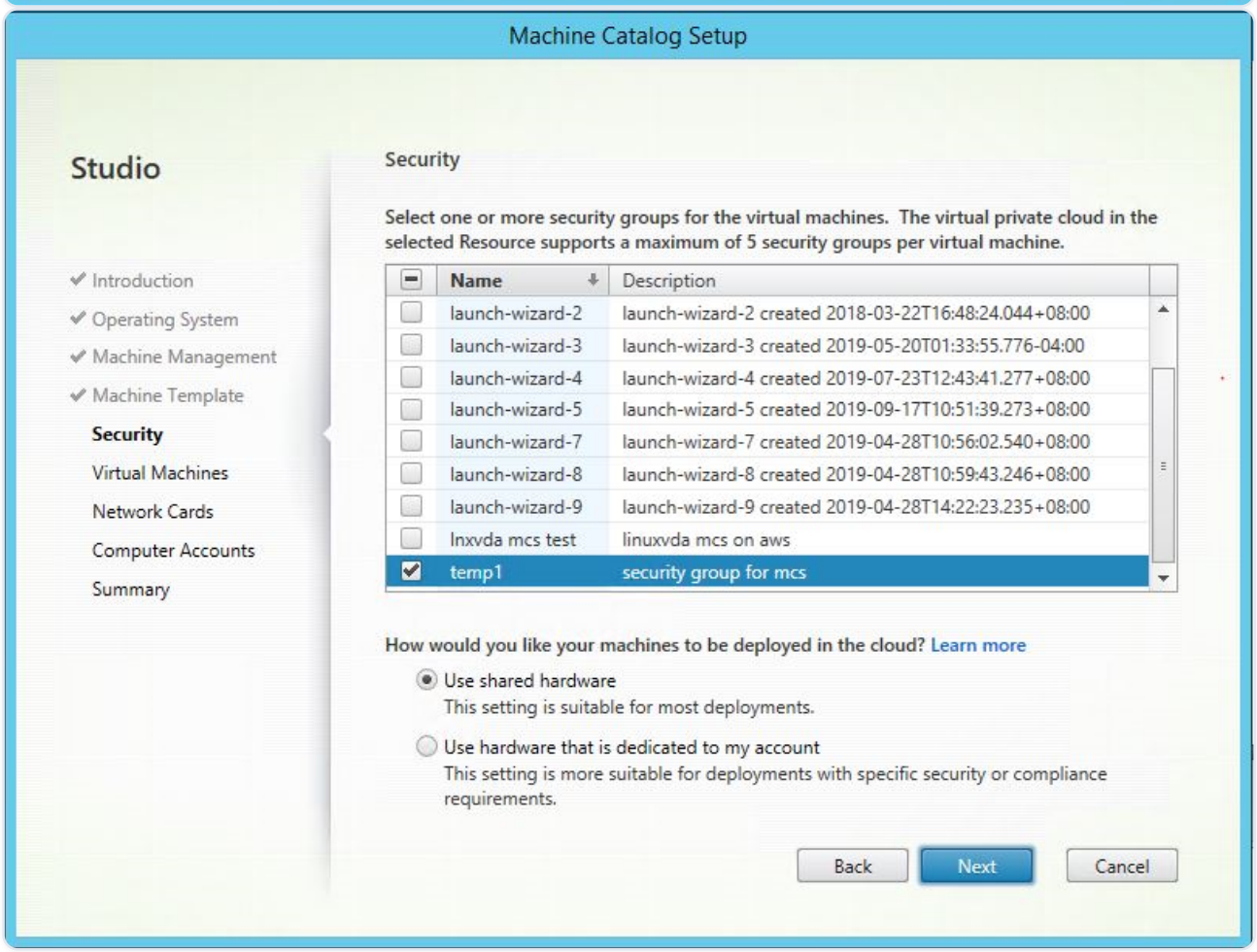
3. Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM über das AWS EC2-Portal herunter. Stellen Sie sicher, dass der Instanzstatus der Vorlagen-VM **Stopped** ist.
4. Klicken Sie mit der rechten Maustaste auf die Vorlagen-VM und wählen Sie **Image > Create Image**. Geben Sie die erforderlichen Informationen ein und nehmen Sie die Einstellungen vor. Klicken Sie auf **Create Image**.



Schritt 3: Maschinenkatalog erstellen

Erstellen Sie in Citrix Studio einen Maschinenkatalog und geben Sie die Anzahl der im Katalog zu erstellenden VMs an. Wählen Sie beim Erstellen des Maschinenkatalogs Ihre Maschinen-Vorlage (das zuvor erstellte Master-Image) aus und wählen Sie eine oder mehrere Sicherheitsgruppen aus.


Machine Catalog Setup
Studio
Introduction
Operating System
Machine Management
Machine Template
Security
Virtual Machines
Network Cards
Computer Accounts
Summary
Machine Template
Select the machine template that the virtual machines will be based upon.
Name
Description
76RHELV100 (ami-
cr77_mcs_1912 (ami-0
crhel77_mcs_1909r (ami-0
cs123_mcs_1912 (ami-0
cs123clean (ami-0
cs123fix (ami-0
cu1604_mcs_1912 (ami-0
cu16mcstest (ami-0
cu1804_mcs_1912 (ami-0
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


Machine Catalog Setup
Studio
Introduction
Operating System
Machine Management
Machine Template
Security
Virtual Machines
Network Cards
Computer Accounts
Summary
Security
Select one or more security groups for the virtual machines. The virtual private cloud in the selected Resource supports a maximum of 5 security groups per virtual machine.
Name
Description
launch-wizard-2
launch-wizard-2 created 2018-03-22T16:48:24.044+08:00
launch-wizard-3
launch-wizard-3 created 2019-05-20T01:33:55.776-04:00
launch-wizard-4
launch-wizard-4 created 2019-07-23T12:43:41.277+08:00
launch-wizard-5
launch-wizard-5 created 2019-09-17T10:51:39.273+08:00
launch-wizard-7
launch-wizard-7 created 2019-04-28T10:56:02.540+08:00
launch-wizard-8
launch-wizard-8 created 2019-04-28T10:59:43.246+08:00
launch-wizard-9
launch-wizard-9 created 2019-04-28T14:22:23.235+08:00
lnxvda mcs test
linuxvda mcs on aws
temp1
security group for mcs
How would you like your machines to be deployed in the cloud? Learn more
Use shared hardware
This setting is suitable for most deployments.
Use hardware that is dedicated to my account
This setting is more suitable for deployments with specific security or compliance requirements.
Back
Next
Cancel

Führen Sie bei Bedarf weitere Konfigurationsaufgaben durch. Weitere Informationen finden Sie unter Maschinenkatalog mit Studio erstellen.

Schritt 4: Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Die Bereitstellungsgruppe legt fest, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

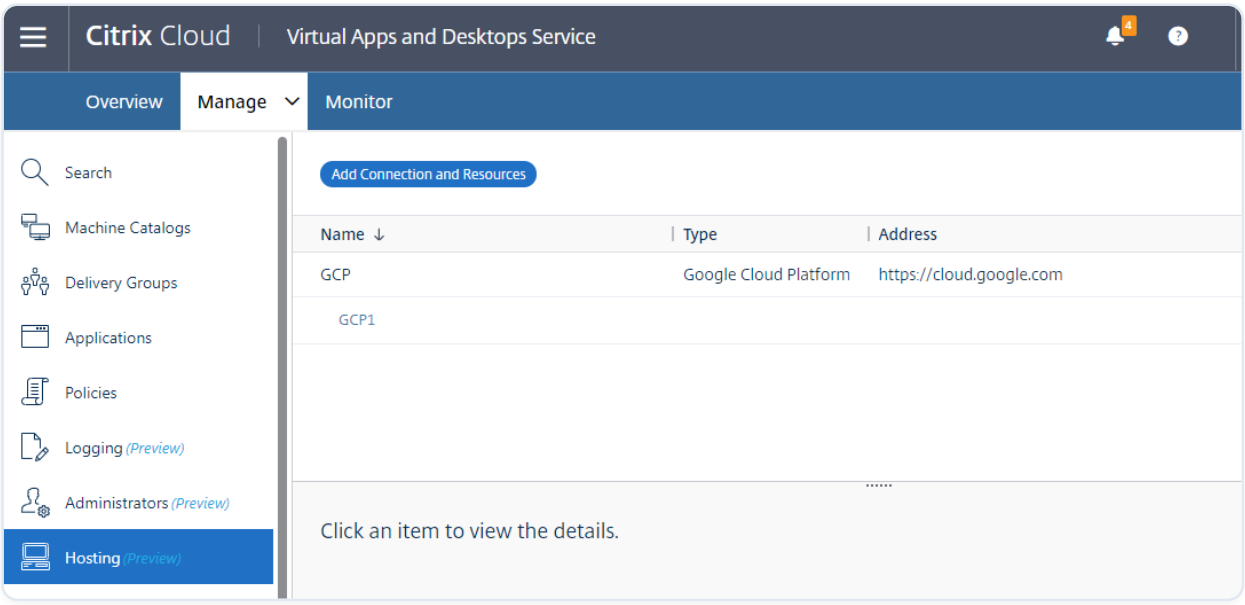
MCS zum Erstellen von Linux-VMs in GCP verwenden

Schritt 1: GCP-Umgebung einrichten

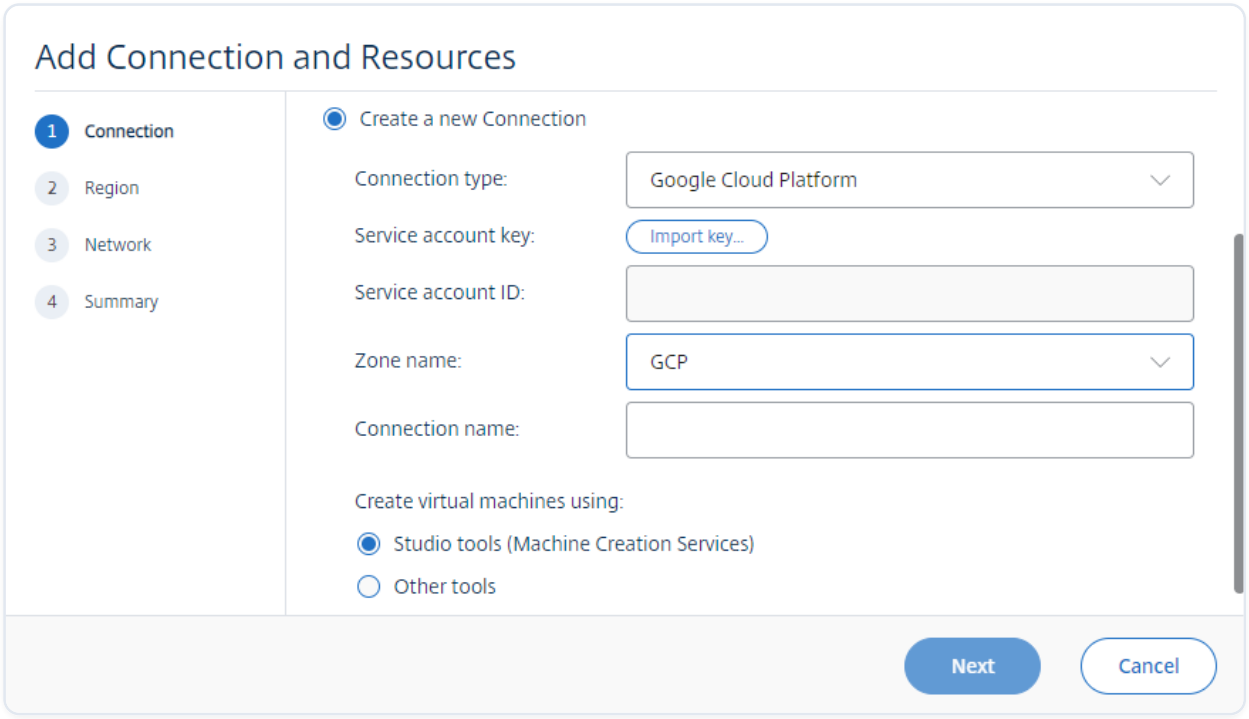
Weitere Informationen finden Sie unter Google Cloud Platform-Virtualisierungsumgebungen.

Schritt 2: Eine Hosting-Verbindung zu GCP in Citrix Studio erstellen

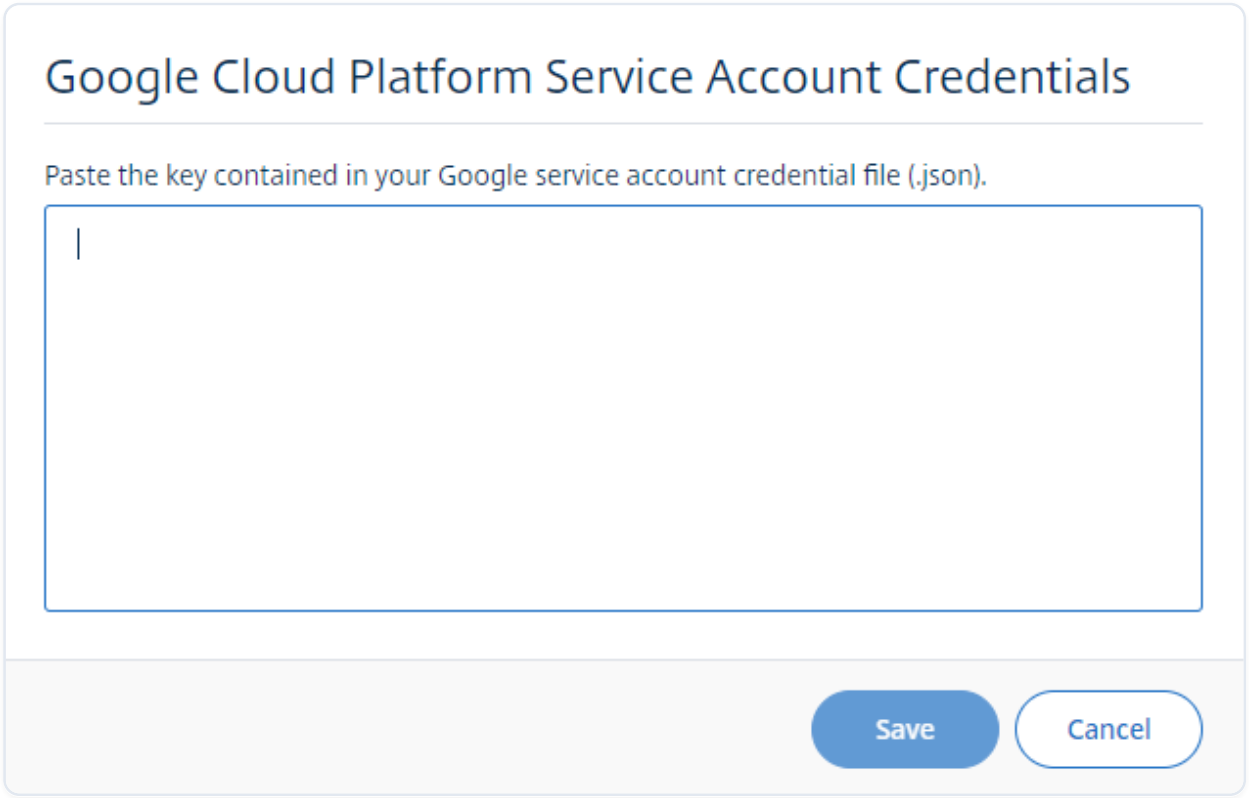
1. Wählen Sie in Citrix Studio in Citrix Cloud **Konfiguration** > **Hosting** > **Verbindung und Ressourcen hinzufügen**, um eine Verbindung zu GCP herzustellen.



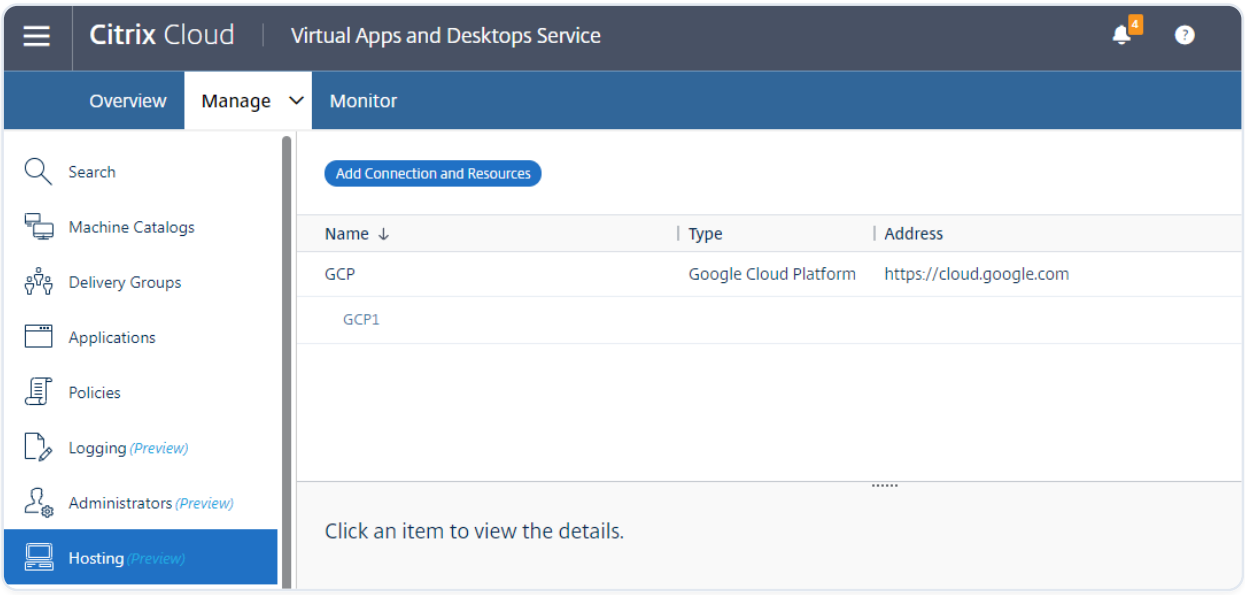
2. Wählen Sie **Google Cloud Platform** als Verbindungstyp.



3. Importieren Sie den Dienstkontoschlüssel Ihres GCP-Kontos und geben Sie Ihren Verbindungsnamen ein.



Eine neue Verbindung wird im Hosting-Bereich angezeigt.



Schritt 3: Masterimage vorbereiten

Ein Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, VDA und andere Software. Gehen Sie wie folgt vor, um ein Masterimage vorzubereiten:

Schritt 3a: (Nur für Ubuntu 16.04) OpenJDK 11 installieren

Unter Ubuntu 16.04 installieren Sie OpenJDK 11, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das neueste OpenJDK 11 von `<https://jdk.java.net/archive/>` herunter.
2. Führen Sie den Befehl `tar zxf openjdk-11.0.2_linux-x64_bin.tar.gz` aus, um das heruntergeladene Paket zu entpacken.
3. (Optional) Führen Sie den Befehl `mv jdk-11.0.2/ <target directory>` aus, um OpenJDK in einem Zielverzeichnis zu speichern.
4. Führen Sie den Befehl `update-alternatives --install /usr/bin/java java <custom directory>/bin/java 2000` aus, um die Java-Laufzeitumgebung einzurichten.
5. Führen Sie den Befehl `java -version` aus, um die Java-Version zu überprüfen.

Schritt 3b: Installieren Sie das Linux VDA-Paket auf der Vorlagen-VM

> **Hinweis:**

> Um einen aktuell ausgeführten VDA als Vorlagen-VM zu verwenden, überspringen Sie diesen Schritt.

> Bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Core Runtime 3.1. Weitere Informationen finden Sie unter Installationsübersicht.

> Führen Sie je nach Linux-Distribution den folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

Für RHEL/CentOS:

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

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE 12:

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

Schritt 3c: Installieren Sie das EPEL-Repository, das ntfs-3g bereitstellen kann

Installieren Sie das EPEL-Repository auf RHEL 8/CentOS 8, RHEL 7/CentOS 7, damit die spätere Ausführung von deploymcs.sh das im EPEL-Repository verfügbare ntfs-3g-Paket installiert.

Schritt 3d: ntfs-3g manuell auf SUSE 12 installieren

Auf der SUSE 12-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC)-Compilersystem und das make-Paket:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

```
./configure

make

make install
```

Schritt 3e: Die Laufzeitumgebung einrichten

Führen Sie vor dem Ausführen von `deploymcs.sh` Folgendes aus:

- Ändern Sie Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Festlegen von MCS und des Linux VDA. Im Folgenden sind einige der Variablen aufgeführt, von denen `dns` und `AD_INTEGRATION` festgelegt werden müssen:

  Hinweis: Wenn eine Variable mit mehreren Werten festgelegt werden kann, setzen Sie die Werte in einfache Anführungszeichen und trennen Sie sie durch Leerzeichen. Beispiel: LDAP_LIST='aaa.lab:389 bbb.lab:389'.

  - `Use_Existing_Configurations_Of_Current_VDA`: Legt fest, ob die vorhandenen Konfigurationen des aktuell ausgeführten VDA verwendet werden sollen. Wenn auf Y gesetzt, sind die Konfigurationsdateien auf MCS-erstellten Maschinen dieselben wie die entsprechenden auf dem aktuell ausgeführten VDA. Sie müssen jedoch weiterhin die Variablen `dns` und `AD_INTEGRATION` konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsvorlagen auf dem Master-Image die Konfigurationsdateien auf MCS-erstellten Maschinen bestimmen.
  - `dns`: Legt die DNS-IP-Adresse fest.
  - `AD_INTEGRATION`: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der von MSC unterstützten Linux-Distributionen und Domänenbeitrittsmethoden finden Sie unter Unterstützte Distributionen in diesem Artikel.

- `CENTRIFY_DOWNLOAD_PATH`: Legt den Pfad für den Download des Centrify-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
- `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Legt den Pfad für den Download des Centrify Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
- `WORKGROUP`: Legt den Namen der Arbeitsgruppe (Groß-/Kleinschreibung beachten) fest, wenn Sie ihn in AD konfiguriert haben.

- Fügen Sie auf der Vorlagenmaschine Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` 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 bereitgestellten Maschine.

  Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

  Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 3f: Masterimage erstellen

1. Führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.
2. (Optional) Aktualisieren Sie auf der Vorlagen-VM die Konfigurationsvorlagen, um die relevanten Dateien `/etc/krb5.conf`, `/etc/samba/smb.conf` und `/etc/sssd/sssd.conf` auf allen erstellten VMs anzupassen.

   Aktualisieren Sie für Winbind-Benutzer die Vorlagen `/etc/xdl/mcs/winbind_krb5.conf.tmpl` und `/etc/xdl/mcs/winbind_smb.conf.tmpl`.

Aktualisieren Sie für SSSD-Benutzer die Vorlagen `/etc/xdl/mcs/sssd.conf.tmpl`, `/etc/xdl/mcs/sssd_krb5.conf.tmpl` und `/etc/xdl/mcs/sssd_smb.conf.tmpl`.

Aktualisieren Sie für Centrify-Benutzer die Vorlagen `/etc/xdl/mcs/centrify_krb5.conf.tmpl` und `/etc/xdl/mcs/centrify_smb.conf.tmpl`.

> **Hinweis:**
>
> Behalten Sie das in den Vorlagendateien verwendete Format bei und verwenden Sie Variablen wie $WORKGROUP, $REALM, $realm, ${new_hostname} und $AD_FQDN.

3. Nachdem Sie die Installation der Anwendungen auf der Vorlagen-VM abgeschlossen haben, fahren Sie die Vorlagen-VM über VMware herunter. Erstellen Sie einen Snapshot der Vorlagen-VM.

Schritt 4: Maschinenkatalog erstellen

Erstellen Sie in Citrix Studio einen Maschinenkatalog und geben Sie die Anzahl der im Katalog zu erstellenden VMs an. Wählen Sie beim Erstellen des Maschinenkatalogs Ihr Masterimage aus der Snapshot-Liste aus.

Abbildung der Auswahl eines Master-Images(/en-us/linux-virtual-delivery-agent/2107/media/choose-master-image-from-the-list.png)

Führen Sie bei Bedarf weitere Konfigurationsaufgaben aus. Weitere Informationen finden Sie unter Maschinenkatalog mit Studio erstellen.

Schritt 5: Eine Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Die Bereitstellungsgruppe legt fest, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

MCS zum Erstellen von Linux-VMs auf Nutanix AHV verwenden

Schritt 1: Nutanix AHV-Plug-In installieren und registrieren

Beziehen Sie das Nutanix AHV-Plug-In-Paket von Nutanix. Installieren und registrieren Sie das Plug-In in Ihrer Citrix Virtual Apps and Desktops-Umgebung. Weitere Informationen finden Sie im

Installationshandbuch für das Nutanix Acropolis MCS-Plug-In, das im Nutanix Support Portal verfügbar ist.

Schritt 1a: Nutanix AHV-Plug-In für lokale Delivery Controller installieren und registrieren

Nach der Installation von Citrix Virtual Apps™ and Desktops wählen und installieren Sie das **XD MCS AHV Plugin** auf Ihren Delivery Controllern.

Nutanix AHV-Plug-In für lokale Delivery Controller(/en-us/linux-virtual-delivery-agent/2107/media/nutanix-plug-in-for-cvad.png)

Schritt 1b: Nutanix AHV-Plug-In für Cloud Delivery Controller installieren und registrieren

Nach der Installation von Citrix Virtual Apps and Desktops wählen und installieren Sie das **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 registrieren, auch wenn sie einen Ressourcenstandort ohne AHV bedienen.

Schritt 1c: Führen Sie die folgenden Schritte nach der Installation des Plug-Ins aus

- Überprüfen Sie, ob ein Nutanix Acropolis-Ordner in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0` 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 Machine Creation Services auf Ihren lokalen Delivery Controllern neu oder starten Sie den Citrix RemoteHCLServer Service auf Citrix Cloud Connectors neu.

> **Tipp:**
>
> Wir empfehlen Ihnen, den Citrix Host, Citrix Broker und Machine Creation Services anzuhalten und dann neu zu starten, wenn Sie das Nutanix AHV-Plug-In installieren oder aktualisieren.

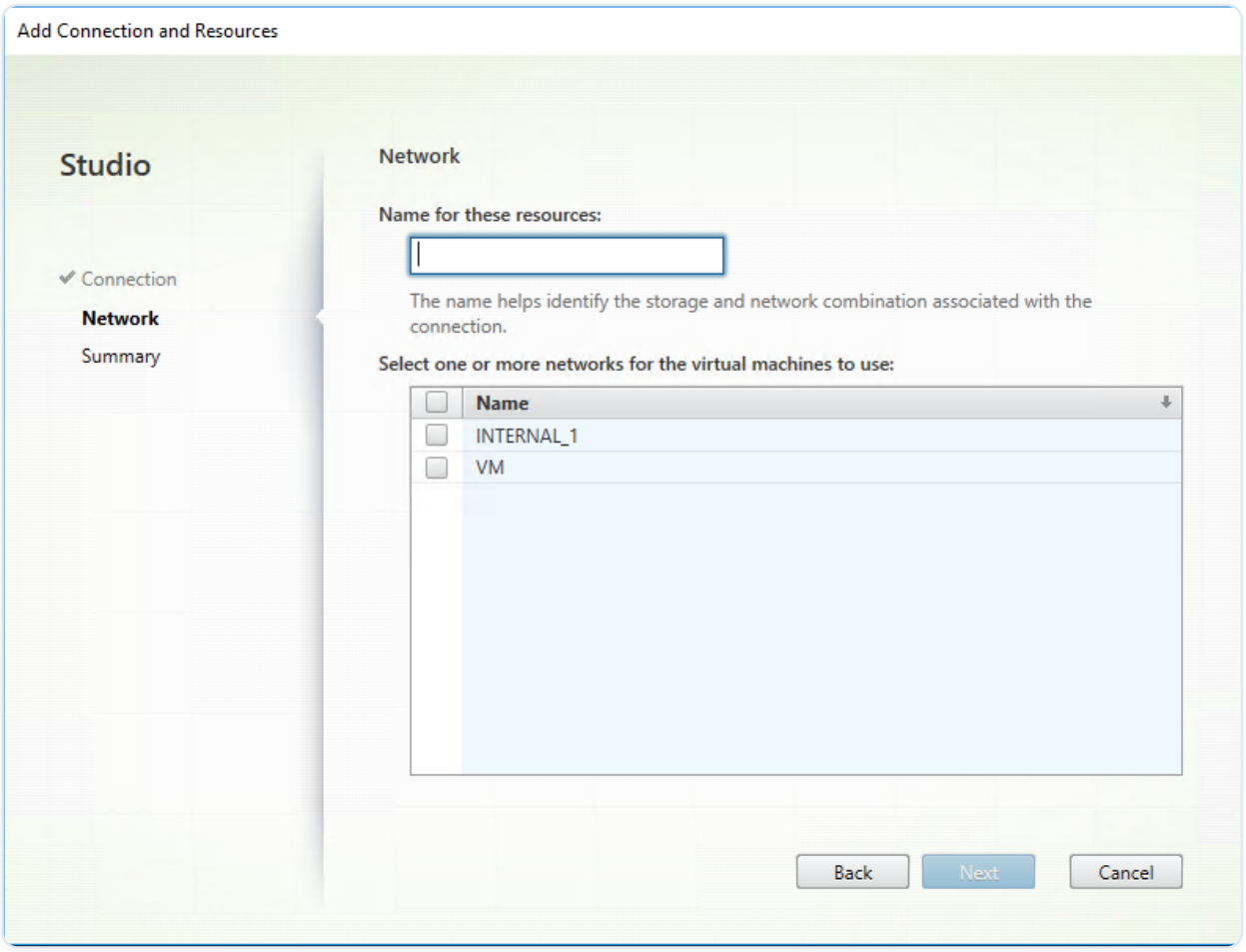
Schritt 2: Hostverbindung zu Nutanix in Citrix Studio erstellen

1. Für lokale Delivery Controller wählen Sie im lokalen Citrix Studio **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**. Für Cloud Delivery Controller wählen Sie in der

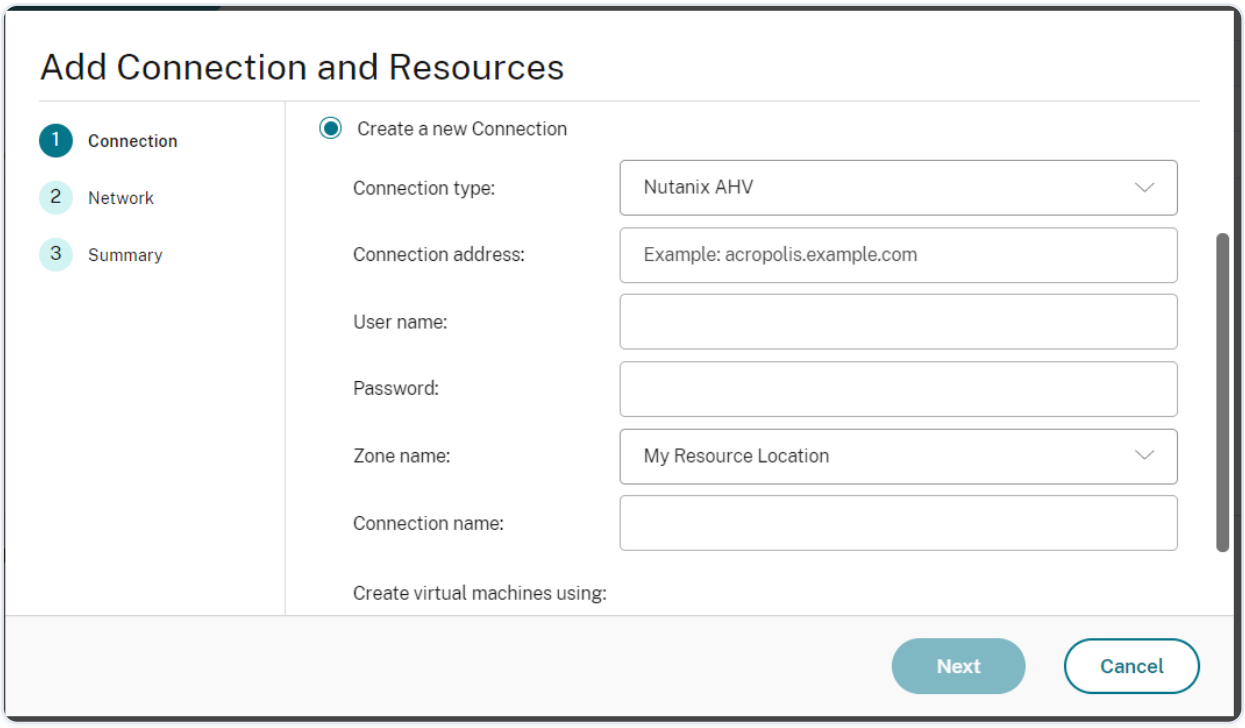
webbasierten Studio-Konsole in Citrix Cloud **Verwalten > Hosting > Verbindung und Ressourcen hinzufügen**, um eine Verbindung zum Nutanix-Hypervisor herzustellen.

2. Wählen Sie im Assistenten **Verbindung und Ressourcen hinzufügen** auf der Seite **Verbindung** Nutanix AHV als Verbindungstyp aus und geben Sie dann die Hypervisoradresse, Anmeldeinformationen und den Verbindungsnamen an. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit aus.

   Beispiel: im lokalen Citrix Studio:



   Beispiel: in der webbasierten Studio-Konsole in Citrix Cloud:



3. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit aus.

Schritt 3: Masterimage auf der Vorlagen-VM vorbereiten

Ein Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, den VDA und andere Software. Führen Sie zum Vorbereiten eines Masterimages die folgenden Schritte aus:

Schritt 3a: Linux-VDA-Paket auf der Vorlagen-VM installieren

> **Hinweis:**

> Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden möchten, überspringen Sie diesen Schritt.

> Bevor Sie das Linux-VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Core Runtime 3.1. Weitere Informationen finden Sie unter Installationsübersicht.

> Führen Sie je nach Linux-Distribution den folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

Für RHEL/CentOS:

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

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE 12:

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

Schritt 3b: Installieren Sie das EPEL-Repository, das ntfs-3g bereitstellen kann

Installieren Sie das EPEL-Repository auf RHEL 8/CentOS 8, RHEL 7/CentOS 7, damit die spätere Ausführung von deploymcs.sh das im EPEL-Repository verfügbare ntfs-3g-Paket installiert.

Schritt 3c: ntfs-3g manuell auf SUSE 12 installieren

Auf der SUSE 12-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC)-Compilersystem und das make-Paket:

   ```
   sudo zypper install gcc

   sudo zypper install make
   ```

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

```
./configure

make

make install
```

Schritt 3d: Die Laufzeitumgebung einrichten

Führen Sie vor dem Ausführen von `deploymcs.sh` Folgendes aus:

- Ändern Sie Variablen in `/etc/xdl/mcs/mcs.conf`. Die Konfigurationsdatei `mcs.conf` enthält Variablen zum Festlegen von MCS und des Linux VDA. Im Folgenden sind einige der Variablen aufgeführt, von denen `dns` und `AD_INTEGRATION` festgelegt werden müssen:

  Hinweis: Wenn eine Variable mit mehreren Werten festgelegt werden kann, setzen Sie die Werte in einfache Anführungszeichen und trennen Sie sie durch Leerzeichen. Beispiel: LDAP_LIST='aaa.lab:389 bbb.lab:389'.

  - `Use_Existing_Configurations_Of_Current_VDA`: Legt fest, ob die vorhandenen Konfigurationen des aktuell ausgeführten VDA verwendet werden sollen. Wenn auf Y gesetzt, sind die Konfigurationsdateien auf MCS-erstellten Maschinen dieselben wie die entsprechenden auf dem aktuell ausgeführten VDA. Sie müssen jedoch weiterhin die Variablen `dns` und `AD_INTEGRATION` konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsvorlagen auf dem Masterimage die Konfigurationsdateien auf MCS-erstellten Maschinen bestimmen.
  - `dns`: Legt die DNS-IP-Adresse fest.
  - `AD_INTEGRATION`: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der Linux-Distributionen und Domänenbeitrittsmethoden, die MSC unterstützt, finden Sie unter Unterstützte Distributionen in diesem Artikel.
  - `CENTRIFY_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
  - `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
  - `WORKGROUP`: Legt den Arbeitsgruppennamen (Groß-/Kleinschreibung beachten) fest, wenn Sie ihn in AD konfiguriert haben.

- Fügen Sie auf der Vorlagenmaschine Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzu, um Registrierungswerte nach Bedarf zu schreiben oder zu aktualisieren. Diese Aktion verhindert den Verlust von Daten und Einstellungen bei jedem Neustart einer MCS-bereitgestellten Maschine.

  Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

  Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 3e: Fahren Sie auf Nutanix AHV die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages

> **Hinweis:**
>
> Sie müssen Acropolis-Snapshot-Namen mit `XD_` präfixieren, um sie in Citrix Virtual Apps and Desktops verwenden zu können. Verwenden Sie die Acropolis-Konsole, um Ihre Snapshots bei Bedarf umzubenennen. Nachdem Sie einen Snapshot umbenannt haben, starten Sie den Assistenten **Katalog erstellen** neu, um eine aktualisierte Liste zu erhalten.

Schritt 4: Maschinenkatalog erstellen

Erstellen Sie in Citrix Studio einen Maschinenkatalog und geben Sie die Anzahl der zu erstellenden VMs im Katalog an. Wählen Sie auf der Seite **Container**, die nur für Nutanix verfügbar ist, den Container aus, den Sie zuvor für die Vorlagen-VM angegeben haben. Wählen Sie auf der Seite **Masterimage** den Image-Snapshot aus. Überprüfen Sie auf der Seite **Virtuelle Maschinen** die Anzahl der virtuellen CPUs und die Anzahl der Kerne pro vCPU.

Führen Sie bei Bedarf weitere Konfigurationsaufgaben aus. Weitere Informationen finden Sie unter Maschinenkatalog mit Studio erstellen.

Hinweis:

Wenn der Erstellungsprozess Ihres Maschinenkatalogs auf dem Delivery Controller™ viel Zeit in Anspruch nimmt, wechseln Sie zu Nutanix Prism und schalten Sie die Maschine mit dem Präfix **Preparation** manuell ein. Dieser Ansatz hilft, den Erstellungsprozess fortzusetzen.

Schritt 5: Eine Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Die Bereitstellungsgruppe legt fest, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

MCS zum Aktualisieren Ihres Linux VDA verwenden

Gehen Sie wie folgt vor, um MCS zum Aktualisieren Ihres Linux VDA zu verwenden:

1. Stellen Sie sicher, dass Sie .NET Core Runtime 3.1 installiert haben, bevor Sie Ihren Linux VDA auf die aktuelle Version aktualisieren.
2. Aktualisieren Sie Ihren Linux VDA auf der Vorlagenmaschine:

   Hinweis:

   Sie können auch die Funktion Linux VDA-Selbstaktualisierung verwenden, um automatische Softwareupdates zu planen. Fügen Sie hierzu Befehlszeilen zur Datei etc/xdl/mcs/mcs_local_setting.reg auf der Vorlagenmaschine hinzu. Sie können beispielsweise die folgenden Befehlszeilen hinzufügen:

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



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

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

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

Für RHEL 7 und CentOS 7:

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

Für RHEL 8 und CentOS 8:

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

Für SUSE 12:

```
sudo rpm -U XenDesktopVDA-<version>.sle12_x.x86_64.rpm
```

Für Ubuntu 16.04:

```
sudo dpkg -i xendesktopvda_<version>.ubuntu16.04_amd64.deb
```

Für Ubuntu 18.04:

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

Für Ubuntu 20.04:

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

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, bevor jede Maschine neu gestartet wird. Starten Sie eine Maschine nicht manuell neu.

Automatisches Aktualisieren von Computerkontokennwörtern

Computerkontokennwörter laufen standardmäßig 30 Tage nach der Erstellung des Maschinenkatalogs ab. Um den Ablauf von Kennwörtern zu verhindern und die Aktualisierung von Computerkontokennwörtern zu automatisieren, gehen Sie wie folgt vor:

1. Fügen Sie den folgenden Eintrag zu /etc/xdl/mcs/mcs.conf hinzu, bevor Sie /opt/Citrix/VDA/sbin/deploymcs.sh ausführen.

   ```
   UPDATE_MACHINE_PW="enabled"
   ```

2. Nachdem Sie /opt/Citrix/VDA/sbin/deploymcs.sh ausgeführt haben, öffnen Sie /etc/cron.d/mcs_update_password_cronjob, um die Aktualisierungszeit und -häufigkeit festzulegen. Die Standardeinstellung aktualisiert die Computerkontokennwörter wöchentlich sonntags um 2:30 Uhr.

Nach jeder Aktualisierung des Computerkontokennworts wird der Ticket-Cache auf dem Delivery Controller ungültig, und der folgende Fehler kann in /var/log/xdl/jproxy.log angezeigt werden:

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

Um den Fehler zu beheben, leeren Sie den Ticket-Cache regelmäßig. Sie können eine Cache-Bereinigungsaufgabe auf allen Delivery Controllern oder auf dem Domänencontroller planen.

FAS auf MCS-erstellten VMs aktivieren

Sie können FAS auf MCS-erstellten VMs aktivieren, die auf den folgenden Distributionen ausgeführt werden:

	WINBIND	SSSD	CENTRIFY
RHEL 8, CentOS 8	Ja	Nein	Nein
RHEL 7, CentOS 7	Ja	Ja	Nein
Ubuntu 20.04	Ja	Nein	Nein

	WINBIND	SSSD	CENTRIFY
Ubuntu 18.04	Ja	Nein	Nein
Ubuntu 16.04	Ja	Nein	Nein
Debian 10.7	Ja	Nein	Nein
SUSE 12.5	Ja	Nein	Nein

FAS aktivieren, wenn Sie ein Master-Image auf der Vorlagen-VM vorbereiten

1. Importieren Sie das Stamm-CA-Zertifikat.

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   ```

2. Führen Sie ctxfascfg.sh aus.
3. Legen Sie Variablen in `/etc/xdl/mcs/mcs.conf` fest.
   a. Legen Sie den Wert von `Use_Existing_Configurations_Of_Current_VDA` auf Y fest.
   b. Legen Sie die Variable `FAS_LIST` auf Ihre FAS-Serveradresse oder mehrere FAS-Serveradressen fest, die durch Semikolons getrennt und in doppelten Anführungszeichen eingeschlossen sind, zum Beispiel `FAS_LIST="<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>"`.
   c. Legen Sie die anderen Variablen nach Bedarf fest, wie zum Beispiel `VDI_MODE`.
4. Führen Sie das Skript `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.

FAS auf einer mit MCS erstellten VM aktivieren

Wenn FAS auf der Vorlagenmaschine nicht wie zuvor beschrieben aktiviert ist, können Sie FAS auf jeder mit MCS erstellten VM aktivieren.

Um FAS auf einer mit MCS erstellten VM zu aktivieren, gehen Sie wie folgt vor:

1. Legen Sie Variablen in /etc/xdl/mcs/mcs.conf fest.
   a. Setzen Sie den Wert von `Use_Existing_Configurations_Of_Current_VDA` auf Y.
   b. Setzen Sie die Variable `FAS_LIST` auf Ihre FAS-Serveradresse.
   c. Legen Sie die anderen Variablen nach Bedarf fest, z. B. `VDI_MODE`.

2. Importieren Sie das Stamm-CA-Zertifikat.

```
sudo cp root.pem /etc/pki/CA/certs/
```

3. Führen Sie das Skript `/opt/Citrix/VDA/sbin/ctxfascfg.sh` aus.

Hinweis:

Sie müssen alle erforderlichen Variablen in `/etc/xdl/mcs/mcs.conf` festlegen, da diese Variablen beim Start der VM aufgerufen werden.

Verwenden von Citrix Provisioning™ zum Erstellen von Linux-VMs

Dieser Artikel enthält Informationen zum Streamen von Linux-Zielgeräten. Mit dieser Funktion können Sie virtuelle Linux-Desktops direkt in der Citrix Virtual Apps and Desktops™-Umgebung bereitstellen.

Die folgenden Linux-Distributionen werden unterstützt:

- Ubuntu 16.04
- Ubuntu 18.04
- Ubuntu 20.04
- RHEL 8.3

Wichtig:

- Wir empfehlen die Verwendung des aktuellen Installationspakets, das in der ausführbaren Datei von Citrix Provisioning verfügbar ist, `Citrix_Provisioning_2106.iso`. Verwenden Sie das Paket, das auf Ihrer Linux-Distribution basiert. Citrix Provisioning Server 2106 oder höher ist erforderlich, um den Linux-Streaming-Agent 2106 und höher zu verwenden.

- Wenn Sie Citrix Provisioning zum Streamen von Linux-Zielgeräten verwenden, erstellen Sie eine separate Bootpartition auf dem einzelnen gemeinsam genutzten Datenträger-Image, damit die bereitgestellten Geräte wie erwartet starten können.

Weitere Informationen finden Sie unter Streaming Linux-Zielgeräte in der Citrix Provisioning-Dokumentation.

Delivery Controller für XenDesktop 7.6 und frühere Versionen konfigurieren

XenDesktop 7.6 und frühere Versionen erfordern Änderungen zur Unterstützung des Linux VDA. Für diese Versionen ist ein Hotfix oder ein Updateskript erforderlich. Die Installations- und Überprüfungsanweisungen werden in diesem Artikel bereitgestellt.

Konfiguration des Delivery Controller™ aktualisieren

Wenden Sie für XenDesktop 7.6 SP2 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 mit dem Namen **Update-BrokerServiceConfig.ps1** verwenden, um die Broker Service-Konfiguration zu aktualisieren. Dieses Skript ist im folgenden Paket verfügbar:

- citrix-linuxvda-scripts.zip

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

1. Kopieren Sie das Skript **Update-BrokerServiceConfig.ps1** auf den Delivery Controller-Computer.
2. Öffnen Sie eine Windows PowerShell-Konsole im Kontext des lokalen Administrators.
3. Navigieren Sie zu dem Ordner, der das Skript **Update-BrokerServiceConfig.ps1** enthält.
4. Führen Sie das Skript **Update-BrokerServiceConfig.ps1** aus:

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

Tipp:

Standardmäßig ist PowerShell so konfiguriert, dass die Ausführung von PowerShell-Skripts verhindert wird. Wenn das Skript nicht ausgeführt werden kann, ändern Sie die PowerShell-Ausführungsrichtlinie, bevor Sie es erneut versuchen:

```
Set-ExecutionPolicy Unrestricted
```

Das Skript **Update-BrokerServiceConfig.ps1** aktualisiert die Broker Service-Konfigurationsdatei, indem es neue WCF-Endpunkte verwendet, die vom Linux VDA benötigt werden, und startet den Broker Service neu. Das Skript ermittelt den Speicherort der Broker Service-Konfigurationsdatei automatisch. Eine Sicherungskopie der ursprünglichen Konfigurationsdatei wird im selben Verzeichnis erstellt, wobei **.prelinux** an den Dateinamen angehängt wird.

Diese Änderungen haben keine Auswirkungen auf das Brokering von Windows VDAs, die für die Verwendung derselben Delivery Controller-Farm konfiguriert sind. Eine einzelne Controller-Farm kann Sitzungen für Windows- und Linux-VDAs nahtlos verwalten und vermitteln.

Hinweis:

Der Linux VDA unterstützt Secure ICA® für die Verschlüsselung nicht. Das Aktivieren von Secure ICA auf dem Linux VDA führt zu einem Fehler beim Starten der Sitzung.

Delivery Controller-Konfiguration überprüfen

Nachdem die erforderlichen Konfigurationsänderungen auf einen Delivery Controller angewendet wurden, erscheint die Zeichenfolge **EndpointLinux** fünfmal in der Datei **%PROGRAMFILES%\\Citrix\\Broker\\Service\\BrokerService.exe.config**.

Melden Sie sich an der Windows-Eingabeaufforderung als lokaler Administrator an, um Folgendes zu überprüfen:

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

findstr EndpointLinux BrokerService.exe.config
```

Konfigurieren des Linux VDA

Dieser Abschnitt beschreibt die Funktionen des Linux VDA, einschließlich Funktionsbeschreibung, Konfiguration und Fehlerbehebung.

> **Tipp:**

> Das `xdlcollect` Bash-Skript zum Sammeln von Protokollen ist in die Linux VDA-Software integriert und befindet sich unter /opt/Citrix/VDA/bin. 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 im selben Ordner wie das Skript generiert. `xdlcollect` kann Sie fragen, ob die komprimierte Protokolldatei in Citrix Insight Services (CIS) hochgeladen werden soll. Wenn Sie zustimmen, gibt `xdlcollect` nach Abschluss des Uploads eine Upload_ID zurück. Der Upload entfernt die komprimierte Protokolldatei nicht von Ihrem lokalen Computer. Andere Benutzer können die Upload_ID verwenden, um auf die Protokolldatei in CIS zuzugreifen.

NIS in Active Directory integrieren

Dieser Artikel beschreibt, wie NIS mit Windows Active Directory (AD) auf dem Linux VDA unter Verwendung von SSSD integriert wird. Der Linux VDA wird als Komponente von Citrix Virtual Apps and Desktops betrachtet. Daher fügt er sich nahtlos in die Windows AD-Umgebung ein.

Die Verwendung von NIS als UID- und GID-Anbieter anstelle von AD erfordert, dass die Kontoinformationen (Benutzername- und Kennwortkombinationen) in AD und NIS identisch sind.

> **Hinweis:**

> Die Authentifizierung wird weiterhin vom AD-Server durchgeführt. NIS+ wird nicht unterstützt. Wenn Sie NIS als UID- und GID-Anbieter verwenden, werden die POSIX-Attribute vom Windows-Server nicht mehr verwendet.

> **Tipp:**

> Diese Methode stellt eine veraltete Art der Bereitstellung des Linux VDA dar, die nur für spezielle Anwendungsfälle verwendet wird. Für eine RHEL/CentOS-Distribution befolgen Sie die Anweisungen unter Installieren des Linux Virtual Delivery Agent für RHEL/CentOS. Für eine Ubuntu-Distribution befolgen Sie die Anweisungen unter Installieren des Linux Virtual Delivery Agent für Ubuntu.

> Was ist SSSD?

SSSD ist ein System-Daemon. Seine Hauptfunktion besteht darin, den Zugriff zur Identifizierung und Authentifizierung entfernter Ressourcen über ein gemeinsames Framework bereitzustellen, das Caching und Offline-Unterstützung für das System bieten kann. Es bietet sowohl PAM- als auch NSS-Module und kann zukünftig D-BUS-basierte Schnittstellen für erweiterte Benutzerinformationen unterstützen. Es bietet auch eine bessere Datenbank zum Speichern lokaler Benutzerkonten und erweiterter Benutzerdaten.

NIS in AD integrieren

Gehen Sie wie folgt vor, um NIS in AD zu integrieren:

1. Linux VDA als NIS-Client hinzufügen
2. Domäne beitreten und Host-Keytab mit Samba erstellen
3. SSSD einrichten
4. NSS/PAM konfigurieren
5. Kerberos-Konfiguration überprüfen
6. Benutzerauthentifizierung überprüfen

Linux VDA als NIS-Client hinzufügen

NIS-Client konfigurieren:

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

NIS-Domäne festlegen:

```
ypdomainname nis.domain

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

IP-Adresse für NIS-Server und -Client in **/etc/hosts** hinzufügen:

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

NIS konfigurieren über `authconfig`:

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

nis.domain stellt den Domänennamen des NIS-Servers dar. **server.nis.domain** ist der Hostname des NIS-Servers, der auch die IP-Adresse des NIS-Servers sein kann.

NIS-Dienste konfigurieren:

```
sudo systemctl start rpcbind ypbind



sudo systemctl enable rpcbind ypbind
```

Sicherstellen, dass die NIS-Konfiguration korrekt ist:

```
ypwhich
```

Überprüfen, ob die Kontoinformationen vom NIS-Server verfügbar sind:

```
getent passwd nisaccount
```

Hinweis:

Das **nisaccount** stellt das tatsächliche NIS-Konto auf dem NIS-Server dar. Stellen Sie sicher, dass UID, GID, Home-Verzeichnis und Anmelde-Shell korrekt konfiguriert sind.

Domäne beitreten und Host-Keytab mit Samba erstellen

SSSD bietet keine AD-Client-Funktionen zum Beitreten zur Domäne und zur Verwaltung der System-Keytab-Datei. Es gibt verschiedene Methoden, um diese Funktionen zu erreichen, darunter:

- `adcli`
- `realmd`
- `Winbind`
- `Samba`

Die Informationen in diesem Abschnitt beschreiben nur den Samba-Ansatz. Für `realmd` siehe die Dokumentation des RHEL- oder CentOS-Anbieters. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

Domäne beitreten und Host-Keytab mit Samba erstellen:

Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

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

Konfigurieren Sie den Computer für die Samba- und Kerberos-Authentifizierung:

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

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

Wenn eine DNS-basierte Suche nach dem KDC-Server und dem Realm-Namen erforderlich ist, fügen Sie die folgenden zwei Optionen zum vorhergehenden Befehl hinzu:

`--enablekrb5kdcdns --enablekrb5realmdns`

Öffnen Sie **/etc/samba/smb.conf** und fügen Sie die folgenden Einträge unter dem Abschnitt **\[Global\]** hinzu, aber nach dem Abschnitt, der vom Tool **authconfig** generiert wurde:

`kerberos method = secrets and keytab`

`winbind offline logon = no`

Das Beitreten zur Windows-Domäne erfordert, dass Ihr Domänencontroller erreichbar ist und Sie über ein AD-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

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

`REALM` ist der Kerberos-Realm-Name in Großbuchstaben und `user` ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Domäne besitzt.

SSSD einrichten

Die Einrichtung von SSSD umfasst die folgenden Schritte:

- Installieren Sie die Pakete **sssd-ad** und **sssd-proxy** auf dem Linux-Client-Computer.
- Nehmen Sie Konfigurationsänderungen an verschiedenen Dateien vor (zum Beispiel **sssd.conf**).
- Starten Sie den **sssd-Dienst**.

/etc/sssd/sssd.conf

Eine Beispielkonfiguration für **sssd.conf** (weitere Optionen können bei Bedarf hinzugefügt werden):

```
[sssd]

config_file_version = 2

domains = EXAMPLE

services = nss, pam



[domain/EXAMPLE]

# Uncomment if you need offline logins

# cache_credentials = true

re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?
```

```
P<domain>.+$))|(^(?P<name>[^@\\]+)$))

id_provider = proxy

proxy_lib_name = nis

auth_provider = ad

access_provider = ad



# Should be specified as the long version of the Active Directory domain.

ad_domain = 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.domain.com**, **server.ad.example.com** durch den entsprechenden Wert. Weitere Informationen finden Sie auf der sssd-ad(5) - Linux-Manpage.

Legen Sie den Dateibesitz und die Berechtigungen für **sssd.conf** fest:

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

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

NSS/PAM konfigurieren

RHEL/CentOS:

Verwenden Sie **authconfig**, um SSSD zu aktivieren. Installieren Sie **oddjob-mkhomedir**, um sicherzustellen, dass die Erstellung des Home-Verzeichnisses mit SELinux kompatibel ist:

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


sudo systemctl start sssd


sudo systemctl enable sssd
```

Tipp:

Berücksichtigen Sie bei der Konfiguration der Linux VDA-Einstellungen, dass es für SSSD keine speziellen Einstellungen für den Linux VDA-Client gibt. Für zusätzliche Lösungen im Skript **ctxsetup.sh** verwenden Sie den Standardwert.

Kerberos-Konfiguration überprüfen

Um sicherzustellen, dass Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, überprüfen Sie, ob die Systemdatei **keytab** erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der verfügbaren Schlüssel für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten an. Führen Sie den Kerberos-Befehl **kinit** aus, um den Computer mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit –k MACHINE\$@REALM
```

Die Computer- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Computerkonto zwischengespeichert wurde, indem Sie Folgendes verwenden:

```
sudo klist -ke
```

Benutzerauthentifizierung überprüfen

Verwenden Sie den Befehl **getent**, um zu überprüfen, ob das Anmeldeformat unterstützt wird und ob NSS funktioniert:

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

Der Parameter **DOMAIN** gibt den Kurznamen der Domäne an. Wenn ein anderes Anmeldeformat erforderlich ist, überprüfen Sie dies zuerst mit dem Befehl **getent**.

Die unterstützten Anmeldeformate sind:

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

Um zu überprüfen, ob das SSSD PAM-Modul korrekt konfiguriert ist, verwenden Sie ein Domänenbenutzerkonto, um sich am Linux VDA anzumelden. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

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



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die vom Befehl zurückgegebene **uid** erstellt wurde:

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

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

Anwendungen veröffentlichen

Mit Linux VDA Version 7.13 hat Citrix die Funktion für nahtlose Anwendungen zu allen unterstützten Linux-Plattformen hinzugefügt. Für die Verwendung dieser Funktion sind keine speziellen Installationsverfahren erforderlich.

> **Tipp:**

> Mit Linux VDA Version 1.4 hat Citrix die Unterstützung für nicht-nahtlose veröffentlichte Anwendungen und Sitzungsfreigabe hinzugefügt.

Anwendungen mit Citrix Studio veröffentlichen

Sie können auf einem Linux-VDA installierte Anwendungen veröffentlichen, wenn Sie eine Bereitstellungsgruppe erstellen oder Anwendungen zu einer vorhandenen Bereitstellungsgruppe hinzufügen. Der Prozess ähnelt dem Veröffentlichen von Anwendungen, die auf einem Windows-VDA installiert sind. Weitere Informationen finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation (basierend auf der verwendeten Version von Citrix Virtual Apps and Desktops).

> **Hinweis:**

- Stellen Sie beim Konfigurieren von Bereitstellungsgruppen sicher, dass der Bereitstellungstyp auf **Desktops und Anwendungen** oder **Anwendungen** festgelegt ist.
- Das Veröffentlichen von Anwendungen wird ab Linux VDA Version 1.4 unterstützt. Der Linux VDA unterstützt jedoch nicht die Bereitstellung von Desktops und Apps auf demselben Computer. Um dieses Problem zu beheben, empfehlen wir, separate Bereitstellungsgruppen für App- und Desktopbereitstellungen zu erstellen.
- Um nahtlose Anwendungen zu verwenden, deaktivieren Sie den nahtlosen Modus in StoreFront nicht. Der nahtlose Modus ist standardmäßig aktiviert. Wenn Sie ihn bereits durch Setzen von „TWIMode=Off“ deaktiviert haben, entfernen Sie diese Einstellung, anstatt sie in „TWIMode=On“ zu ändern. Andernfalls können Sie einen veröffentlichten Desktop möglicherweise nicht starten.

Einschränkung

Der Linux VDA unterstützt nicht den Start mehrerer gleichzeitiger Instanzen derselben Anwendung durch einen einzelnen Benutzer.

In einer App-Sitzung funktionieren nur anwendungsspezifische Verknüpfungen wie erwartet.

Bekannte Probleme

Die folgenden bekannten Probleme treten beim Veröffentlichen von Anwendungen auf:

- Nicht-rechteckige Fenster werden nicht unterstützt. Die Ecken eines Fensters zeigen möglicherweise den serverseitigen Hintergrund an.
- Die Vorschau des Fensterinhalts einer veröffentlichten Anwendung wird nicht unterstützt.
- Der nahtlose Modus unterstützt derzeit die folgenden Fenstermanager: Mutter, Metacity und Compiz (Ubuntu 16.04). Kwin und andere Fenstermanager werden nicht unterstützt. Stellen Sie sicher, dass Ihr Fenstermanager auf einen unterstützten eingestellt ist.
- Wenn Sie mehrere LibreOffice-Anwendungen ausführen, wird in Citrix Studio nur die zuerst gestartete angezeigt, da diese Anwendungen den Prozess gemeinsam nutzen.
- Veröffentlichte Qt5-basierte Anwendungen wie „Dolphin“ zeigen möglicherweise keine Symbole an. Informationen zur Behebung des Problems finden Sie im Artikel unter `<https://wiki.archlinux.org/title/Qt>`.
- Alle Taskleistenschaltflächen von veröffentlichten Anwendungen, die in derselben ICA®-Sitzung ausgeführt werden, werden in derselben Gruppe zusammengefasst. Um dieses

Problem zu beheben, legen Sie die Taskleisteneigenschaft so fest, dass Taskleistenschaltflächen nicht kombiniert werden.

Linux VDA-Selbstaktualisierung

Diese Funktion hilft, Ihre Linux VDA-Software automatisch zu aktualisieren – sofort oder zu einem geplanten Zeitpunkt. Dies ist besonders vorteilhaft, wenn Sie Linux-VDAs in Citrix Virtual Apps and Desktops Standard für Azure erstellen. Sie haben keine Administratorrechte für die VMs in Azure. Weitere Informationen finden Sie unter Linux-VDAs in Citrix Virtual Apps and Desktops Standard für Azure erstellen.

Konfiguration

Um diese Funktion zu verwenden, führen Sie die folgenden Schritte aus:

Schritt 1: Aktualisierungsinformationen und neue VDA-Pakete in Ihren Azure-Container hochladen

Schritt 1a: Erstellen Sie einen Container unter Ihrem Azure-Speicherkonto und legen Sie die Zugriffsebene Ihres Containers auf **Blob (Anonymer Lesezugriff nur für Blobs)** fest.

> **Hinweis:**

> Azure-Container und -Blobs werden ausschließlich von Kunden gehalten und verwaltet. Citrix® haftet nicht für Sicherheitsprobleme, die damit verbunden sind. Um Datensicherheit und Kosteneffizienz zu gewährleisten, setzen Sie die Zugriffsebene Ihres Containers nach jeder Selbstaktualisierung auf **Privat (kein anonymer Zugriff)**.

> Schritt 1b: Fügen Sie Ihre VDA-Aktualisierungsinformationen in eine JSON-Datei namens UpdateInfo.json ein. Ein Beispiel für das Dateiformat finden Sie im folgenden Block:

```
{

 "Version": "21.04.200.4",

"Distributions":[

{
```

```
"TargetOS": "RHEL7_9",

"PackageName": "",

"PackageHash": ""

},

{

"TargetOS": "RHEL8_3",

"PackageName": "XenDesktopVDA-21.04.200.4-1.el8_x.x86_64.rpm",

"PackageHash":
"a6f2aba23b84bbc3a4640294a8bb92474e0cacbab1e5ae33416c0a4473a28d73"

},

{

"TargetOS": "UBUNTU16_04",

"PackageName": "",

"PackageHash": ""

},

{

"TargetOS": "UBUNTU18_04",

"PackageName": "xendesktopvda_21.04.200.4-1.ubuntu18.04_amd64.deb",

"PackageHash":
"4148cc3f25d3717e3cbc19bd953b42c72bd38ee3fcd7f7034c2cd6f2b15b3c5a"

},

{

"TargetOS": "UBUNTU20_04",
```

```
"PackageName": "",

"PackageHash": ""

}

]

}
```

Dabei gibt **„Version“** die neue VDA-Version an und **„Distributions“** ist ein Array von Update-Objekten. Jedes Objekt enthält drei Elemente:

- **„TargetOS“**: muss „RHEL7_9“ (für RHEL 7 und CentOS 7), „RHEL8_3“, „UBUNTU16_04“, „UBUNTU18_04“ oder „UBUNTU20_04“ sein. Das `ctxmonitorservice` erkennt keine anderen Distributionen.
- **„PackageName“**: Vollständiger Name des VDA-Pakets der angegebenen Version.
- **„PackageHash“**: Ein SHA-256-Wert, den Sie mit dem Befehl `shasum -a 256 <pkgname>` berechnen.

Schritt 1c: Laden Sie die JSON-Datei und die neue Version der Linux VDA-Pakete in Ihren Azure-Container hoch.

Schritt 2: Aktivieren Sie die Selbstaktualisierungsfunktion auf dem Masterimage oder auf jedem VDA

Standardmäßig ist die Selbstaktualisierung deaktiviert. Wenn Sie Linux-VDAs in Citrix Virtual Apps and Desktops™ Standard für Azure erstellen, muss die Funktionsaktivierung auf dem Masterimage erfolgen. Andernfalls aktivieren Sie die Funktion direkt auf jedem Ziel-VDA.

Um die Selbstaktualisierung zu aktivieren, führen Sie Befehle ähnlich den folgenden aus, um den Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SelfUpdate zu bearbeiten.

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

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"ScheduledTime" -d "Immediately" –force



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



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
```

Die folgende Tabelle beschreibt die Registrierungseinstellungen.

REGISTRIERUNGSEINSTELLUNG	BESCHREIBUNG
fEnabled	Diese Einstellung ist erforderlich. Standardmäßig ist der Wert 0, was bedeutet, dass die Selbstaktualisierung deaktiviert ist. Sie können ihn auf 1 setzen, um die Selbstaktualisierung zu aktivieren.
Url	Diese Einstellung ist erforderlich. Sie legt die URL Ihres Azure-Containers fest, um die Updateinformationen und neue VDA-Pakete abzurufen.
ScheduledTime	Diese Einstellung ist erforderlich. Sie können sie auf **Immediately** oder **NextStart** setzen. **Immediately** bedeutet, ein Update sofort nach dem Herunterladen der VDA-Pakete auszuführen. Diese Option ist geeignet, wenn die Downloadgeschwindigkeit hoch und Ihr Update dringend ist. Sie kann jedoch die Benutzererfahrung beeinträchtigen, wenn während des Paketdownloads Live-Sitzungen vorhanden sind. **NextStart** bedeutet, ein Update beim nächsten Start des

REGISTRIERUNGSEINSTELLUNG	BESCHREIBUNG
	`ctxmonitorservice` auszuführen. Diese Option ist geeignet, wenn die Downloadgeschwindigkeit nicht hoch und Ihr Update nicht dringend ist.
CaCertificate	Diese Einstellung ist optional. Sie legt den vollständigen Pfad eines PEM-Zertifikats fest, um die URL Ihres Azure-Containers zu überprüfen. Für 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 Ihnen, diese Registrierungseinstellung hinzuzufügen, sie wird jedoch nur unter Ubuntu unterstützt. Unter RHEL fehlen einige NSS-Bibliotheken für den `curl`-Befehl. Stellen Sie sicher, dass die geringsten Berechtigungen für das Zertifikat festgelegt sind.

Wenn der `ctxmonitorservice` neu startet, fragt er zuerst die **Url** ab, um die Datei UpdateInfo.json zu erhalten, und ruft die Updateversion aus der JSON-Datei ab. Dann vergleicht der `ctxmonitorservice` die Updateversion mit der aktuellen Version. Wenn die aktuelle Version älter ist, lädt der Dienst die neue Version des VDA-Pakets von Azure herunter und speichert sie lokal. Danach führt er ein Update gemäß der Einstellung von **ScheduledTime** aus. Für eine lokale Bereitstellung können Sie den `ctxmonitorservice` direkt neu starten, um das Update auszulösen. In Citrix Virtual Apps and Desktops Standard für Azure, wo Sie keine Administratorrechte für die VMs haben, kann der `ctxmonitorservice` jedoch erst nach dem Neustart der VDA-Maschine neu gestartet werden. Wenn ein Update fehlschlägt, wird Ihr VDA auf die vorhandene Version zurückgesetzt.

Hinweis:

- Die Registrierungseinstellungen, die Sie auf dem Masterimage konfiguriert haben, können nicht geändert werden.

- Wenn alle VMs in einer Umgebung gleichzeitig ein Paket herunterladen, kann das lokale Netzwerk überlastet werden.
- Wenn sowohl ein Update als auch das Rollback fehlschlagen, gehen Benutzerdaten verloren.
- Wenn ein Update fehlschlägt, das Rollback jedoch erfolgreich ist, haben Benutzer im selben Netzwerk möglicherweise unterschiedliche Versionen des Linux VDA. Dieser Fall ist suboptimal.
- Ein Update dauert in der Regel mehrere Minuten. Es gibt keine Statusanzeige in Citrix Studio.

Remote PC Access

Übersicht

Remote PC Access ist eine Erweiterung von Citrix Virtual Apps and Desktops. Es ermöglicht Unternehmen, ihren Mitarbeitern auf einfache Weise den sicheren Fernzugriff auf ihre physischen Büro-PCs zu 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 Access verwendet dieselben Citrix Virtual Apps™ and Desktops-Komponenten, die virtuelle Desktops und Anwendungen bereitstellen. Die Anforderungen und der Prozess für die Bereitstellung und Konfiguration von Remote PC Access sind dieselben wie die Anforderungen und der Prozess für die Bereitstellung von Citrix Virtual Apps and Desktops zur Bereitstellung virtueller Ressourcen. Diese Einheitlichkeit bietet eine konsistente und einheitliche administrative Erfahrung. Benutzer erhalten die beste Benutzererfahrung durch die Verwendung von Citrix HDX zur Bereitstellung ihrer Remote-Büro-PC-Sitzungen.

Weitere Informationen finden Sie unter Remote PC Access in der Citrix Virtual Apps and Desktops-Dokumentation.

Überlegungen

Diese Überlegungen beziehen sich speziell auf 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 ausgeschaltet werden und zeigt die Aktivitäten der Sitzung an, wenn der HDX™ 3D-Modus aktiviert ist. Das Anzeigen dieses Bildschirms stellt ein potenzielles Sicherheitsrisiko dar.

- Verwenden Sie Maschinenkataloge vom Typ Single-Session-OS für physische Linux-Maschinen.
- Die automatische Benutzerzuweisung ist für Linux-Maschinen nicht verfügbar. Bei der automatischen Benutzerzuweisung werden Benutzer ihren Maschinen automatisch zugewiesen, wenn sie sich lokal an den PCs anmelden. Diese Anmeldung erfolgt ohne Administratorintervention. Die auf dem Clientgerät ausgeführte Citrix Workspace™-App ermöglicht Benutzern den Zugriff auf die Anwendungen und Daten auf dem Büro-PC innerhalb der Remote PC Access-Desktopsitzung.
- Wenn Benutzer bereits lokal an ihren PCs angemeldet sind, schlagen Versuche, die PCs von StoreFront™ aus zu starten, fehl.
- Energiesparoptionen sind für Linux-Maschinen nicht verfügbar.

Konfiguration

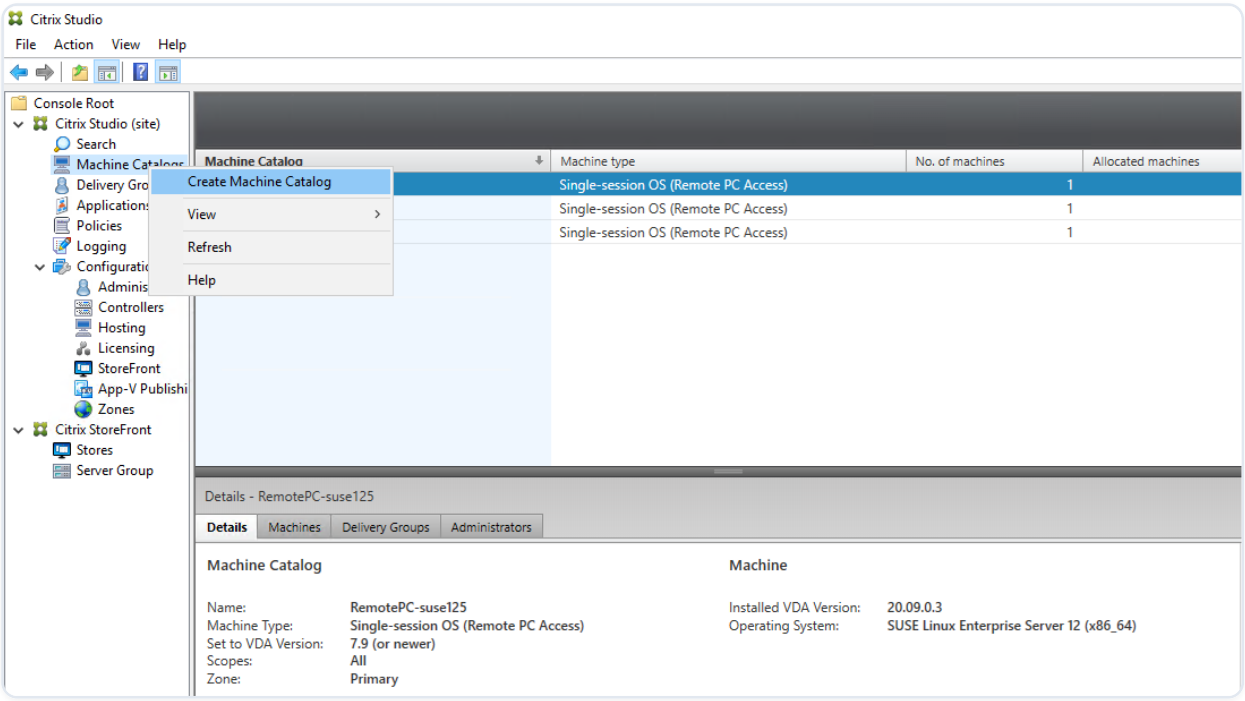
Um Linux-PC-Sitzungen bereitzustellen, installieren Sie den Linux VDA auf den Ziel-PCs, erstellen Sie einen Maschinenkatalog vom Typ **Remote PC Access** und erstellen Sie eine Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern. Der folgende Abschnitt beschreibt das Verfahren:

Schritt 1 – Installieren Sie den Linux VDA auf den Ziel-PCs

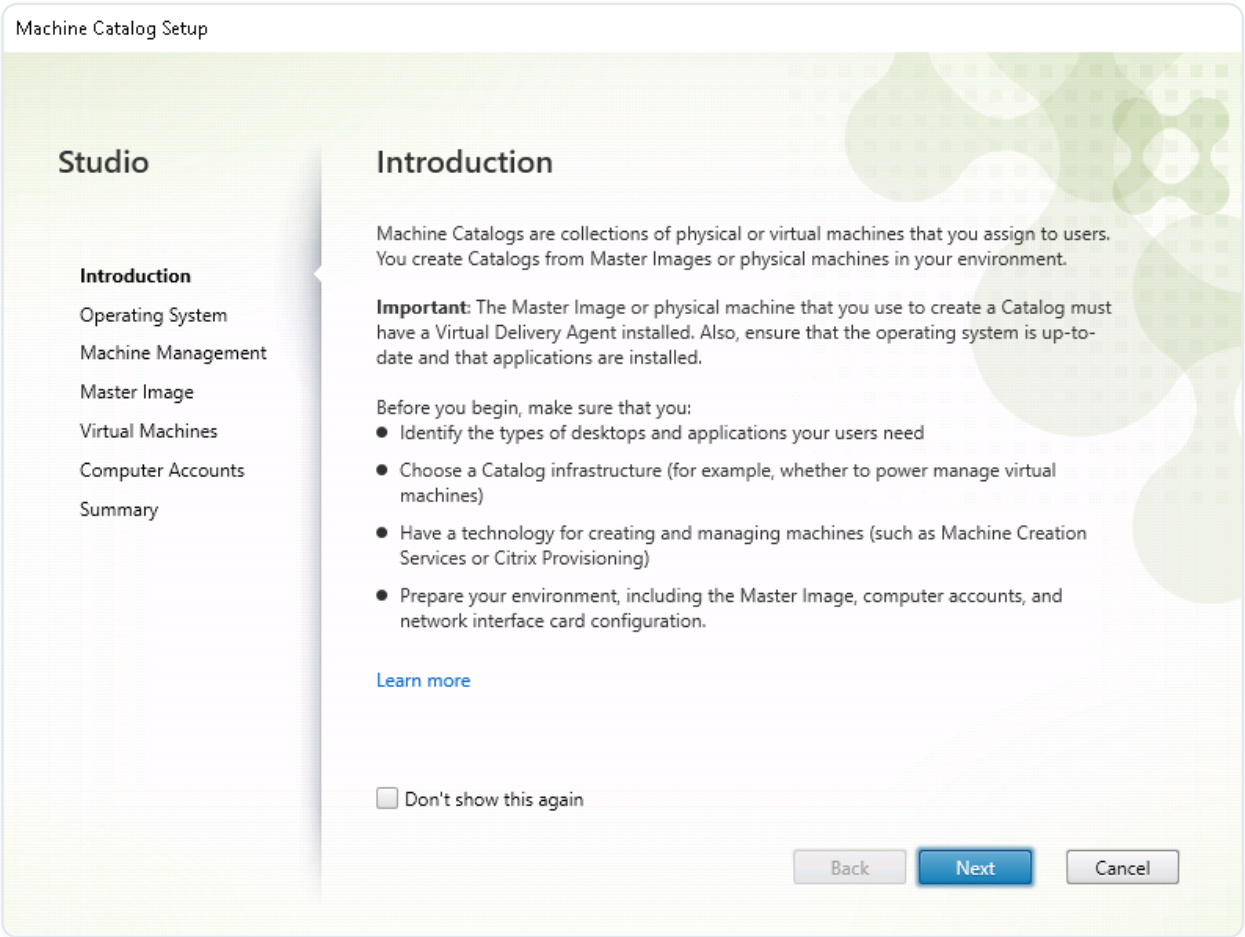
Wir empfehlen Ihnen, easy install zur Installation des Linux VDA zu verwenden. Legen Sie während der Installation den Wert der Variablen `CTX_XDL_VDI_MODE` auf `Y` fest.

Schritt 2 – Erstellen Sie einen Maschinenkatalog vom Typ Remote PC Access

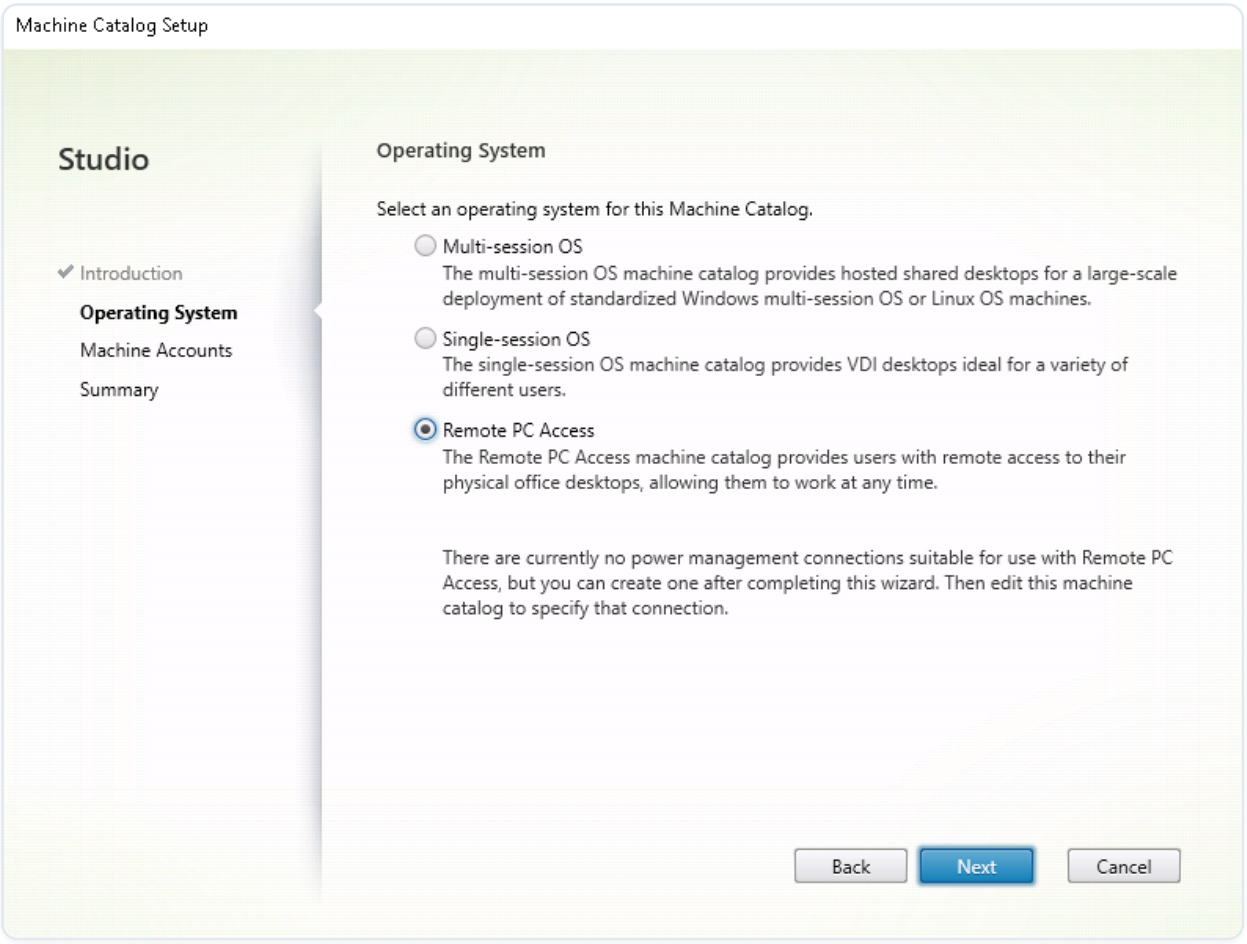
1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Maschinenkataloge** und wählen Sie im Kontextmenü **Maschinenkatalog erstellen** aus.



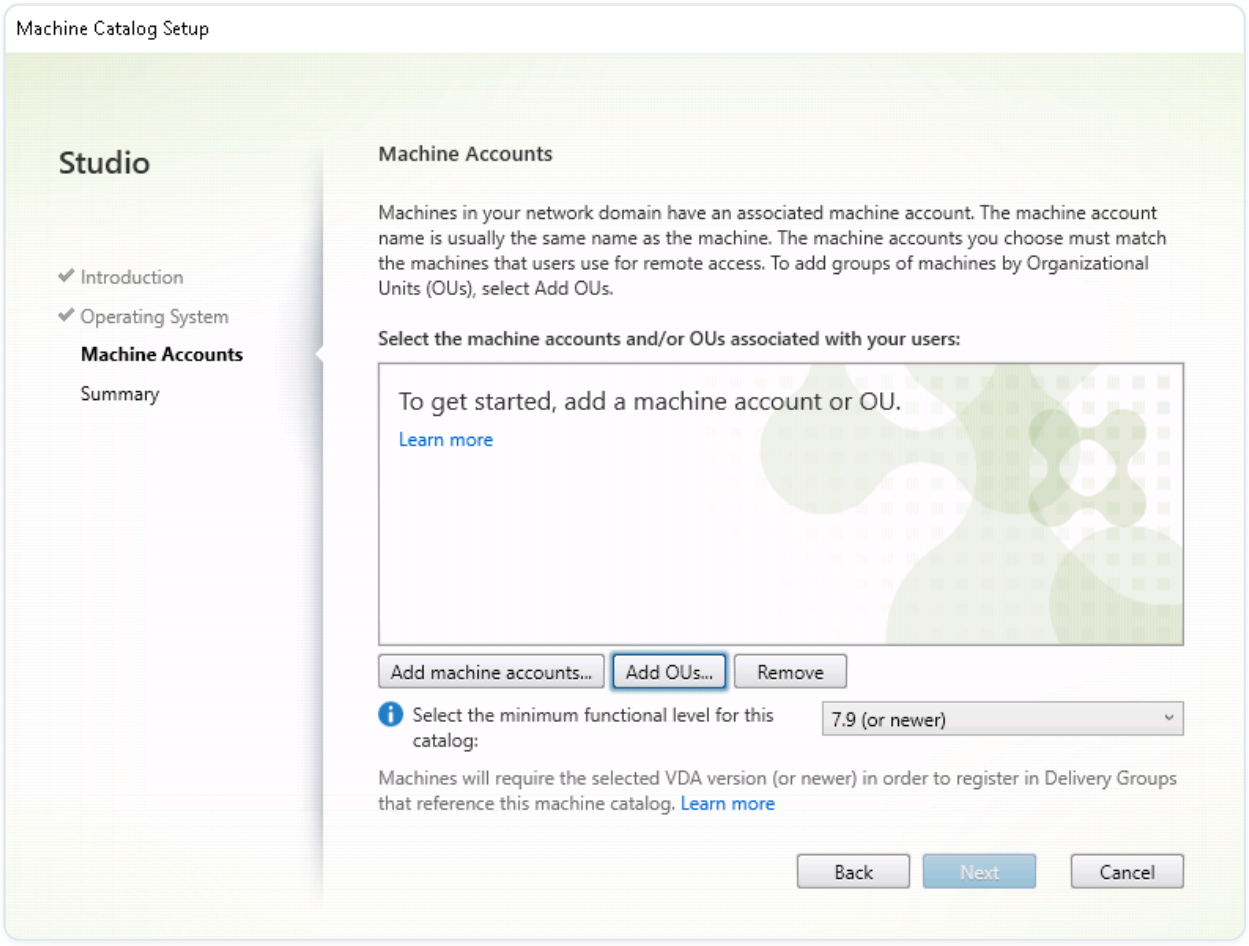
2. Klicken Sie auf der Seite **Einführung** auf **Weiter**.



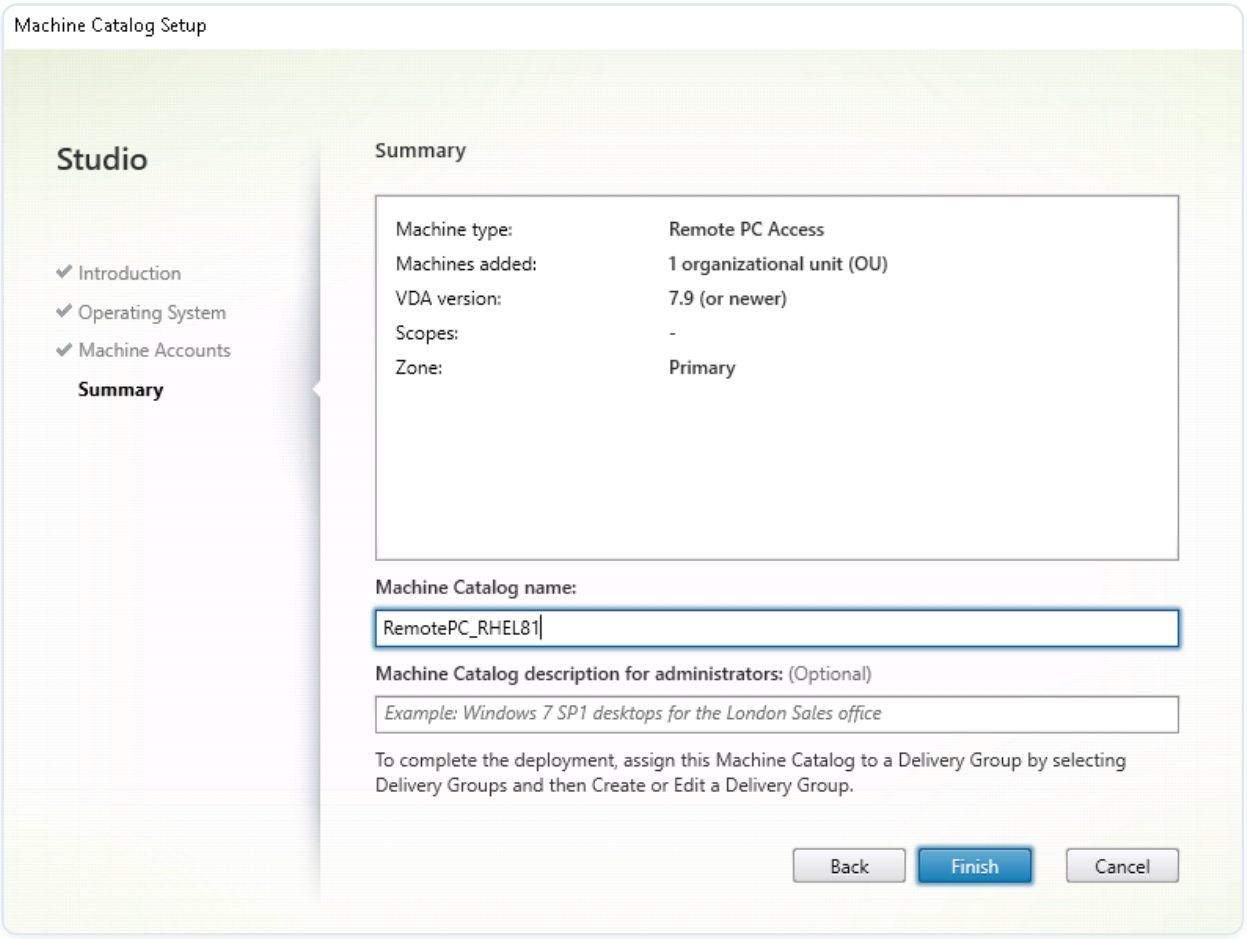
3. Wählen Sie auf der Seite **Betriebssystem** die Option **Remote PC Access** aus.



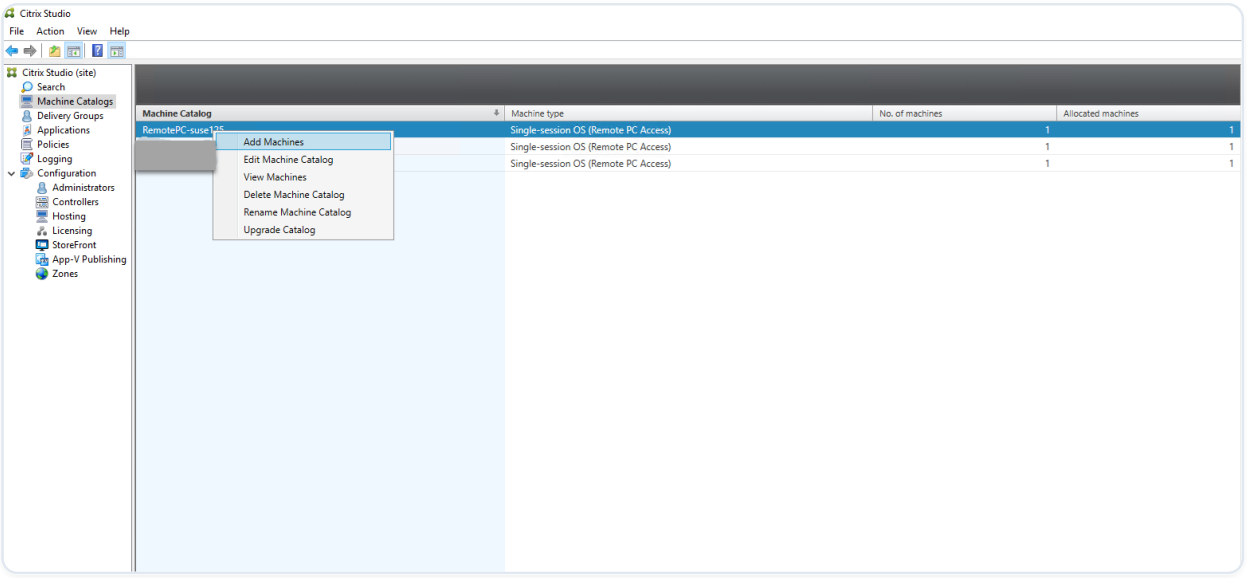
4. Klicken Sie auf **OUs hinzufügen**, um OUs auszuwählen, die die Ziel-PCs enthalten, oder klicken Sie auf **Maschinenkonten hinzufügen**, um einzelne Maschinen zum Maschinenkatalog hinzuzufügen.



5. Benennen Sie den Maschinenkatalog.

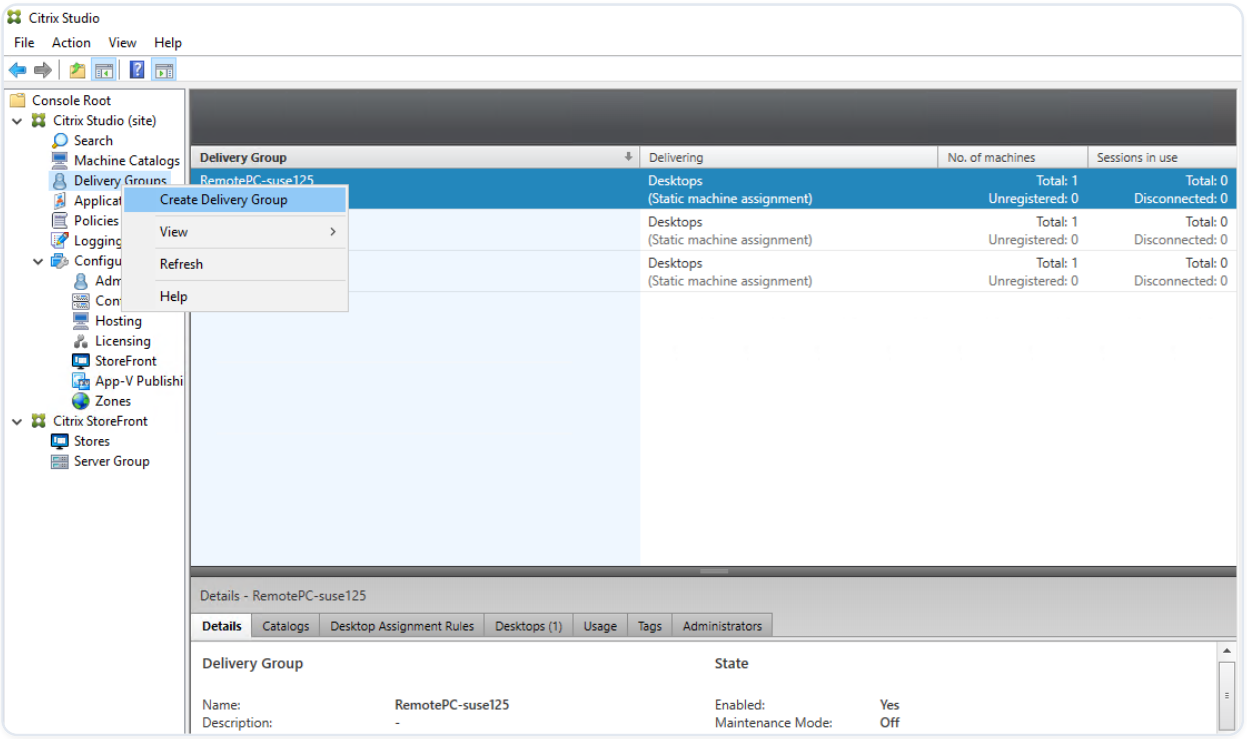


6. (Optional) Klicken Sie mit der rechten Maustaste auf den Maschinenkatalog, um relevante Operationen durchzuführen.

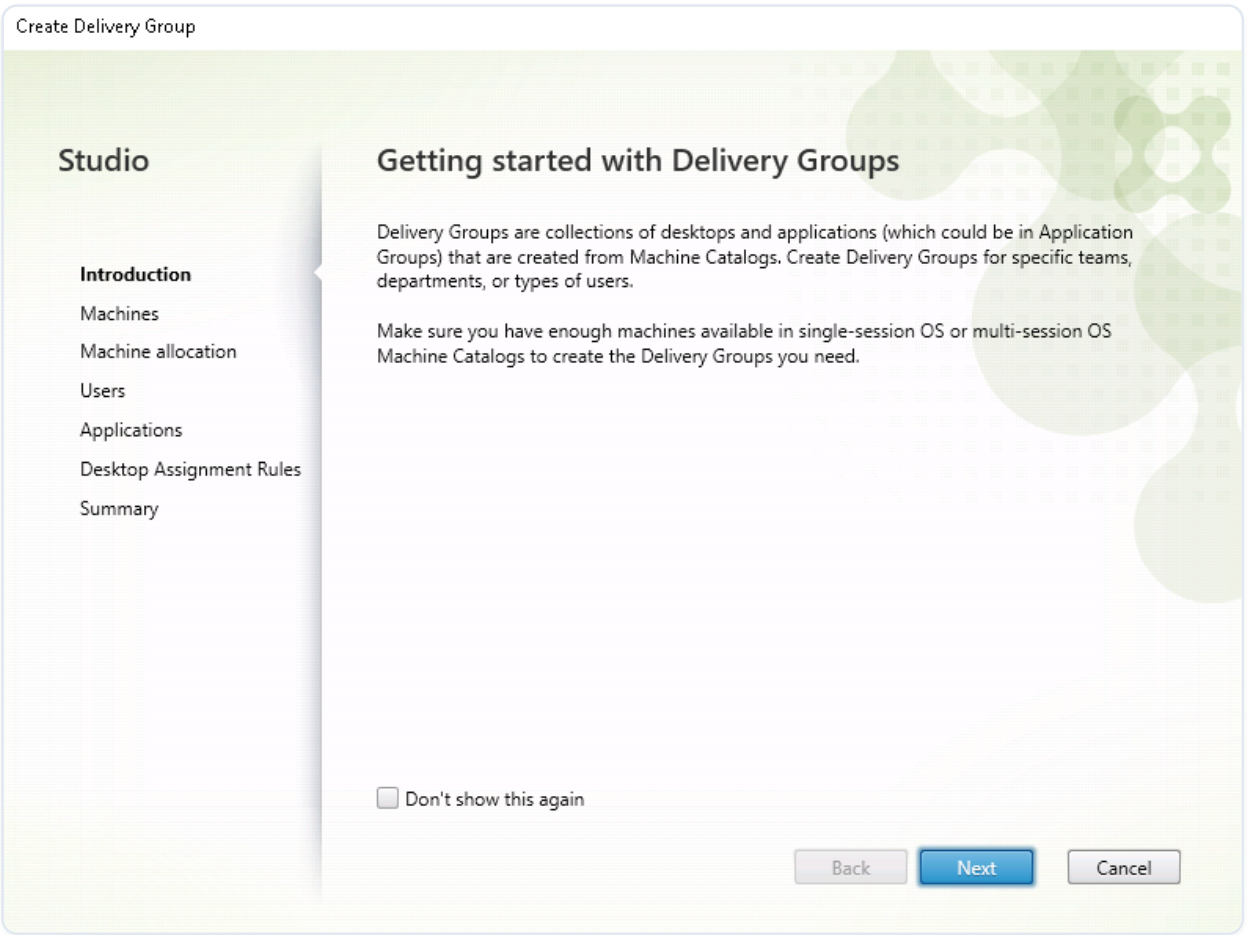


Schritt 3 – Erstellen Sie eine Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern

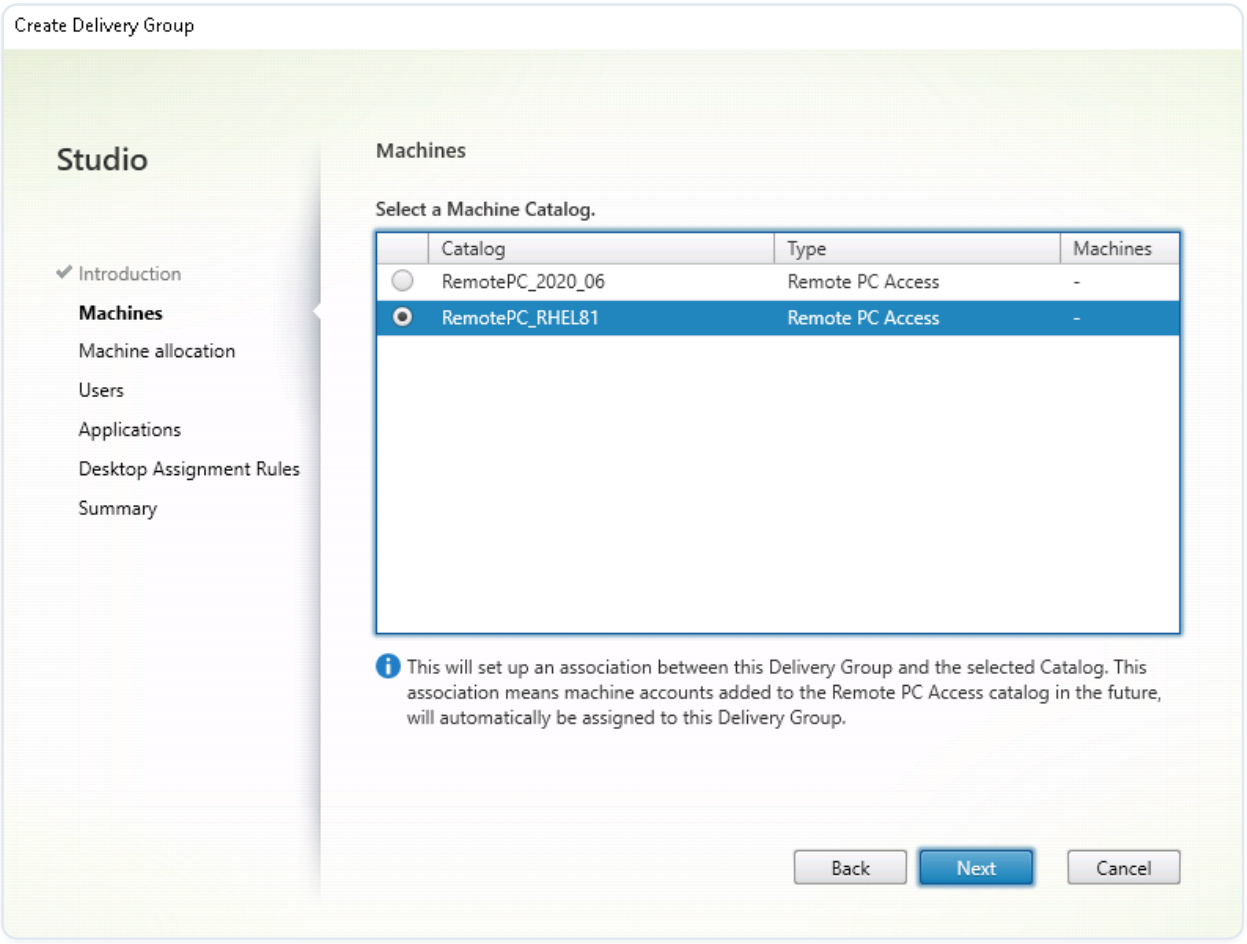
1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Bereitstellungsgruppen** und wählen Sie im Kontextmenü **Bereitstellungsgruppe erstellen** aus.



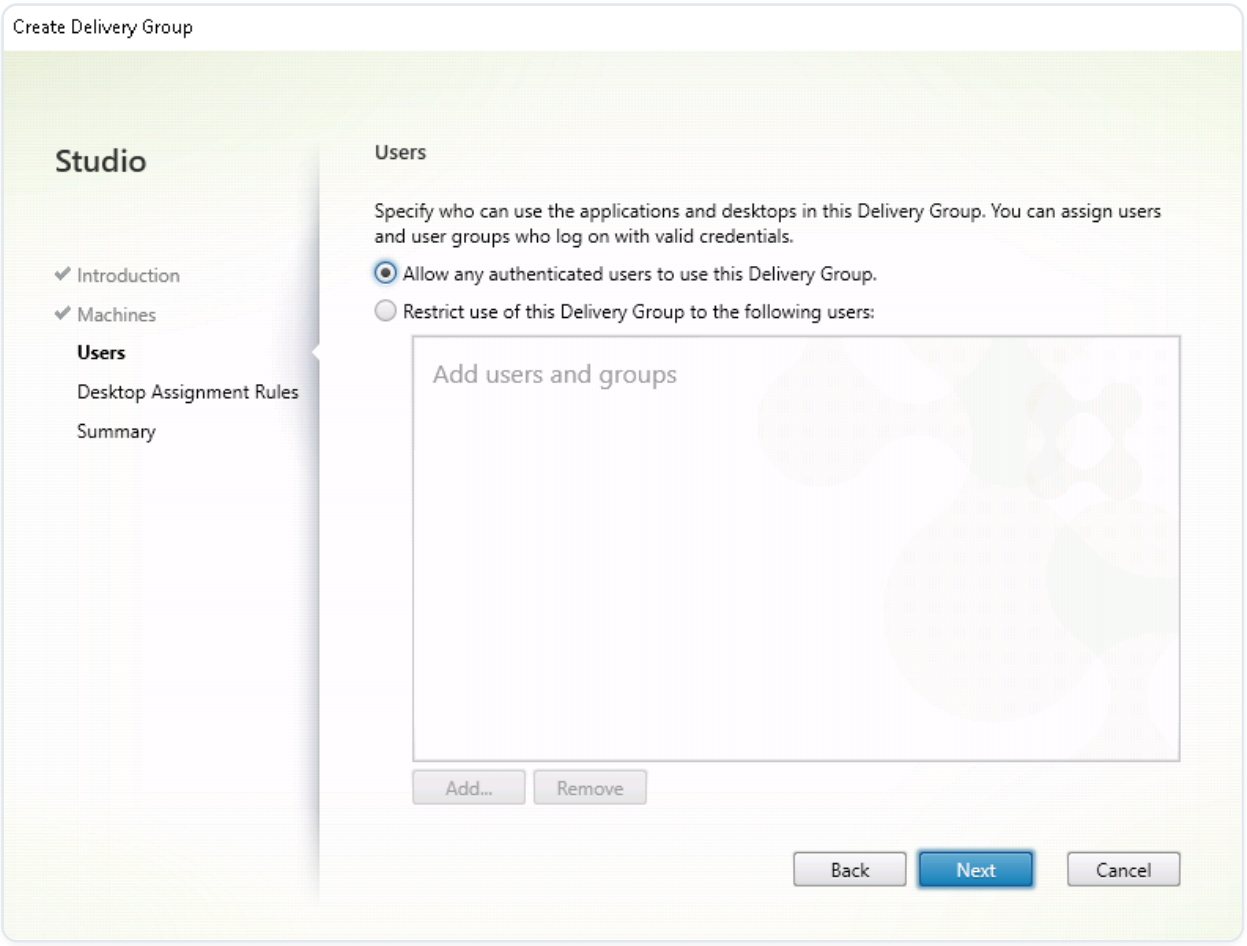
2. Klicken Sie auf der Seite **Erste Schritte mit Bereitstellungsgruppen** auf **Weiter**.



3. Wählen Sie den in Schritt 2 erstellten Maschinenkatalog aus, um ihn der Bereitstellungsgruppe zuzuordnen.



4. Fügen Sie Benutzer hinzu, die auf die PCs im Maschinenkatalog zugreifen können. Die hinzugefügten Benutzer können die Citrix Workspace-App auf einem Clientgerät verwenden, um remote auf die PCs zuzugreifen.



Wake on LAN

Remote PC Access unterstützt Wake on LAN, wodurch Benutzer physische PCs remote einschalten können. Diese Funktion ermöglicht es Benutzern, ihre Büro-PCs bei Nichtgebrauch ausgeschaltet zu lassen, um Energiekosten zu sparen. Sie ermöglicht auch den Fernzugriff, wenn ein Computer versehentlich ausgeschaltet wurde.

Mit der Wake-on-LAN-Funktion werden die Magic Pakete direkt vom auf dem PC ausgeführten VDA an das Subnetz gesendet, in dem sich der PC befindet, wenn dies vom Delivery Controller angewiesen wird. Dadurch kann die Funktion ohne Abhängigkeiten von zusätzlichen Infrastrukturkomponenten oder Drittanbieterlösungen für die Zustellung von Magic Paketen arbeiten.

Die Wake-on-LAN-Funktion unterscheidet sich von der älteren SCCM-basierten Wake-on-LAN-Funktion. Informationen zum SCCM-basierten Wake-on-LAN finden Sie unter Wake on LAN – SCCM-integriert.

Systemanforderungen

Die folgenden Systemanforderungen gelten für die Verwendung der Wake on LAN-Funktion:

- Steuerungsebene:
  - Citrix Virtual Apps and Desktops Dienst
  - Citrix Virtual Apps and Desktops 2012 oder höher
- Physische PCs:
  - VDA-Version 2012 oder höher
  - Wake-on-LAN im BIOS und auf der NIC aktiviert

Wake-on-LAN konfigurieren

Derzeit wird die Konfiguration von integriertem Wake-on-LAN nur über PowerShell unterstützt.

So konfigurieren Sie Wake-on-LAN:

1. Erstellen Sie den Maschinenkatalog für Remote-PC-Zugriff, falls Sie noch keinen haben.
2. Erstellen Sie die Wake on LAN-Hostverbindung, falls Sie noch keine haben.

> **Hinweis:**
>
> Um die Wake-on-LAN-Funktion zu verwenden, erstellen Sie eine Hostverbindung, wenn Sie eine Hostverbindung vom Typ „Microsoft Configuration Manager Wake-on-LAN“ haben.

3. Rufen Sie die eindeutige Kennung der Wake on LAN-Hostverbindung ab.
4. Ordnen Sie die Wake on LAN-Hostverbindung einem Maschinenkatalog zu.

   So erstellen Sie die Wake on LAN-Hostverbindung:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"
```

```
# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
            -Name $connectionName `
            -HypervisorAddress "N/A" `
            -UserName "woluser" `
            -Password "wolpwd" `
            -ConnectionType Custom `
            -PluginId VdaWOLMachineManagerFactory `
            -CustomProperties "<CustomProperties></CustomProperties>" `
            -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{
    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
}
```

Wenn die Hostverbindung bereit ist, führen Sie die folgenden Befehle aus, um die eindeutige Kennung der Hostverbindung abzurufen:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

Nachdem Sie die eindeutige Kennung der Verbindung abgerufen haben, führen Sie die folgenden Befehle aus, um die Verbindung mit dem Remote-PC-Zugriff-Maschinenkatalog zu verknüpfen:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

5. Aktivieren Sie Wake-on-LAN im BIOS und auf der NIC jeder VM im Maschinenkatalog.

   Hinweis: Die Methode zum Aktivieren von Wake-on-LAN variiert je nach Maschinenkonfiguration.

   - So aktivieren Sie Wake-on-LAN im BIOS:

     a. Rufen Sie das BIOS auf und aktivieren Sie die Wake-on-LAN-Funktion.

        Die Methode für den Zugriff auf das BIOS hängt vom Hersteller Ihres Motherboards und dem vom Hersteller ausgewählten BIOS-Anbieter ab.

     b. Speichern Sie Ihre Einstellungen und starten Sie die Maschine neu.

   - So aktivieren Sie Wake-on-LAN auf der NIC:

     a. Führen Sie den Befehl `sudo ethtool <NIC>` aus, um zu prüfen, ob Ihre NIC Magic Packets unterstützt.

        `<NIC>` ist der Gerätename Ihrer NIC, z. B. `eth0`. Der Befehl `sudo ethtool <NIC>` liefert eine Ausgabe über die Funktionen Ihrer NIC:

        - Wenn die Ausgabe eine Zeile ähnlich `Supports Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` enthält, unterstützt Ihre NIC die Wake on LAN Magic Packet Methode.
        - Wenn die Ausgabe eine Zeile ähnlich `Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` enthält und nicht den Buchstaben `d` enthält, ist

die Wake on LAN Magic Packet Methode aktiviert. Wenn jedoch `<letters>` den Buchstaben `d` enthält, bedeutet dies, dass die Wake on LAN Funktion deaktiviert ist. Aktivieren Sie in diesem Fall Wake on LAN, indem Sie den Befehl `sudo ethtool -s <NIC> wol g` ausführen.

b. Auf den meisten Distributionen ist der Befehl `sudo ethtool -s <NIC> wol g` nach jedem Start erforderlich. Um diese Option dauerhaft einzustellen, führen Sie die folgenden Schritte basierend auf Ihren Distributionen aus:

Ubuntu:

Fügen Sie die Zeile `up ethtool -s <NIC> wol g` zur Schnittstellenkonfigurationsdatei `/etc/network/interfaces` hinzu. Zum Beispiel:

```
# ifupdown has been replaced by netplan(5) on this system. See

# /etc/netplan for current configuration.

# To re-enable ifupdown on this system, you can run:

# sudo apt install ifupdown

auto eth0

iface eth0 inet static

           address 10.0.0.1

           netmask 255.255.240.0

           gateway 10.0.0.1

           up ethtool -s eth0 wol g
```

RHEL/SUSE:

Fügen Sie den folgenden Parameter `ETHTOOL_OPTS` zur Schnittstellenkonfigurationsdatei `/etc/sysconfig/network-scripts/ifcfg-<NIC>` hinzu:

```
ETHTOOL_OPTS="-s ${DEVICE} wol g"
```

Designüberlegungen

Wenn Sie Wake on LAN mit Remote-PC-Zugriff verwenden möchten, beachten Sie Folgendes:

- Mehrere Maschinenkataloge können dieselbe Wake on LAN-Hostverbindung verwenden.
- Damit ein PC einen anderen PC aufwecken kann, müssen sich beide PCs im selben Subnetz befinden und dieselbe Wake on LAN-Hostverbindung verwenden. Es spielt keine Rolle, ob sich die PCs in denselben oder verschiedenen 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. Dasselbe gilt für Maschinenkataloge.
- Magic Pakete werden über die globale Broadcast-Adresse 255.255.255.255 gesendet. Stellen Sie sicher, dass die Adresse nicht blockiert ist.
- Es muss mindestens ein PC im Subnetz eingeschaltet sein – für jede Wake-on-LAN-Verbindung –, um Maschinen in diesem Subnetz aufwecken zu können.

Betriebliche Überlegungen

Im Folgenden sind Überlegungen zur Verwendung der Wake-on-LAN-Funktion aufgeführt:

- Der VDA muss sich mindestens einmal registrieren, bevor der PC mithilfe der integrierten Wake-on-LAN-Funktion aufgeweckt werden kann.
- Wake on LAN kann nur zum Aufwecken von PCs verwendet werden. Es unterstützt keine anderen Energieaktionen, wie Neustart oder Herunterfahren.
- Nachdem die Wake on LAN Verbindung erstellt wurde, ist sie in Studio sichtbar. Das Bearbeiten ihrer Eigenschaften innerhalb von Studio wird jedoch nicht unterstützt.
- Magic Pakete werden auf eine von zwei Arten gesendet:
  - Wenn ein Benutzer versucht, eine Sitzung auf seinem PC zu starten und der VDA nicht registriert ist
  - Wenn ein Administrator manuell einen Einschaltbefehl von Studio oder PowerShell sendet
- Da der Delivery Controller den Energiezustand eines PCs nicht kennt, zeigt Studio unter Energiezustand **Nicht unterstützt** an. Der Delivery Controller verwendet den VDA-Registrierungsstatus, um festzustellen, ob ein PC ein- oder ausgeschaltet ist.

Weitere Ressourcen

Im Folgenden finden Sie weitere Ressourcen für den Remote-PC-Zugriff:

- Leitfaden für das Lösungsdesign: Entscheidungen zum Design des Remote-PC-Zugriffs.
- Beispiele für Architekturen für den Remote-PC-Zugriff: Referenzarchitektur für die Citrix Remote-PC-Zugriffslösung.

Drucken

Dieser Artikel enthält Informationen zu Best Practices für den Druck.

Installation

Der Linux-VDA erfordert sowohl **cups**- als auch **foomatic**-Filter. Die Filter werden bei der Installation des VDA installiert. Sie können die Filter auch manuell je nach Distribution installieren. Beispiel:

Unter RHEL 7:

```
sudo yum –y install cups



sudo yum -y install foomatic-filters
```

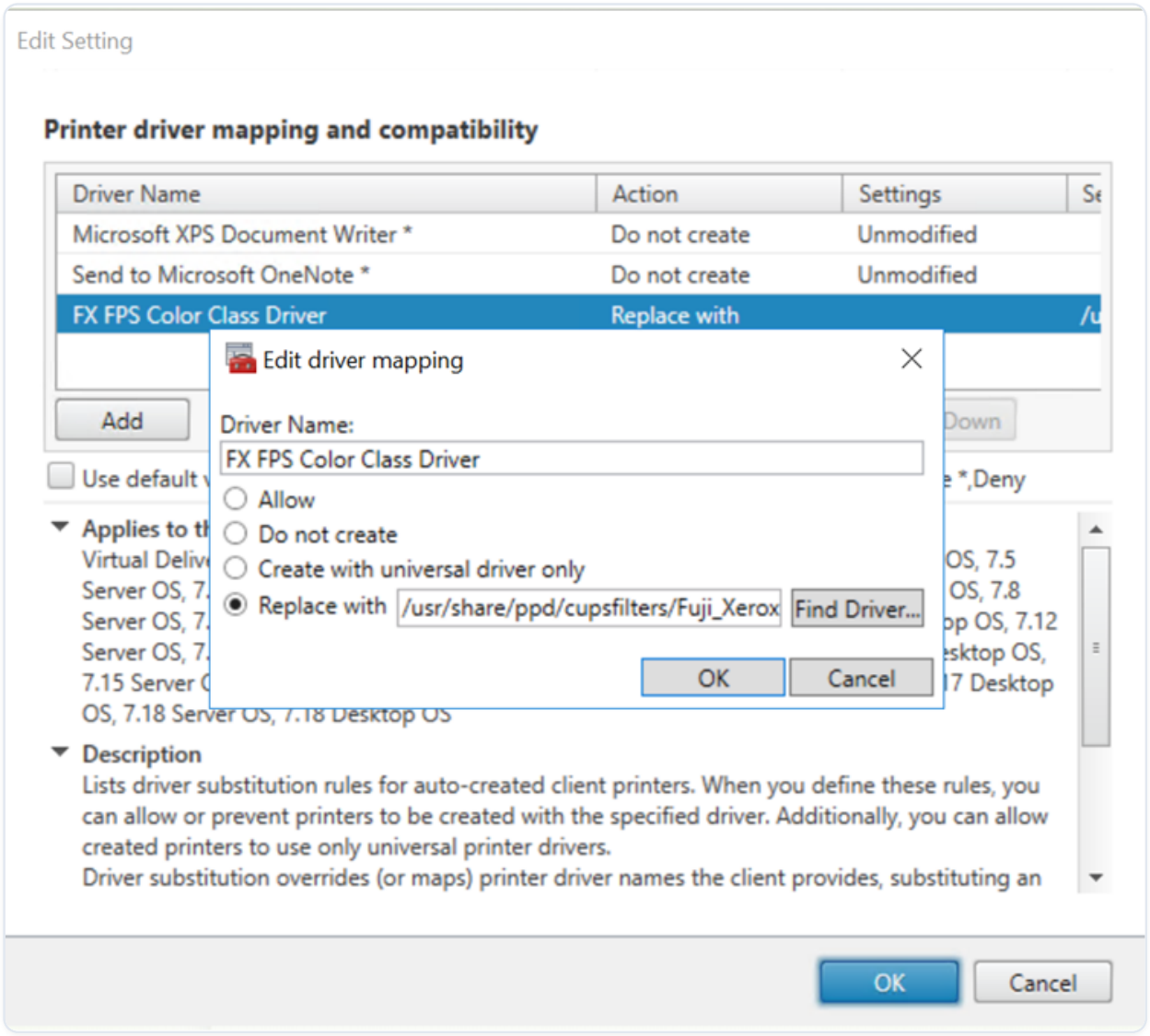
Konfiguration

Citrix stellt drei Arten von universellen Druckertreibern bereit (PostScript, PCL5 und PCL6). Der universelle Druckertreiber ist jedoch möglicherweise nicht mit Ihrem Clientdrucker kompatibel. In diesem Fall bestand Ihre einzige Option in früheren Releases darin, die Konfigurationsdatei ~/.CtxlpProfile$CLIENT_NAME zu bearbeiten. Ab Version 1906 können Sie stattdessen die Richtlinie **Druckertreiberzuordnung und -kompatibilität** in Citrix Studio konfigurieren.

So konfigurieren Sie die 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. Wenn Sie die Citrix Workspace™-App für Linux verwenden, 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. Nur **Ersetzen durch** wird wirksam.

Verwendung

Sie können sowohl von veröffentlichten Desktops als auch von veröffentlichten Anwendungen drucken. Nur der clientseitige Standarddrucker wird einer Linux-VDA-Sitzung zugeordnet. Die Druckernamen sind für Desktops und Anwendungen unterschiedlich:

- Für veröffentlichte Desktops:

`CitrixUniversalPrinter:$CLIENT_NAME:dsk$SESSION_ID`

- Für veröffentlichte Anwendungen:

`CitrixUniversalPrinter:$CLIENT_NAME:app$SESSION_ID`

> **Hinweis:**
>
> Wenn derselbe Benutzer sowohl einen veröffentlichten Desktop als auch eine veröffentlichte Anwendung öffnet, stehen beide Drucker der Sitzung zur Verfügung. Das Drucken auf einem Desktop-Drucker in einer veröffentlichten Anwendungssitzung oder das Drucken auf einem Anwendungsdrucker in einem veröffentlichten Desktop schlägt fehl.

Problembehandlung

Drucken nicht möglich

Wenn das Drucken nicht ordnungsgemäß funktioniert, überprüfen Sie den Druck-Daemon, **ctxlpmngt**, und das CUPS-Framework.

Der Druck-Daemon, **ctxlpmngt**, ist ein pro-Sitzung-Prozess und muss für die Dauer der Sitzung ausgeführt werden. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Druck-Daemon ausgeführt wird. Wenn **ctxlpmngt** nicht ausgeführt wird, starten Sie **ctxlpmngt** manuell über die Befehlszeile.

```
ps –ef | grep ctxlpmngt
```

Wenn das Drucken immer noch nicht funktioniert, überprüfen Sie das CUPS-Framework. Der Dienst **ctxcups** wird für die Druckerverwaltung verwendet und kommuniziert mit dem Linux CUPS-Framework. Es handelt sich um einen einzelnen Prozess pro Maschine, der mit dem folgenden Befehl überprüft werden kann:

```
service ctxcups status
```

Zusätzliche Schritte zum Sammeln von CUPS-Protokollen

Um CUPS-Protokolle zu sammeln, führen Sie die folgenden Befehle aus, um die CUPS-Dienstdatei zu konfigurieren. Andernfalls können CUPS-Protokolle nicht in **hdx.log** aufgezeichnet werden:

```
sudo service cups stop


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


PrivateTmp=false


sudo service cups start


sudo systemctl daemon-reload
```

Hinweis:

Diese Konfiguration dient nur zum Sammeln des vollständigen Druckprotokolls, wenn ein Problem auftritt. Unter normalen Umständen wird diese Konfiguration nicht empfohlen, da sie die CUPS-Sicherheit beeinträchtigt.

Druckausgabe ist fehlerhaft

Ein inkompatibler Druckertreiber kann zu einer fehlerhaften Ausgabe führen. Eine treiberbezogene Konfiguration pro Benutzer ist verfügbar und kann durch Bearbeiten der Konfigurationsdatei **~/.CtxlpProfile$CLIENT_NAME** vorgenommen werden:

```
[DEFAULT_PRINTER]


printername=


model=
```

```
ppdpath=


drivertype=
```

Wichtig:

Das Feld **printername** enthält den Namen des aktuellen clientseitigen Standarddruckers. Es ist ein schreibgeschützter Wert. Bearbeiten Sie ihn nicht.

Die Felder **ppdpath**, **model** und **drivertype** können nicht gleichzeitig festgelegt werden, da nur eines für den zugeordneten Drucker wirksam wird.

- Wenn der Universelle Druckertreiber nicht mit dem Client-Drucker kompatibel ist, konfigurieren Sie das Modell des nativen Druckertreibers mit der Option **model**=. Den aktuellen Modellnamen des Druckers finden Sie mit dem Befehl **lpinfo**:

  ```
  lpinfo –m


  …


  xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0


  xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

  xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
  ```

  Sie können dann das Modell an den Drucker anpassen:

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

- Wenn der Universelle Druckertreiber nicht mit dem Client-Drucker kompatibel ist, konfigurieren Sie den PPD-Dateipfad des nativen Druckertreibers. Der Wert von **ppdpath** ist der absolute Pfad der nativen Druckertreiberdatei.

  Zum Beispiel gibt es einen **ppd driver** unter /home/tester/NATIVE_PRINTER_DRIVER.ppd:

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

- Citrix liefert drei Arten von Universal Printer Driver (PostScript, PCL5 und PCL6). Sie können den Treibertyp basierend auf den Eigenschaften Ihres Druckers konfigurieren.

  Wenn der Standarddruckertreibertyp des Clients beispielsweise PCL5 ist, setzen Sie **drivertype** auf:

  ```
  drivertype=pcl5
  ```

Ausgabegröße ist null

Probieren Sie verschiedene Druckertypen aus. Und versuchen Sie es mit einem virtuellen Drucker wie CutePDF und PDFCreator, um herauszufinden, ob dieses Problem mit dem Druckertreiber zusammenhängt.

Der Druckauftrag hängt vom Druckertreiber des Standarddruckers des Clients ab. Es ist wichtig, den Typ des aktuell aktiven Treibertyps zu identifizieren. Wenn der Clientdrucker einen PCL5-Treiber verwendet, der Linux VDA jedoch einen PostScript-Treiber wählt, kann ein Problem auftreten.

Wenn der Druckertreibertyp korrekt ist, können Sie das Problem durch Ausführen der folgenden Schritte identifizieren:

1. Melden Sie sich bei einer veröffentlichten Desktopsitzung an.
2. Führen Sie den Befehl **vi ~/.CtxlpProfile$CLIENT_NAME** aus.
3. Fügen Sie das folgende Feld hinzu, um die Spool-Datei auf dem Linux VDA zu speichern:

   ```
   deletespoolfile=no
   ```

4. Melden Sie sich ab und wieder an, um die Konfigurationsänderungen zu laden.

5. Drucken Sie das Dokument, um das Problem zu reproduzieren. Nach dem Drucken wird eine Spool-Datei unter **/var/spool/cups-ctx/$logon_user/$spool_file** gespeichert.
6. Überprüfen Sie, ob der Spool leer ist. Wenn die Spool-Datei null ist, deutet dies auf ein Problem hin. Wenden Sie sich an den Citrix Support (und stellen Sie das Druckprotokoll bereit), um weitere Unterstützung zu erhalten.
7. Wenn die Spool-Größe nicht null ist, kopieren Sie die Datei auf den Client. Der Inhalt der Spool-Datei hängt vom Druckertreibertyp des Standarddruckers des Clients ab. Wenn der Treiber des zugeordneten (nativen) Druckers PostScript ist, kann die Spool-Datei direkt im Linux-Betriebssystem geöffnet werden. Überprüfen Sie, ob der Inhalt korrekt ist.

   Wenn die Spool-Datei PCL ist oder wenn das Client-Betriebssystem Windows ist, kopieren Sie die Spool-Datei auf den Client und drucken Sie sie auf dem clientseitigen Drucker mit einem anderen Druckertreiber.
8. Ändern Sie den zugeordneten Drucker, um einen anderen Druckertreiber zu verwenden. Das folgende Beispiel verwendet den PostScript-Clientdrucker als Beispiel:

   a. Melden Sie sich bei einer aktiven Sitzung an und öffnen Sie einen Browser auf dem Client-Desktop.
   b. Öffnen Sie das Druckverwaltungsportal:

      ```
      localhost:631
      ```

   c. Wählen Sie den zugeordneten Drucker **CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID** und **Drucker ändern**. Dieser Vorgang erfordert Administratorrechte.
   d. Behalten Sie die cups-ctx-Verbindung bei und klicken Sie dann auf Weiter, um den Druckertreiber zu ändern.
   e. Wählen Sie in den Feldern **Hersteller** und **Modell** einen anderen Druckertreiber als den Citrix UPD-Treiber aus. Wenn beispielsweise der virtuelle CUPS-PDF-Drucker installiert ist, wählen Sie den generischen CUPS-PDF-Druckertreiber aus. Speichern Sie die Änderung.
   f. Wenn dieser Vorgang erfolgreich ist, konfigurieren Sie den PPD-Dateipfad des Treibers in **.CtxlpProfile** damit der zugeordnete Drucker den neu ausgewählten Treiber verwenden kann.

Bekannte Probleme

Die folgenden Probleme wurden beim Drucken auf dem Linux VDA festgestellt:

CTXPS-Treiber ist nicht mit einigen PLC-Druckern kompatibel

Wenn Sie auf eine Beschädigung der Druckausgabe stoßen, stellen Sie den Druckertreiber auf den nativen Treiber ein, der vom Hersteller bereitgestellt wird.

Langsame Druckleistung bei großen Dokumenten

Wenn Sie ein großes Dokument auf einem lokalen Client-Drucker drucken, wird das Dokument über die Serververbindung übertragen. Bei langsamen Verbindungen kann die Übertragung lange dauern.

Drucker- und Druckauftragsbenachrichtigungen aus anderen Sitzungen sichtbar

Linux hat nicht dasselbe Sitzungskonzept wie das Windows-Betriebssystem. Daher erhalten alle Benutzer systemweite Benachrichtigungen. Sie können diese Benachrichtigungen deaktivieren, indem Sie die CUPS-Konfigurationsdatei ändern: **/etc/cups/cupsd.conf**.

Suchen Sie den aktuellen Richtliniennamen, der in der Datei konfiguriert ist:

`DefaultPolicy default`

Wenn der Richtlinienname *default* ist, fügen Sie die folgenden Zeilen zum XML-Block der Standardrichtlinie hinzu:

```
<Policy default>

    # Job/subscription privacy...

    JobPrivateAccess default

    JobPrivateValues default

    SubscriptionPrivateAccess default
```

```
    SubscriptionPrivateValues default

    … …

    <Limit Create-Printer-Subscription>

        Require user @OWNER

        Order deny,allow

    </Limit>

    <Limit All>

        Order deny,allow

    </Limit>

</Policy>
```

Dateien kopieren und einfügen

Benutzer können Dateien zwischen einer Sitzung und einem lokalen Client kopieren und einfügen. Diese Funktion erfordert Citrix Virtual Apps and Desktops™ 2006 oder höher und Citrix Workspace™ App 1903 oder höher für Windows. Kopier- und Einfügefunktionen werden über das Rechtsklickmenü oder Tastenkombinationen ausgeführt.

Um Dateien erfolgreich zu kopieren und einzufügen, stellen Sie sicher, dass:

- Die maximale Anzahl von Dateien 20 nicht überschreitet.
- Die maximale Dateigröße 200 MB nicht überschreitet.

Unterstützte Plattformen

Die Funktion zum Kopieren und Einfügen von Dateien ist verfügbar für:

- RHEL 7.8
- SLES 12.5
- Ubuntu 16.04
- Ubuntu 18.04
- Debian 10

Relevante Richtlinien

Die folgenden Zwischenablage-Richtlinien sind für die Konfiguration der Funktion relevant. Weitere Informationen zu den Zwischenablage-Richtlinien finden Sie unter Richtlinien-Supportliste.

- Client-Zwischenablagenumleitung
- Aktualisierungsmodus für die Zwischenablageauswahl
- Aktualisierungsmodus für die primäre Auswahl

> **Hinweis:**
>
> Um die Funktion zum Kopieren und Einfügen von Dateien zu deaktivieren, legen Sie die Richtlinie **Client-Zwischenablageumleitung** auf **Verboten** in Citrix Studio fest.

Einschränkungen

- Ausschneiden wird nicht unterstützt. Anforderungen zum Ausschneiden einer Datei werden als Kopieren behandelt.
- Drag & Drop wird nicht unterstützt.
- Das Kopieren von Verzeichnissen wird nicht unterstützt.

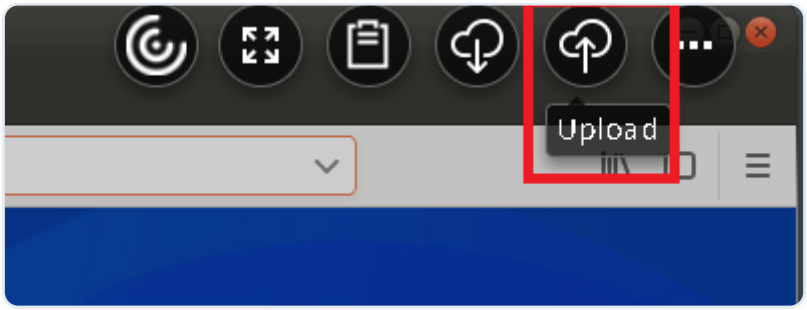
Dateiübertragung

File transfer is supported between the Linux VDA and the client device. This feature is available when the client device runs a web browser that supports the HTML5 sandbox attribute. The HTML5 sandbox attribute allows users to access virtual desktops and apps using Citrix Workspace™ app for HTML5 and for Chrome.

> **Hinweis:**

> File transfer is available for Citrix Workspace app for HTML5 and for Chrome.

> Innerhalb veröffentlichter App- und Desktopsitzungen ermöglicht die Dateiübertragung das Hoch- und Herunterladen von Dateien zwischen dem Linux-VDA und dem Clientgerät. Um Dateien vom Clientgerät auf den Linux-VDA hochzuladen, klicken Sie auf das Symbol **Hochladen** in der Symbolleiste von Citrix Workspace app und wählen Sie die gewünschte Datei aus den Dateidialogen aus. Um Dateien vom Linux-VDA auf das Clientgerät herunterzuladen, klicken Sie auf das Symbol **Herunterladen**. Sie können Dateien während des Hoch- oder Herunterladens hinzufügen. Sie können bis zu 100 Dateien gleichzeitig übertragen.



> **Hinweis:**

> Um Dateien zwischen dem Linux-VDA und dem Clientgerät hoch- und herunterzuladen, stellen Sie sicher, dass die Symbolleiste von Citrix Workspace app aktiviert ist.

> Sie können eine Version von Citrix Workspace app verwenden, die das Ziehen und Ablegen von Dateien ermöglicht.

> Der automatische Download ist eine Verbesserung für die Dateiübertragung. Dateien, die Sie herunterladen oder in das Verzeichnis **Auf meinem Gerät speichern** auf dem VDA verschieben, werden automatisch auf das Clientgerät übertragen.

> **Hinweis:**
>
> Für den automatischen Download ist erforderlich, dass die Richtlinien **Dateiübertragung zwischen Desktop und Client zulassen** und **Datei vom Desktop herunterladen** auf **Zulässig** festgelegt sind.

> Hier sind einige Anwendungsfälle für den automatischen Download:

- Dateien in **Auf meinem Gerät speichern** herunterladen

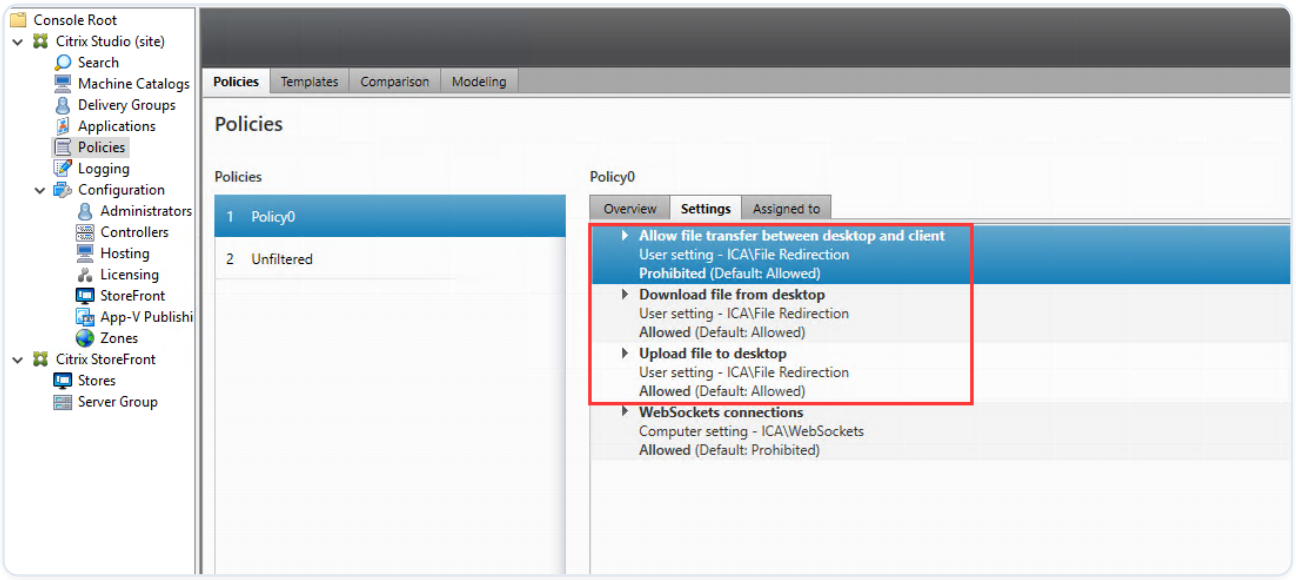
  Innerhalb veröffentlichter Desktop- und Webbrowser-App-Sitzungen können Dateien, die Sie von Websites herunterladen, im Verzeichnis **Auf meinem Gerät speichern** auf dem VDA zur automatischen Übertragung auf das Clientgerät gespeichert werden. Um den automatischen Download zu ermöglichen, legen Sie das Standard-Downloadverzeichnis des In-Session-Webbrowsers auf **Auf meinem Gerät speichern** fest und legen Sie ein lokales Downloadverzeichnis in dem Webbrowser fest, der Ihre Citrix Workspace app für HTML5 oder für Chrome ausführt.

- Dateien in **Auf meinem Gerät speichern** verschieben oder kopieren

  Innerhalb veröffentlichter Desktopsitzungen wählen Sie die Zieldateien aus und verschieben oder kopieren Sie sie in das Verzeichnis **Auf meinem Gerät speichern** zur Verfügbarkeit auf dem Clientgerät.

Richtlinien für die Dateiübertragung

Sie können Citrix Studio verwenden, um die Richtlinien für die Dateiübertragung festzulegen. Standardmäßig ist die Dateiübertragung aktiviert.



Richtlinienbeschreibungen:

- **Dateitransfer zwischen Desktop und Client zulassen.** Ermöglicht oder verhindert Benutzern die Übertragung von Dateien zwischen einer Citrix Virtual Apps and Desktops™-Sitzung und ihren Geräten.
- **Datei vom Desktop herunterladen.** Ermöglicht oder verhindert Benutzern das Herunterladen von Dateien von einer Citrix Virtual Apps™ and Desktops-Sitzung auf ihr Gerät.
- **Datei auf den Desktop hochladen.** Ermöglicht oder verhindert Benutzern das Hochladen von Dateien von ihrem Gerät in eine Citrix Virtual Apps and Desktops-Sitzung.

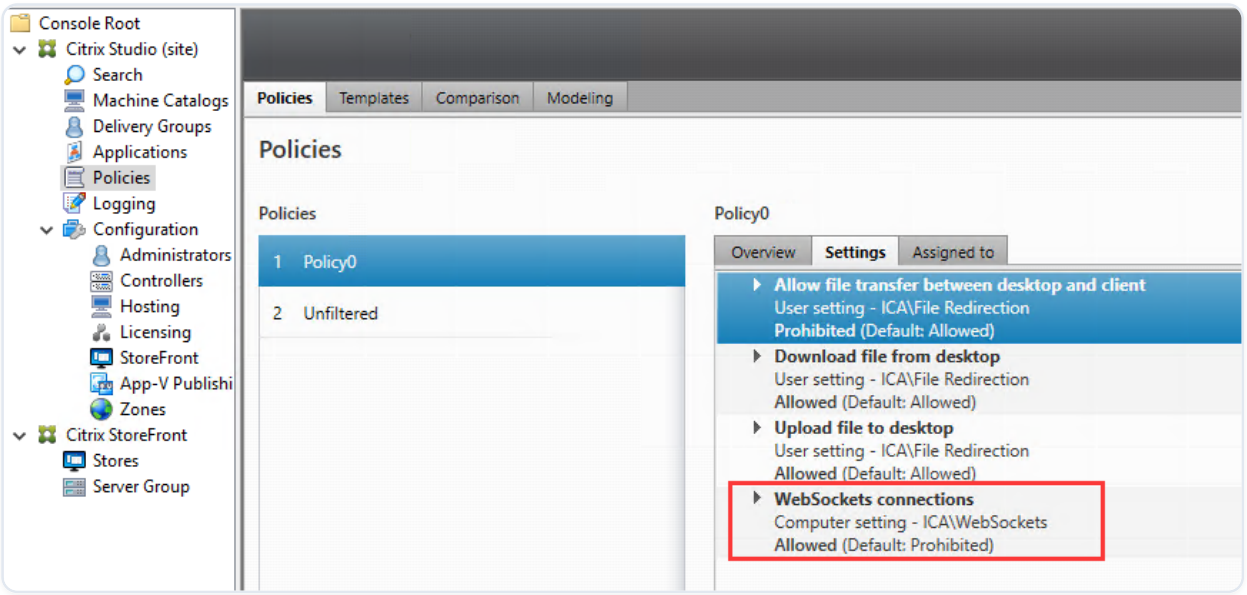
> **Hinweis:**

> Um sicherzustellen, dass die Richtlinien **Datei vom Desktop herunterladen** und **Datei auf den Desktop hochladen** wirksam werden, setzen Sie die Richtlinie **Dateitransfer zwischen Desktop und Client zulassen** auf **Zugelassen**.

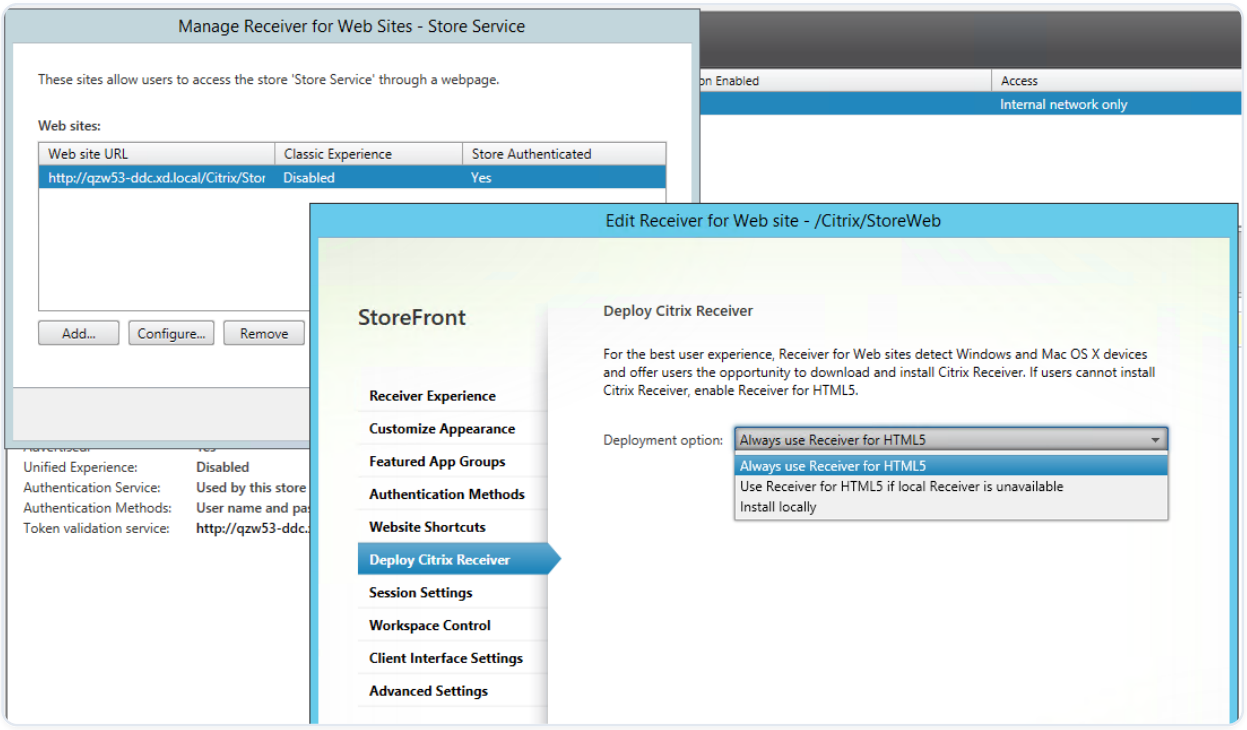
Verwendung

So verwenden Sie die Dateitransferfunktion über die Citrix Workspace-App für HTML5:

1. Legen Sie in Citrix Studio die Richtlinie **WebSockets-Verbindungen** auf **Zugelassen** fest.



2. Aktivieren Sie in Citrix Studio den Dateitransfer über die zuvor beschriebenen Dateitransferrichtlinien.
3. Klicken Sie in der Citrix StoreFront-Verwaltungskonsole auf **Stores**, wählen Sie den Knoten **Receiver für Web-Sites verwalten** aus und aktivieren Sie Citrix Receiver™ für HTML5, indem Sie die Option **Immer Receiver für HTML5 verwenden** auswählen.



4. Starten Sie eine virtuelle Desktop- oder Webbrowser-App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux VDA und Ihrem Clientgerät durch.

So verwenden Sie die Dateitransferfunktion über die Citrix Workspace-App für Chrome:

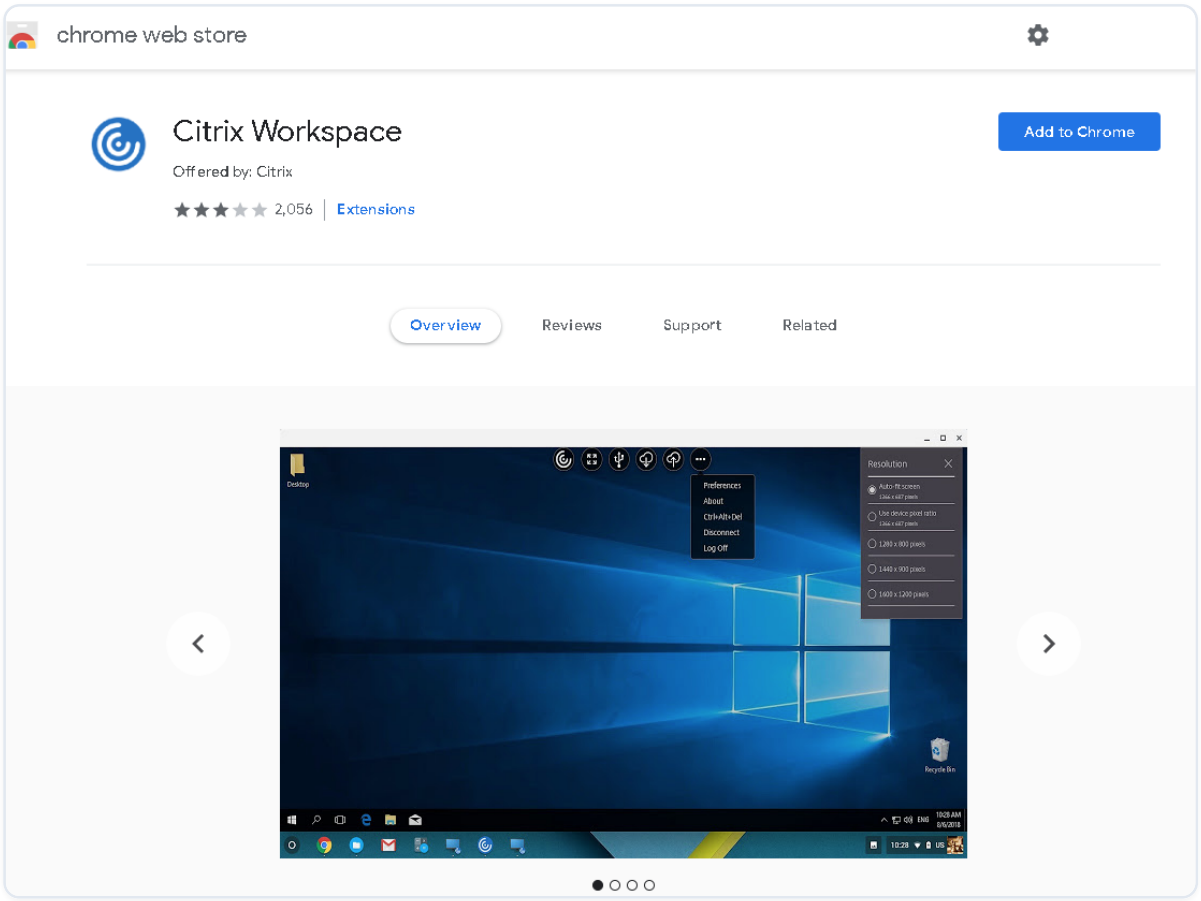
1. Aktivieren Sie den Dateitransfer über die zuvor beschriebenen Dateitransferrichtlinien.

2. Beziehen Sie die Citrix Workspace-App aus dem Chrome Web Store.

   Überspringen Sie diesen Schritt, wenn Sie die Citrix Workspace-App für Chrome bereits zur Seite „Chrome-Apps“ hinzugefügt haben.

   a. Geben Sie **Citrix Workspace for Chrome** in das Suchfeld von Google Chrome ein. Klicken Sie auf das Suchsymbol.

   b. Klicken Sie in den Suchergebnissen auf die URL zum Chrome Web Store, wo 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 die Citrix Workspace-App für Chrome.
4. Geben Sie die URL Ihres StoreFront™-Stores ein, um eine Verbindung herzustellen.

   Überspringen Sie diesen Schritt, wenn Sie die URL bereits eingegeben haben.

5. Starten Sie eine virtuelle Desktop- oder App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux-VDA und Ihrem Clientgerät durch.

PDF-Druck

Mit einer Version der Citrix Workspace™-App, die PDF-Druck unterstützt, können Sie PDFs drucken, die aus Linux VDA-Sitzungen konvertiert wurden. Sitzungsdruckaufträge 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 Ihrem bevorzugten Drucker ausdrucken.

Der Linux VDA unterstützt den PDF-Druck in den 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

Neben der Verwendung einer Version der Citrix Workspace-App, die PDF-Druck unterstützt, aktivieren Sie die folgenden Richtlinien in Citrix Studio:

- **Clientdruckerumleitung** (standardmäßig aktiviert)
- **PDF-Universaldrucker automatisch erstellen** (standardmäßig deaktiviert)

Wenn diese Richtlinien aktiviert sind, wird auf dem lokalen Computer eine Druckvorschau angezeigt, in der Sie einen Drucker auswählen können, wenn Sie in Ihrer gestarteten Sitzung auf **Drucken** klicken. Informationen zum Festlegen von Standarddruckern finden Sie in der Dokumentation zur Citrix Workspace-App.

Grafiken konfigurieren

Dieser Artikel enthält Anleitungen zur Grafikkartenkonfiguration und Feinabstimmung des Linux VDA.

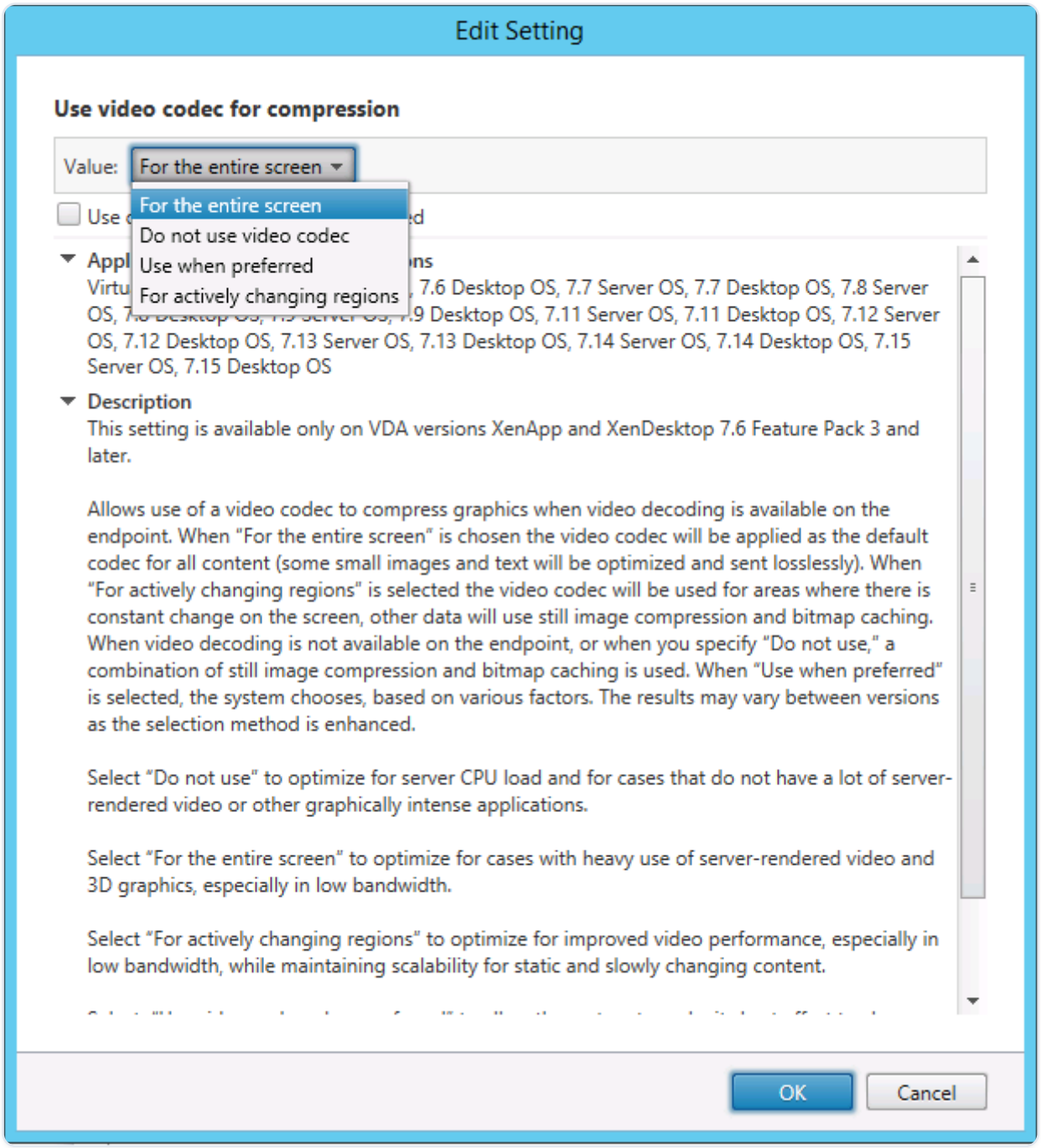
Weitere Informationen finden Sie unter Systemanforderungen und im Abschnitt Installationsübersicht.

Konfiguration

Thinwire ist die im Linux VDA verwendete Anzeigeremoting-Technologie. Die Technologie ermöglicht die Übertragung von auf einem Computer generierten Grafiken, typischerweise über ein Netzwerk, an einen anderen Computer zur Anzeige.

Die Grafikrichtlinie Videocodec für Komprimierung verwenden legt den Standardgrafikmodus fest und bietet die folgenden Optionen für verschiedene Anwendungsfälle:

- **Bei Bedarf verwenden**. Diese Einstellung ist die Standardeinstellung. Es ist keine zusätzliche Konfiguration erforderlich. Wenn Sie diese Einstellung beibehalten, wird Thinwire für alle Citrix®-Verbindungen ausgewählt und für Skalierbarkeit, Bandbreite und überragende Bildqualität bei typischen Desktop-Workloads optimiert.
- **Für den gesamten Bildschirm**. Liefert Thinwire mit Vollbild-H.264 oder H.265, um die Benutzererfahrung und Bandbreite zu optimieren, insbesondere bei intensiver Nutzung von 3D-Grafiken.
- **Für sich aktiv ändernde Bereiche**. Die adaptive Anzeigetechnologie in Thinwire identifiziert bewegte Bilder (Video, 3D in Bewegung) und verwendet H.264 nur in dem Bereich des Bildschirms, in dem sich das Bild bewegt. Die ***selektive Verwendung des H.264-Videocodecs*** ermöglicht es HDX Thinwire, häufig aktualisierte Bildschirmbereiche, z. B. Videoinhalte, zu erkennen und mit dem H.264-Videocodec zu kodieren. Für den Rest des Bildschirms, einschließlich Text und fotografischer Bilder, werden weiterhin Standbildkomprimierung (JPEG, RLE) und Bitmap-Caching verwendet. Benutzer profitieren von geringerer Bandbreite und besserer Qualität für Videoinhalte in Kombination mit verlustfreiem Text oder hochwertigen Bildern an anderer Stelle. Um diese Funktion zu aktivieren, ändern Sie die Richtlinieneinstellung **Videocodec für Komprimierung verwenden** in **Bei Bedarf verwenden** (Standard) oder **Für sich aktiv ändernde Bereiche**. Weitere Informationen finden Sie unter Grafikrichtlinieneinstellungen.



Einige andere Richtlinieneinstellungen, einschließlich der folgenden visuellen Anzeigerichtlinieneinstellungen, können zur Feinabstimmung der Leistung des Anzeigeremoting verwendet werden:

- **Bevorzugte Farbtiefe für einfache Grafiken**
- **Zielbildrate**
- **Visuelle Qualität**

H.264 für Build to Lossless in Thinwire verwenden

Standardmäßig ist die Einstellung **Build to Lossless** der Richtlinie **Visuelle Qualität** für bewegte Bilder jetzt H.264 anstelle von JPEG.

Die H.264-Codierung bietet eine überragende Bildqualität. Die Richtlinie **Videocodec für Komprimierung verwenden** steuert diese Präferenz, wobei die Standardeinstellung **Verwenden, wenn bevorzugt** ist. Um **Build to Lossless** zur Verwendung von JPEG zu zwingen, setzen Sie die Richtlinie **Videocodec für Komprimierung verwenden** auf **Videocodec nicht verwenden**. Wenn Ihr Client Selective H.264 nicht unterstützt, greift **Build to Lossless** unabhängig von den Richtlinieneinstellungen auf JPEG zurück. 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 sowie Citrix Workspace-App 1808 für Linux und höher unterstützen Selective H.264. Weitere Informationen zu den Richtlinieneinstellungen **Visuelle Qualität** und **Videocodec für Komprimierung verwenden** finden Sie unter Richtlinieneinstellungen für die visuelle Anzeige und Richtlinieneinstellungen für Grafiken.

Unterstützung für H.265-Videocodec

Ab Release 7.18 unterstützt der Linux VDA den H.265-Videocodec für die Hardwarebeschleunigung von Remotegrafiken und -videos. Sie können diese Funktion mit Citrix Receiver für Windows 4.10 bis 4.12 und mit der Citrix Workspace-App 1808 für Windows und höher verwenden. Um diese Funktion nutzen zu können, müssen Sie sie sowohl auf dem Linux VDA als auch auf Ihrem Client aktivieren. Wenn die GPU Ihres Clients die H.265-Decodierung über die DXVA-Schnittstelle nicht unterstützt, wird die Richtlinieneinstellung „H.265-Decodierung für Grafiken“ ignoriert und die Sitzung greift auf die Verwendung des H.264-Videocodecs zurück. Weitere Informationen finden Sie unter H.265-Videocodierung.

So aktivieren Sie die H.265-Hardwarecodierung auf dem VDA:

1. Aktivieren Sie die Richtlinie **Hardwarecodierung für Videocodec verwenden**.
2. Aktivieren Sie die Richtlinie **Für 3D-Grafik-Workload optimieren**.
3. Stellen Sie sicher, dass die Richtlinie **Videocodec für Komprimierung verwenden** auf den Standardwert oder auf **Für den gesamten Bildschirm** eingestellt ist.
4. Stellen Sie sicher, dass die Richtlinie **Visuelle Qualität NICHT** auf **Build to Lossless** oder **Always Lossless** eingestellt ist.

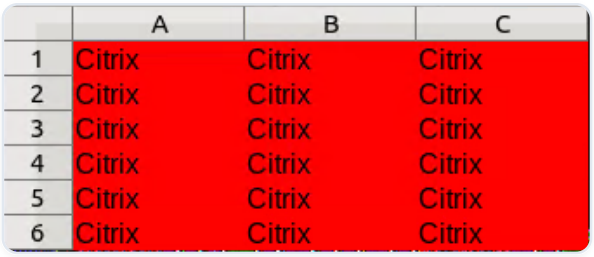
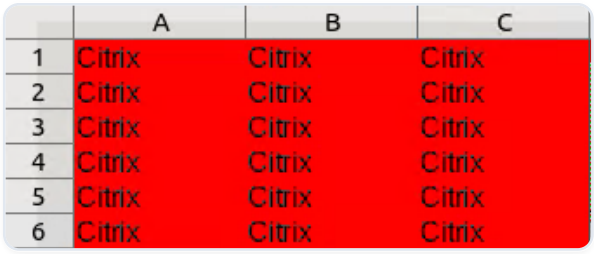
Informationen zum Aktivieren der H.265-Hardwarecodierung auf Ihrem Client finden Sie unter H.265-Videocodierung.

Unterstützung für YUV444-Softwarecodierung

Der Linux VDA unterstützt die YUV444-Softwarecodierung. Das YUV-Codierungsschema weist jedem Pixel sowohl Helligkeits- als auch Farbwerte zu. In YUV stellt '`Y`' die Helligkeit oder den '`luma`'-Wert dar, und '`UV`' stellt die Farb- oder 'Chroma'-Werte dar. Sie können diese Funktion

des Linux VDA mit Citrix Receiver für Windows 4.10 bis 4.12 und mit der Citrix Workspace-App 1808 für Windows und höher verwenden.

Jeder eindeutige Y-, U- und V-Wert umfasst 8 Bit oder ein Byte an Daten. Das YUV444-Datenformat überträgt 24 Bit pro Pixel. Das YUV422-Datenformat teilt sich U- und V-Werte zwischen zwei Pixeln, was zu einer durchschnittlichen Übertragungsrate von 16 Bit pro Pixel führt. Die folgende Tabelle zeigt einen intuitiven Vergleich zwischen YUV444 und YUV420.

YUV444	YUV420
	

So aktivieren Sie die YUV444-Softwarekodierung auf dem VDA:

1. Stellen Sie sicher, dass die Richtlinie **Videocodec für Komprimierung verwenden** auf **Für den gesamten Bildschirm** festgelegt ist.
2. Stellen Sie sicher, dass die Richtlinie **Visuelle Qualität** auf **Immer verlustfrei** oder **Verlustfrei aufbauen** festgelegt ist.

Durchschnittliche Bitraten basierend auf Bandbreitenschätzungen anpassen

Citrix verbessert die HDX™ 3D Pro Hardwarekodierung durch Anpassen der durchschnittlichen Bitraten basierend auf Bandbreitenschätzungen.

Wenn die HDX 3D Pro Hardwarekodierung verwendet wird, kann der VDA die Bandbreite des Netzwerks zeitweise schätzen und die Bitraten der kodierten Frames basierend auf den Bandbreitenschätzungen anpassen. Diese neue Funktion bietet einen Mechanismus, um ein Gleichgewicht zwischen Schärfe und Flüssigkeit zu finden.

Diese Funktion ist standardmäßig aktiviert. Um sie zu deaktivieren, führen Sie den folgenden Befehl aus:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "DisableReconfigureEncoder" -d "0x00000001" --force
```

Zusätzlich zur Verwendung dieser Funktion können Sie auch die folgenden Befehle ausführen, um zwischen Schärfe und Flüssigkeit anzupassen. Die Parameter **AverageBitRatePercent** und **MaxBitRatePercent** legen den Prozentsatz der Bandbreitennutzung fest. Je höhere Werte Sie festlegen, desto schärfer die Grafiken und desto geringer die Flüssigkeit. Der empfohlene Einstellungsbereich ist 50–100.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "AverageBitRatePercent" -d "90" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "MaxBitRatePercent" -d "100" --force
```

Bei der Anpassung der durchschnittlichen Bitrate bleibt der aktuellste Frame in einem Zustand geringer Qualität, wenn Ihr Bildschirm stillsteht, da keine neuen Frames gesendet werden. Die Schärfungsunterstützung kann dieses Problem beheben, indem der aktuellste Frame neu konfiguriert und sofort in höchster Qualität gesendet wird.

Eine vollständige Liste der vom Linux VDA Thinwire unterstützten Richtlinien finden Sie unter Liste der unterstützten Richtlinien.

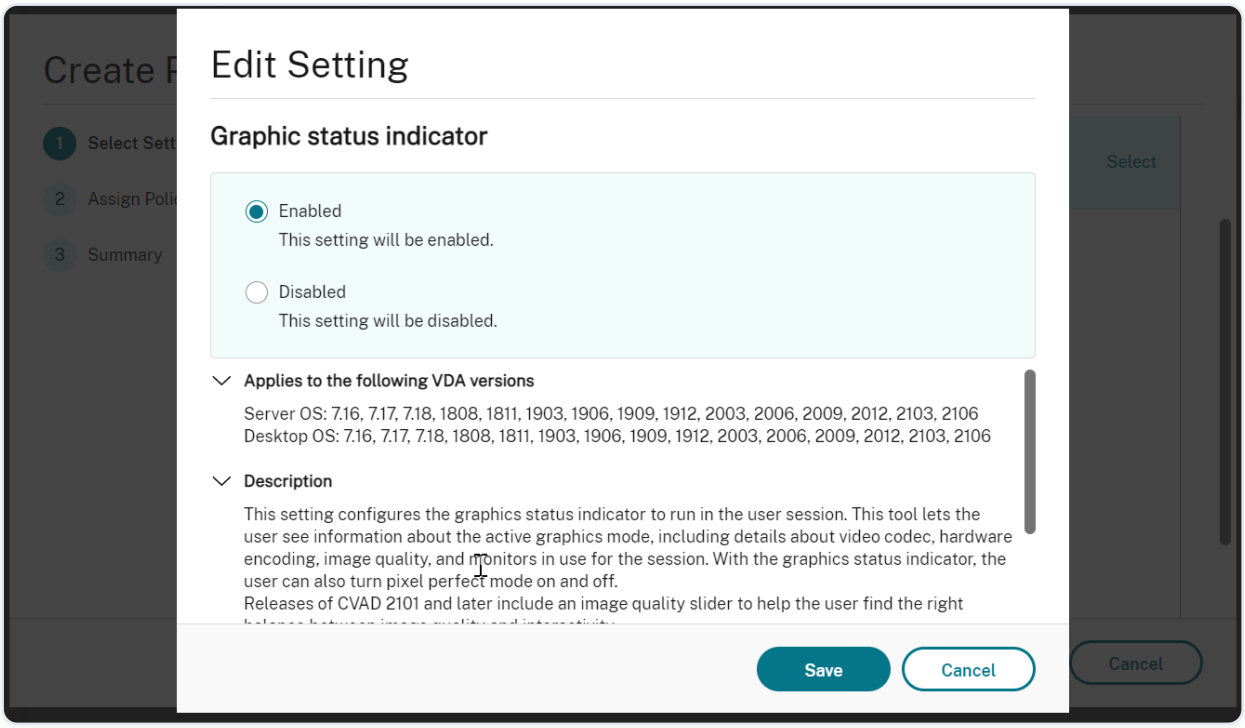
Informationen zur Konfiguration der Multi-Monitor-Unterstützung auf dem Linux VDA finden Sie unter CTX220128.

Schieberegler für Grafikqualität

Wir haben einen Schieberegler für die Grafikqualität in das Grafikstatusanzeige-Tool integriert, das in Ihren virtuellen Linux-Sitzungen ausgeführt wird. Der Schieberegler hilft, das richtige Gleichgewicht zwischen Bildqualität und Interaktivität zu finden.

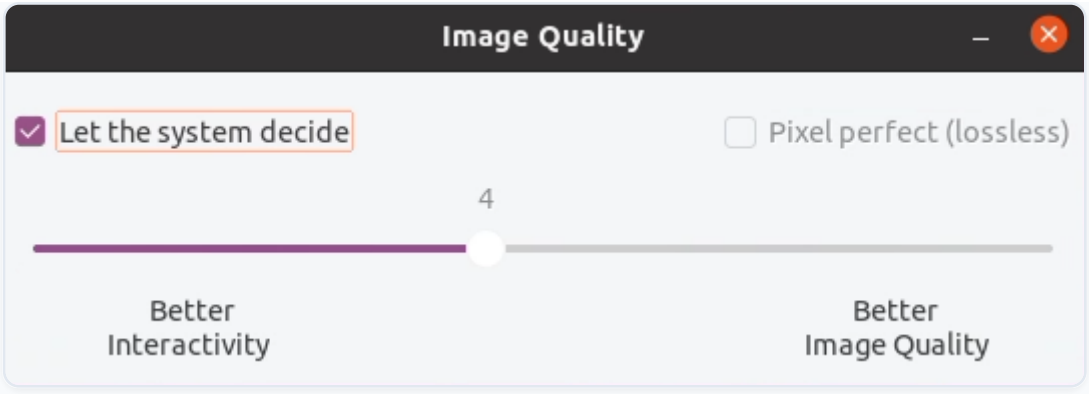
Um den Schieberegler zu verwenden, führen Sie die folgenden Schritte aus:

1. Aktivieren Sie die Richtlinie **Grafikstatusanzeige** in Citrix Studio.



2. Öffnen Sie das Terminal und führen Sie den Befehl `ctxslider` aus. Die Schieberegler-Benutzeroberfläche wird angezeigt.

> **Hinweis:**
>
> Wenn Sie die Richtlinie **Visuelle Qualität** auf **Immer verlustfrei** oder **Verlustfrei erstellen** eingestellt haben, wird die Schieberegler-Benutzeroberfläche nicht angezeigt.



Die folgenden Optionen sind jetzt verfügbar:

- Um die Bildqualität zu ändern, bewegen Sie den Schieberegler. Der Schieberegler unterstützt 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**.

Problembehandlung

Überprüfen, welcher Grafikmodus verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, welcher Grafikmodus verwendet wird (**0** bedeutet TW+; **1** bedeutet Vollbild-Videocodec):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

Das Ergebnis sieht wie folgt aus:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000000" --force`

Überprüfen, ob H.264 verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob H.264 verwendet wird (**0** bedeutet nicht in Gebrauch; **1** bedeutet in Gebrauch):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

Das Ergebnis sieht wie folgt aus:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000000" --force`

Prüfen, ob H.265 verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob H.265 im Vollbildmodus verwendet wird (**0** bedeutet nicht in Gebrauch; **1** bedeutet in Gebrauch):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

Das Ergebnis sieht wie folgt aus:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H265" -d "0x00000000" --force`

Prüfen, welches YUV-Kodierungsschema verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, welches YUV-Kodierungsschema verwendet wird (**0** bedeutet YUV420. **1** bedeutet YUV422. **2** bedeutet YUV444):

Hinweis: Der Wert von YUVFormat ist nur aussagekräftig, wenn ein Video-Codec verwendet wird.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

Das Ergebnis sieht wie folgt aus:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000000" --force`

Prüfen, ob YUV444-Softwarekodierung verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob YUV444-Softwarekodierung verwendet wird:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
```

Wenn YUV444 verwendet wird, sieht das Ergebnis wie folgt aus:

`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`

Prüfen, ob Hardwarekodierung für 3D Pro verwendet wird

Führen Sie den folgenden Befehl aus (**0** bedeutet nicht in Gebrauch; **1** bedeutet in Gebrauch):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
```

Die Ergebnisse sehen wie folgt aus:

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

Eine andere Möglichkeit ist die Verwendung des Befehls **nvidia-smi**. Die Ausgaben sehen wie folgt aus, wenn Hardwarekodierung verwendet wird:

```
Tue Apr 12 10:42:03 2016

+-----------------------------------------------------+

| NVIDIA-SMI 361.28     Driver Version: 361.28         |

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

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr.
ECC |

| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute
M. |

|
===============================+======================+==================
===|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
N/A |

| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
Default |

+-------------------------------+----------------------
+----------------------+



+-----------------------------------------------------------------------------
----+

| Processes:                                                       GPU
Memory |

|  GPU       PID  Type  Process name
```

```
Usage      |

|
=============================================================================
===|

|    0      2164  C+G   /usr/local/bin/ctxgfx
106MiB |

|    0      2187    G   Xorg
85MiB |

+-----------------------------------------------------------------------------
----+
```

Überprüfen Sie, ob der NVIDIA GRID-Grafiktreiber korrekt installiert ist

Um zu überprüfen, ob der NVIDIA GRID-Grafiktreiber korrekt installiert ist, führen Sie **nvidia-smi** aus. Die Ergebnisse ähneln:

```
+-----------------------------------------------------+

| NVIDIA-SMI 352.70     Driver Version: 352.70         |

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

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr.
ECC |

| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute
M. |

|
===============================+======================+==================
===|

|   0  Tesla M60           Off  | 0000:00:05.0     Off |
Off |

| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
Default |
```

```
+-------------------------------+----------------------
+----------------------+



+-----------------------------------------------------------------------------
----+

| Processes:                                                            GPU
Memory |

|  GPU       PID  Type  Process name
Usage      |

|
=============================================================================
===|

|  No running processes found
                                 |

+-----------------------------------------------------------------------------
----+
```

Legen Sie die korrekte Konfiguration für die Karte fest:

`etc/X11/ctx-nvidia.sh`

HDX 3D Pro-Probleme beim Neuzeichnen auf mehreren Monitoren

Wenn auf anderen Bildschirmen als dem primären Monitor Neuzeichnungsprobleme auftreten, überprüfen Sie, ob die NVIDIA GRID-Lizenz verfügbar ist.

Xorg-Fehlerprotokolle überprüfen

Die Protokolldatei von Xorg heißt ähnlich wie **Xorg.{DISPLAY}.log** im Ordner **/var/log/**.

Bekannte Probleme und Einschränkungen

Bei vGPU zeigt die lokale Citrix Hypervisor™-Konsole den ICA-Desktopsitzungsbildschirm an

Problemumgehung: Deaktivieren Sie die lokale VGA-Konsole der VM, indem Sie den folgenden Befehl ausführen:

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

NVIDIA K2-Grafikkarten unterstützen keine YUV444-Hardwarekodierung im Pass-Through-Modus

Wenn **Build to Lossless** über die Richtlinieneinstellung aktiviert ist, wird ein schwarzer oder grauer Bildschirm angezeigt, wenn Benutzer eine App-/Desktopsitzung mit einer NVIDIA K2-Grafikkarte starten. Das Problem tritt auf, weil NVIDIA K2-Grafikkarten die YUV444-Hardwarekodierung im Pass-Through-Modus nicht unterstützen. Weitere Informationen finden Sie unter Video Encode and Decode GPU Support Matrix.

Gnome 3-Desktop-Popups langsam beim Anmelden

Dies ist eine Einschränkung des Gnome 3-Desktop-Sitzungsstarts.

Einige OpenGL/WebGL-Anwendungen werden beim Ändern der Größe des Citrix Workspace-App-Fensters nicht gut gerendert

Das Ändern der Größe des Fensters der Citrix Workspace-App ändert die Bildschirmauflösung. Der proprietäre NVIDIA-Treiber ändert einige interne Zustände und erfordert möglicherweise, dass Anwendungen entsprechend reagieren. Zum Beispiel könnte das WebGL-Bibliothekselement **lightgl.js** einen Fehler auslösen, der besagt, dass '`Rendering to this texture is not supported (incomplete frame buffer)`'.

Thinwire Progressive Display

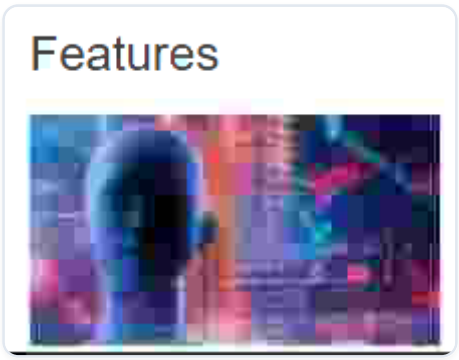
Die Interaktivität der Sitzung kann bei Verbindungen mit geringer Bandbreite oder hoher Latenz beeinträchtigt werden. Bei Verbindungen mit weniger als 2 Mbit/s Bandbreite oder einer Latenz von mehr als 200 ms kann beispielsweise das Scrollen auf einer Webseite langsam, nicht reagierend oder ruckelig werden. Tastatur- und Mausoperationen können hinter Grafikaktualisierungen zurückbleiben.

Bis Version 7.17 konnten Sie Richtlinieneinstellungen verwenden, um den Bandbreitenverbrauch zu reduzieren, indem Sie die Sitzung auf die visuelle Qualität **Niedrig** konfigurierten oder eine geringere Farbtiefe (16-Bit- oder 8-Bit-Grafik) einstellten. Sie mussten jedoch wissen, dass ein Benutzer eine schwache Verbindung hatte. HDX Thinwire passte die statische Bildqualität nicht dynamisch an die Netzwerkbedingungen an.

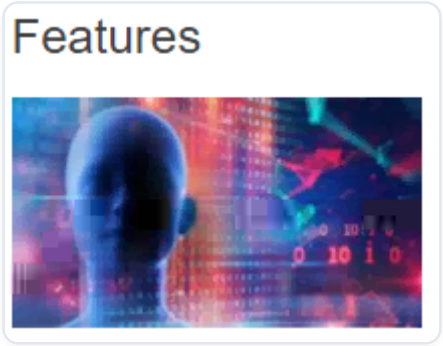
Ab Version 7.18 wechselt HDX Thinwire standardmäßig in einen progressiven Aktualisierungsmodus, wenn die verfügbare Bandbreite unter 2 Mbit/s fällt oder die Netzwerklatenz 200 ms überschreitet. In diesem Modus:

- Alle statischen Bilder werden stark komprimiert.
- Die Textqualität wird reduziert.

In der folgenden Grafik, in der der progressive Aktualisierungsmodus aktiv ist, weisen beispielsweise die Buchstaben **F** und **e** blaue Artefakte auf, und das Bild ist stark komprimiert. Dieser Ansatz reduziert den Bandbreitenverbrauch erheblich, wodurch Bilder und Text schneller empfangen werden können und die Interaktivität der Sitzung verbessert wird.



Wenn Sie die Interaktion mit der Sitzung beenden, werden die beeinträchtigten Bilder und Texte schrittweise verlustfrei geschärft. In der folgenden Grafik enthalten die Buchstaben beispielsweise keine blauen Artefakte mehr, und das Bild wird in Quellqualität angezeigt.



Bei Bildern wird das Schärfen mit einer zufälligen blockartigen Methode durchgeführt. Bei Text werden einzelne Buchstaben oder Wortteile geschärft. Der Schärfungsprozess erfolgt über

mehrere Frames. Dieser Ansatz vermeidet eine Verzögerung durch einen einzelnen großen Schärfungsframe.

Transiente Bilder (Video) werden weiterhin mit adaptiver Anzeige oder Selective H.264 verwaltet.

Verwendung des progressiven Modus

Standardmäßig ist der progressive Modus für die Richtlinieneinstellungen der **Visuellen Qualität** in Bereitschaft: **Hoch**, **Mittel** (Standard) und **Niedrig**.

Der progressive Modus wird erzwungen deaktiviert (nicht verwendet), wenn:

- **Visuelle Qualität** = **Immer verlustfrei** oder **Verlustfrei aufbauen**
- **Bevorzugte Farbtiefe für einfache Grafiken** = 8-Bit
- **Videocodec für Komprimierung verwenden** = **Für den gesamten Bildschirm** (wenn Vollbild-H.264 gewünscht ist)

Wenn der progressive Modus im Standby ist, wird er standardmäßig aktiviert, wenn eine der folgenden Bedingungen eintritt:

- Verfügbare Bandbreite fällt unter 2 Mbit/s
- Netzwerklatenz steigt über 200 ms

Nach einem Moduswechsel wird mindestens 10 Sekunden in diesem Modus verbracht, selbst wenn die ungünstigen Netzwerkbedingungen nur vorübergehend sind.

Verhalten des progressiven Modus ändern

Sie können das Verhalten des progressiven Modus ändern, indem Sie den folgenden Befehl ausführen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplay" -d "<value>" --force
```

wobei \<value\>:

0 = Immer aus (unter keinen Umständen verwenden)

1 = Automatisch (Umschaltung basierend auf Netzwerkbedingungen, Standardwert)

2 = Immer ein

Im automatischen Modus (1) können Sie einen der folgenden Befehle ausführen, um die Schwellenwerte zu ändern, bei denen der progressive Modus umgeschaltet wird:

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
```

wobei \<value\> der \<Schwellenwert in Kbit/s\> ist (Standard = 2.048)

Beispiel: 4096 = progressiven Modus einschalten, wenn die Bandbreite unter 4 Mbit/s fällt

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayLatencyThreshold" -d "<value>" --force
```

wobei \<value\> der \<Schwellenwert in ms\> ist (Standard = 200)

Beispiel: 100 = aktiviert den progressiven Modus, wenn die Netzwerklatenz unter 100 ms fällt.

Nicht-GRID-3D-Grafik

Übersicht

Mit dieser Funktionserweiterung unterstützt der Linux VDA nicht nur NVIDIA GRID 3D-Karten, sondern auch 3D-Karten ohne GRID.

Installation

Um die 3D-Grafikfunktion ohne GRID zu nutzen, müssen Sie:

- Installieren Sie XDamage als Voraussetzung. Typischerweise existiert XDamage als Erweiterung von XServer.
- Setzen Sie `CTX_XDL_HDX_3D_PRO` auf `Y` bei der Installation des Linux VDA. Informationen zu Umgebungsvariablen finden Sie unter Schritt 6: Einrichten der Laufzeitumgebung zur Durchführung der Installation.

Konfiguration

Xorg-Konfigurationsdateien

Wenn Ihr 3D-Kartentreiber NVIDIA ist, werden die Konfigurationsdateien automatisch installiert und eingerichtet.

Andere Arten von 3D-Karten

Wenn Ihr 3D-Kartentreiber NICHT NVIDIA ist, müssen Sie die vier unter `/etc/X11/` installierten Vorlagen-Konfigurationsdateien ändern:

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf
- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

Am Beispiel von **ctx-driver_name-1.conf** gehen Sie wie folgt vor, um die Vorlagen-Konfigurationsdateien zu ändern:

1. Ersetzen Sie ***driver_name*** durch Ihren tatsächlichen Treibernamen.

   Wenn Ihr Treibername beispielsweise `intel` lautet, können Sie den Namen der Konfigurationsdatei in `ctx-intel-1.conf` ändern.
2. Fügen Sie die Informationen zum Videotreiber hinzu.

   Jede Vorlagen-Konfigurationsdatei enthält einen Abschnitt namens „Device“, der auskommentiert ist. Dieser Abschnitt beschreibt die Informationen zum Videotreiber. Aktivieren Sie diesen Abschnitt, bevor Sie Ihre Videotreiberinformationen hinzufügen. So aktivieren Sie diesen Abschnitt:

   a. Informationen zur Konfiguration finden Sie im Handbuch zur 3D-Karte des Herstellers. Eine native Konfigurationsdatei kann generiert werden. Überprüfen Sie, ob Ihre 3D-Karte in einer lokalen Umgebung mit der nativen Konfigurationsdatei funktioniert, wenn Sie keine Linux VDA ICA®-Sitzung verwenden.

   b. Kopieren Sie den Abschnitt „Device“ der nativen Konfigurationsdatei nach **ctx-driver_name-1.conf**.
3. Führen Sie den folgenden Befehl aus, um den Registrierungsschlüssel so festzulegen, dass der Linux VDA den in Schritt 1 festgelegten Namen der Konfigurationsdatei erkennen kann.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_SZ" -v "DriverName" -d "intel" --force
```

Nicht-GRID-3D-Grafikfunktion aktivieren

Die Nicht-GRID-3D-Grafikfunktion ist standardmäßig deaktiviert. Sie können den folgenden Befehl ausführen, um sie zu aktivieren, indem Sie XDamageEnabled auf 1 setzen.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_DWORD" -v "XDamageEnabled" -d "0x00000001" --force
```

Problembehandlung

Keine oder fehlerhafte Grafikausgabe

Wenn Sie 3D-Anwendungen lokal ausführen können und alle Konfigurationen korrekt sind, ist eine fehlende oder fehlerhafte Grafikausgabe das Ergebnis eines Fehlers. Verwenden Sie /opt/Citrix/VDA/bin/setlog und setzen Sie GFX_X11 auf verbose, um die Ablaufverfolgungsinformationen für das Debugging zu sammeln.

Hardware-Kodierung funktioniert nicht

Diese Funktion unterstützt nur Software-Kodierung.

Richtlinien konfigurieren

Installation

Befolgen Sie die Installationsartikel, um den Linux VDA vorzubereiten.

Abhängigkeiten

Stellen Sie sicher, dass Sie diese Abhängigkeiten installieren, bevor Sie das Linux VDA-Paket installieren.

RHEL/CentOS:

```
sudo yum -y install openldap
```

```
sudo yum -y install libxml2
```

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

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

SLES/SELD:

```
sudo zypper install openldap2
```

```
sudo zypper install libxml2
```

```
sudo zypper install cyrus-sasl
```

```
sudo zypper install cyrus-sasl-gssapi
```

Ubuntu:

```
sudo apt-get install -y libldap-2.4-2
```

```
sudo apt-get install -y libsasl2-2
```

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

Konfiguration

Richtlinieneinstellungen in Citrix Studio

Gehen Sie wie folgt vor, um Richtlinien in Citrix Studio festzulegen:

1. Öffnen Sie **Citrix Studio**.
2. Wählen Sie den Bereich **Richtlinien** aus.
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 auf dem Linux VDA ist für Umgebungen mit einer einzelnen Domäne optional, aber für Umgebungen mit mehreren Domänen und mehreren Gesamtstrukturen obligatorisch. Die Einstellung ist erforderlich, damit der Richtliniendienst in diesen Umgebungen eine LDAP-Suche durchführen kann.

Nach der Installation des Linux VDA-Pakets führen Sie den Befehl aus:

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

Geben Sie alle LDAP-Server im vorgeschlagenen Format ein: eine durch Leerzeichen getrennte Liste von LDAP-FQDNs (Fully Qualified Domain Names) mit dem LDAP-Port (zum Beispiel ad1.mycompany.com:389 ad2.mycomany.com:389).

Abbildung der LDAP-Servereinstellung auf dem Linux VDA(/en-us/linux-virtual-delivery-agent/2107/media/ldap-server-setting-on-linux-vda-new.png)

Sie können auch den Befehl **ctxreg** ausführen, um diese Einstellung direkt in die Registrierung zu schreiben:

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

Liste der unterstützten Richtlinien

Liste der unterstützten Richtlinien für Linux VDA

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Lokale Zeit des Clients verwenden	UseLocalTimeOfClient	Benutzer	ICA\Time Zone Control	Server-Zeitzone verwenden
ICA-Roundtrip-Berechnung	IcaRoundTripCheckEnabled	Computer	ICA\End User Monitoring	Aktiviert (1)
ICA-Roundtrip-Berechnungsintervall	IcaRoundTripCheckPeriod	Computer	ICA\End User Monitoring	15
ICA-Roundtrip-Berechnungen für inaktive Verbindungen	IcaRoundTripCheckWhenIdle	Computer	ICA\End User Monitoring	Deaktiviert (0)
Gesamtbandbreitenlimit für Sitzungen	LimitOverallBw	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Audiodatenumleitung	LimitAudioBw	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Audio-Umleitung in Prozent	LimitAudioBwPercent	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Client-USB-Geräteumleitung	LimitUSBBw	Benutzer	ICA\Bandwidth	0

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Prozentsatz der Bandbreite für die Client-USB-Geräteumleitung	LimitUSBBwPercent	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Zwischenablagenumleitung	LimitClipbdBW	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Zwischenablage-Umleitung in Prozent	LimitClipbdBWPercent	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Dateiumleitung	LimitCdmBw	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Datei-Umleitung in Prozent	LimitCdmBwPercent	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Druckerumleitung	LimitPrinterBw	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Drucker-Umleitung in Prozent	LimitPrinterBwPercent	Benutzer	ICA\Bandwidth	0

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
WebSockets-Verbindungen	AcceptWebSocketsConnections	Computer	ICA\WebSockets	Verboten
WebSockets-Portnummer	WebSocketsPort	Computer	ICA\WebSockets	8008
WebSockets-Liste vertrauenswürdiger Ursprungsserver	WSTrustedOriginServerList	Computer	ICA\WebSockets	*
ICA® Keep-Alives	SendICAKeepAlives	Computer	ICA Keep-Alive	Keine ICA Keep-Alive-Nachrichten senden (0)
ICA Keep-Alive-Zeitüberschreitung	ICAKeepAliveTimeout	Computer	ICA Keep-Alive	60 Sekunden
ICA-Listener-Portnummer	IcaListenerPortNumber	Computer	ICA	1494
HDX™ adaptiver Transport	HDXoverUDP	Computer	ICA	Bevorzugt(2)
Sitzungszuverlässigkeitsverbindungen	AcceptSessionReliabilityConnections	Computer	ICA\Sitzungszuverlässigkeit	Zulässig(1)
Transparenzstufe der Wiederverbindungs-UI	ReconnectionUiTransparencyLevel	Computer	ICA\Automatisches Client-Reconnect	80 %

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Portnummer für Sitzungszuverlässigkeit	SessionReliabilityPort	Computer	ICA\Sitzungszuverlässigkeit	2598
Timeout für Sitzungszuverlässigkeit	SessionReliabilityTimeout	Computer	ICA\Sitzungszuverlässigkeit	180 s
Automatisches Client-Reconnect	AllowAutoClientReconnect	Benutzer	ICA\Automatisches Client-Reconnect	Zugelassen (1)
Client-Audiodirektübertragung	AllowAudioRedirection	Benutzer	Audio	Zugelassen (1)
Clientdruckerumleitung	AllowPrinterRedir	Benutzer	Drucken	Zugelassen (1)
PDF-Universal-Drucker automatisch erstellen	AutoCreatePDFPrinter	Benutzer	Drucken	Deaktiviert (0)
Druckertreiberzuordnung und -kompatibilität	DriverMappingList	Benutzer	Drucken	`"Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny"`
Client-Zwischenablagenumleitung	AllowClipboardRedir	Benutzer	Zwischenablage	Zulässig (1)
Client-USB-Geräteumleitung	AllowUSBRedir	Benutzer	USB	Verboten (0)

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Client-USB-Geräteumleitungsregeln	USBDeviceRules	Benutzer	USB	“\0”
Komprimierung bewegter Bilder	MovingImageCompressionConfiguration	Benutzer	Thinwire	Aktiviert (1)
Zusätzliche Farbkomprimierung	ExtraColorCompression	Benutzer	Thinwire	Deaktiviert (0)
Ziel-Mindestbildrate	TargetedMinimumFramesPerSecond	Benutzer	Thinwire	10 Bilder pro Sekunde
Zielbildrate	Frames pro Sekunde	Benutzer	Thinwire	30 Bilder pro Sekunde
Visuelle Qualität	Visuelle Qualität	Benutzer	Thinwire	Mittel (3)
Videocodec für Komprimierung verwenden	Videocodec	Benutzer	Thinwire	Verwenden, wenn bevorzugt (3)
Hardwarecodierung für Videocodec verwenden	Hardwarekodierung für Videocodec verwenden	Benutzer	Thinwire	Aktiviert (1)
Visuell verlustfreie Komprimierung zulassen	Visuell verlustfreie Komprimierung zulassen	Benutzer	Thinwire	Deaktiviert (0)
Für 3D-Grafik-Workload optimieren	Für 3D-Workload optimieren	Benutzer	Thinwire	Deaktiviert (0)

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Bevorzugte Farbtiefe für einfache Grafiken	Bevorzugte Farbtiefe	Benutzer	Thinwire	24 Bit pro Pixel (1)
Audioqualität	Tonqualität	Benutzer	Audio	Hoch – High-Definition-Audio (2)
Clientmikrofonumleitung	AllowMicrophoneRedir	Benutzer	Audio	Zulässig (1)
Maximale Anzahl von Sitzungen	MaximumNumberOfSessions	Computer	Lastverwaltung	250
Toleranz für gleichzeitige Anmeldungen	ConcurrentLogonsTolerance	Computer	Lastverwaltung	2
Automatische Aktualisierung der Controller aktivieren	EnableAutoUpdateOfControllers	Computer	Einstellungen des Virtual Delivery Agent	Zulässig (1)
Aktualisierungsmodus für die Zwischenablageauswahl	ClipboardSelectionUpdateMode	Benutzer	Zwischenablage	3
Aktualisierungsmodus für die primäre Auswahl	PrimarySelectionUpdateMode	Benutzer	Zwischenablage	3
Maximale Speex-Qualität	MaxSpeexQuality	Benutzer	Audio	5

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Clientlaufwerke automatisch verbinden	Laufwerke automatisch verbinden	Benutzer	Dateiumleitung/CDM	Aktiviert (1)
Optische Clientlaufwerke	CD-ROM-Laufwerke zulassen	Benutzer	Dateiumleitung/CDM	Zugelassen (1)
Feste Clientlaufwerke	Feste Laufwerke zulassen	Benutzer	Dateiumleitung/CDM	Zugelassen (1)
Client-Diskettenlaufwerke	Diskettenlaufwerke zulassen	Benutzer	Dateiumleitung/CDM	Zugelassen (1)
Client-Netzwerklaufwerke	Netzwerklaufwerke zulassen	Benutzer	Dateiumleitung/CDM	Zugelassen (1)
Clientlaufwerksumleitung	AllowDriveRedir	Benutzer	Dateiumleitung/CDM	Zugelassen (1)
Schreibgeschützter Client-Laufwerkszugriff	ReadOnlyMappedDrive	Benutzer	Dateiumleitung/CDM	Deaktiviert (0)
Automatische Tastaturanzeige	AllowAutoKeyboardPopUp	Benutzer	MRVC	Deaktiviert (0)
Dateitransfer zwischen Desktop und Client zulassen	AllowFileTransfer	Benutzer	Dateiübertragung	Zulässig
Datei vom Desktop herunterladen	AllowFileDownload	Benutzer	Dateiübertragung	Zulässig

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Datei auf den Desktop hochladen	AllowFileUpload	Benutzer	Dateiübertragung	Zulässig
Zeitgeber für inaktive Sitzungen	EnableSessionIdleTimer	Benutzer	Sitzungstimer	Aktiviert (1)
Intervall des Zeitgebers für inaktive Sitzungen	SessionIdleTimerInterval	Benutzer	Sitzungstimer	1440 Minuten
Zeitgeber für getrennte Sitzungen	EnableSessionDisconnectTimer	Benutzer	Sitzungstimer	Deaktiviert (0)
Intervall des Zeitgebers für getrennte Sitzungen	SessionDisconnectTimerPeriod	Benutzer	Sitzungstimer	1440 Minuten

Hinweis:

Nur der Windows Virtual Delivery Agent (VDA) unterstützt Audio über das User Datagram Protocol (UDP). Der Linux VDA unterstützt dies nicht. Weitere Informationen finden Sie unter Audio über User Datagram Protocol (UDP) Real-time Transport.

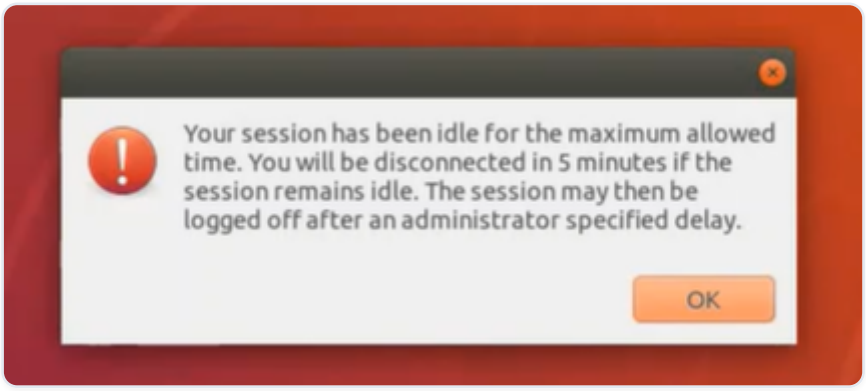
Sie können die folgenden Citrix-Richtlinieneinstellungen verwenden, um Sitzungsverbindungstimer in Citrix Studio zu konfigurieren:

- **Sitzungsinaktivitätstimer**: Legt fest, ob eine Zeitbegrenzung für inaktive Sitzungen erzwungen werden soll.
- **Sitzungsinaktivitätstimer-Intervall**: Legt eine Zeitbegrenzung für inaktive Sitzungen fest. Wenn der Sitzungsinaktivitätstimer **aktiviert** ist und eine aktive Sitzung während der festgelegten Zeit keine Benutzereingaben erhalten hat, wird die Sitzung getrennt.

- **Timer für getrennte Sitzungen**: Legt fest, ob eine Zeitbegrenzung für getrennte Sitzungen erzwungen werden soll.
- **Intervall des Timers für getrennte Sitzungen**: Legt ein Intervall fest, bevor eine getrennte Sitzung abgemeldet wird.

Wenn Sie eine der Richtlinieneinstellungen aktualisieren, stellen Sie sicher, dass diese in Ihrer gesamten Bereitstellung konsistent sind.

Eine Warnmeldung wird angezeigt, wenn Ihr Zeitlimit für inaktive Sitzungen abläuft. Ein Beispiel finden Sie im folgenden Screenshot. Durch Drücken von **OK** wird die Warnmeldung geschlossen, aber Ihre Sitzung bleibt nicht aktiv. Um Ihre Sitzung aktiv zu halten, geben Sie eine Benutzereingabe ein, um den Inaktivitätstimer zurückzusetzen.



Die folgenden Richtlinien können in Citrix Studio Version 7.12 und höher konfiguriert werden.

- MaxSpeexQuality

  Wert (Ganzzahl):

  Standardwert: 5

  Details:

  Die Audioumleitung kodiert Audiodaten mit dem Speex-Codec, wenn die Audioqualität mittel oder niedrig ist (siehe die Richtlinie Audioqualität). Speex ist ein verlustbehafteter Codec, was bedeutet, dass er Komprimierung auf Kosten der Wiedergabetreue des eingehenden Sprachsignals erreicht. Im Gegensatz zu einigen anderen Sprach-Codecs ist es möglich, den Kompromiss zwischen Qualität und Bitrate zu steuern. Der Speex-Kodierungsprozess wird meistens durch einen Qualitätsparameter gesteuert, der von 0 bis 10 reicht. Je höher die Qualität, desto höher die Bitrate.

  Die maximale Speex-Qualität wählt die beste Speex-Qualität zur Kodierung von Audiodaten entsprechend der Audioqualität und der Bandbreitenbegrenzung (siehe die Richtlinie

Bandbreitenbegrenzung für Audioumleitung). Wenn die Audioqualität mittel ist, arbeitet der Encoder im Breitbandmodus, was eine höhere Abtastrate bedeutet. Wenn die Audioqualität niedrig ist, arbeitet der Encoder im Schmalbandmodus, was eine niedrigere Abtastrate bedeutet. Dieselbe Speex-Qualität hat in verschiedenen Modi unterschiedliche Bitraten. Die beste Speex-Qualität liegt vor, wenn der größte Wert die folgenden Bedingungen erfüllt:

- Sie ist gleich oder kleiner als die maximale Speex-Qualität.
- Ihre Bitrate ist gleich oder kleiner als die Bandbreitenbegrenzung.

Verwandte Einstellungen: Audioqualität, Bandbreitenbegrenzung für Audioumleitung

- PrimarySelectionUpdateMode

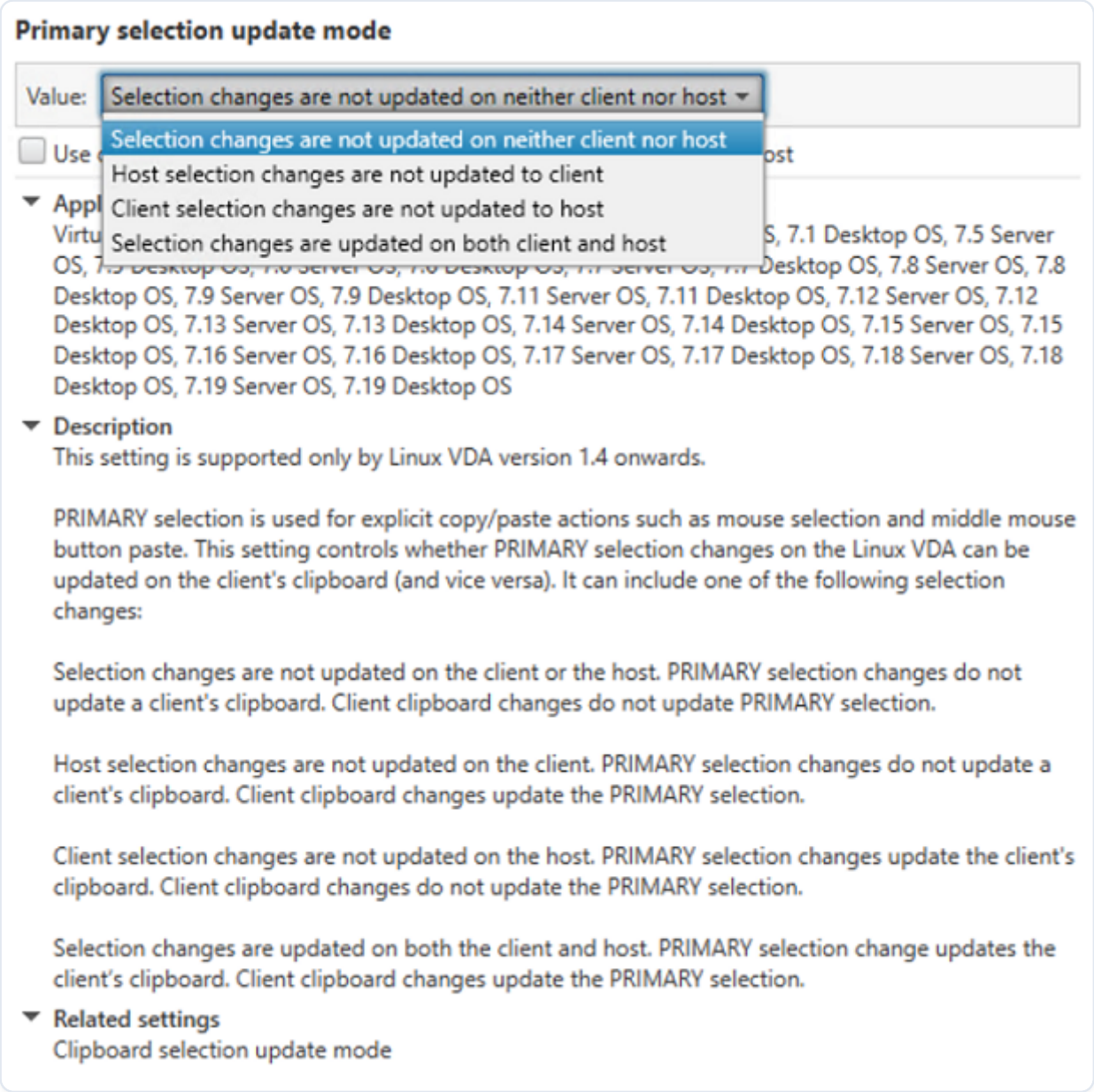
  Wert (Enum):

  Standardwert: 3

  Details:

  Die primäre Auswahl wird verwendet, wenn Sie Daten auswählen und diese durch Drücken der mittleren Maustaste einfügen.

  Diese Richtlinie steuert, ob Änderungen der primären Auswahl auf dem Linux VDA und dem Client die Zwischenablage des jeweils anderen aktualisieren können. Es gibt vier Wertoptionen:



- **Auswahländerungen werden weder auf dem Client noch auf dem Host aktualisiert**

  Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Host-Auswahländerungen werden nicht auf den Client aktualisiert**

  Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA.

- **Client-Auswahländerungen werden nicht auf den Host aktualisiert**

Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Auswahländerungen werden sowohl auf dem Client als auch auf dem Host aktualisiert**

  Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA. Diese Option ist der Standardwert.

Zugehörige Einstellung: Aktualisierungsmodus der Zwischenablageauswahl

- ClipboardSelectionUpdateMode

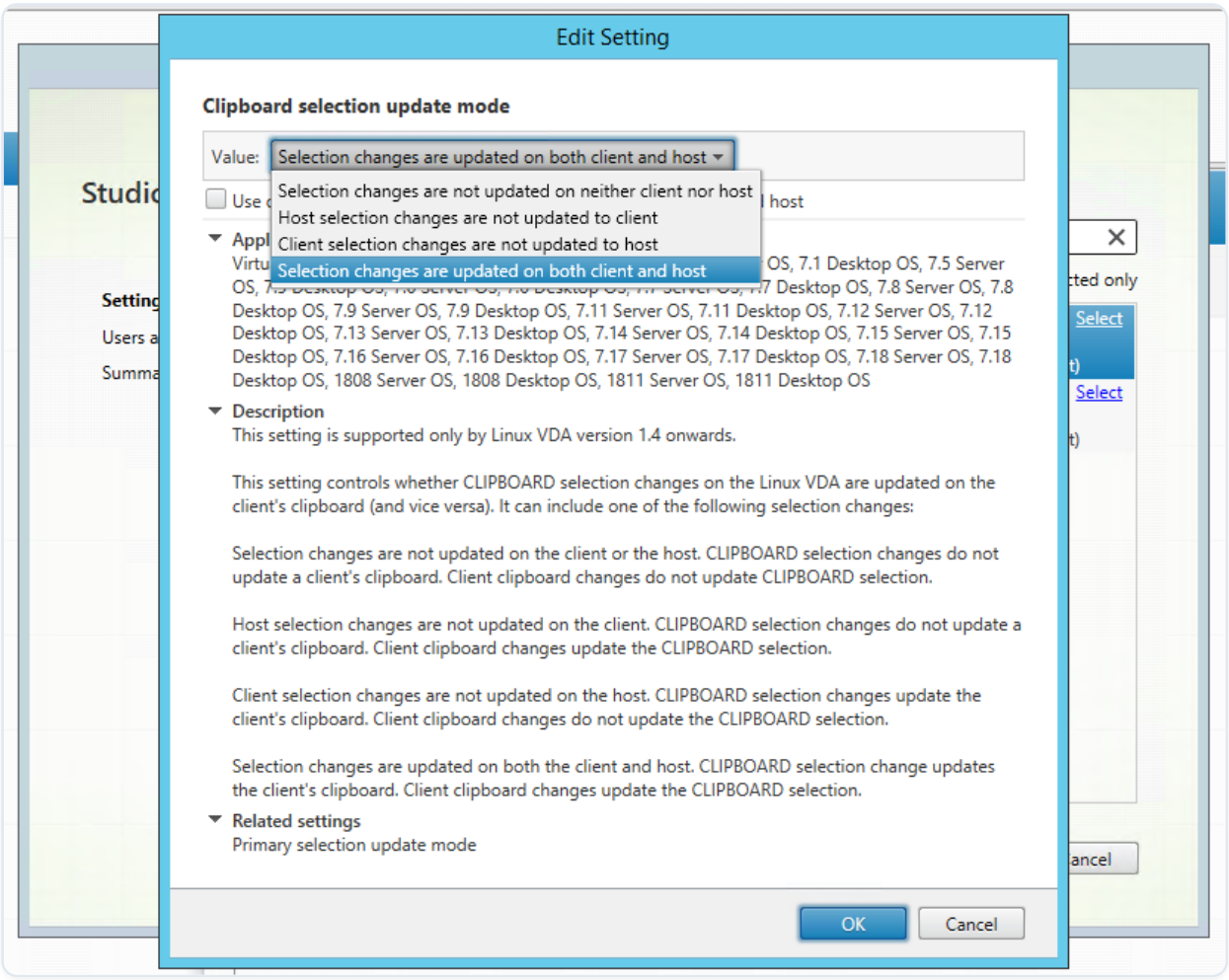
  Wert (Enum):

  Standardwert: 3

  Details:

  Die Zwischenablageauswahl wird verwendet, wenn Sie Daten auswählen und explizit anfordern, dass sie in die Zwischenablage „kopiert“ werden, z. B. durch Auswahl von „Kopieren“ aus dem Kontextmenü. Die Zwischenablageauswahl wird hauptsächlich in Verbindung mit Microsoft Windows-Zwischenablagevorgängen verwendet, während die primäre Auswahl einzigartig für Linux ist.

  Diese Richtlinie steuert, ob Änderungen der Zwischenablageauswahl auf dem Linux VDA und dem Client die Zwischenablage des jeweils anderen aktualisieren können. Es gibt vier Wertoptionen:



- **Auswahländerungen werden weder auf dem Client noch auf dem Host aktualisiert**

  Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Host-Auswahländerungen werden nicht auf den Client aktualisiert**

  Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA.

- **Client-Auswahländerungen werden nicht auf den Host aktualisiert**

  Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Auswahländerungen werden sowohl auf dem Client als auch auf dem Host aktualisiert**

Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA. Diese Option ist der Standardwert.

Zugehörige Einstellung: Aktualisierungsmodus für die primäre Auswahl

Hinweis:

Der Linux VDA unterstützt sowohl die Zwischenablageauswahl als auch die primäre Auswahl. Um das Kopier- und Einfügeverhalten zwischen dem Linux VDA und dem Client zu steuern, empfehlen wir, sowohl den Aktualisierungsmodus für die Zwischenablageauswahl als auch den Aktualisierungsmodus für die primäre Auswahl auf denselben Wert einzustellen.

IPv6 konfigurieren

Der Linux VDA unterstützt IPv6, um mit Citrix Virtual Apps and Desktops kompatibel zu sein. Beachten Sie bei der Verwendung dieser Funktion Folgendes:

- In Dual-Stack-Umgebungen wird IPv4 verwendet, es sei denn, IPv6 ist explizit aktiviert.
- Wenn IPv6 in einer IPv4-Umgebung aktiviert ist, funktioniert der Linux VDA nicht.

Wichtig:

- Die gesamte Netzwerkumgebung muss IPv6 sein, nicht nur für den Linux VDA.
- Centrify unterstützt kein reines IPv6.

Bei der Installation des Linux VDA sind keine speziellen Einrichtungsschritte für IPv6 erforderlich.

IPv6 für den Linux VDA konfigurieren

Bevor Sie die Konfiguration für den Linux VDA ändern, stellen Sie sicher, dass Ihre Linux-VM zuvor in einem IPv6-Netzwerk funktioniert hat. Es gibt zwei Registrierungsschlüssel, die sich auf die IPv6-Konfiguration beziehen:

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

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

OnlyUseIPv6ControllerRegistration muss auf 1 gesetzt werden, um IPv6 auf dem Linux VDA zu aktivieren:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
```

Wenn der Linux VDA mehr als eine Netzwerkschnittstelle hat, kann **ControllerRegistrationIPv6Netmask** verwendet werden, um anzugeben, welche für die Linux VDA-Registrierung verwendet wird:

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

Ersetzen Sie **{IPv6 netmask}** durch die tatsächliche Netzmaske (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 verwenden Sie ping6, um zu prüfen, ob AD und Delivery Controller™ erreichbar sind.

Konfigurieren des Citrix Customer Experience Improvement Program (CEIP)

Wenn Sie am CEIP teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, um die Qualität und Leistung von Citrix-Produkten zu verbessern. Zusätzlich wird eine Kopie der anonymen Daten zur schnellen und effizienten Analyse an Google Analytics (GA) gesendet.

Registrierungseinstellungen

Standardmäßig nehmen Sie automatisch am CEIP teil, wenn Sie den Linux VDA installieren. Der erste Daten-Upload erfolgt etwa sieben Tage nach der Installation des Linux VDA. Sie können diese Standardeinstellung in der Registrierung ändern.

- **CEIPSwitch**

Registrierungseinstellung, die das CEIP aktiviert oder deaktiviert (Standard = 0):

Speicherort: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Name: CEIPSwitch

Wert: 1 = deaktiviert, 0 = aktiviert

Wenn nicht angegeben, ist das CEIP aktiviert.

Sie können den folgenden Befehl auf einem Client ausführen, um das CEIP zu deaktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

- **GASwitch**

Registrierungseinstellung, die GA aktiviert oder deaktiviert (Standard = 0):

Speicherort: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Name: GASwitch

Wert: 1 = deaktiviert, 0 = aktiviert

Wenn nicht angegeben, ist GA aktiviert.

Sie können den folgenden Befehl auf einem Client ausführen, um GA zu deaktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "GASwitch" -d "1"
```

- **DataPersistPath**

Registrierungseinstellung, die den Datenpfad steuert (Standard = /var/xdl/ceip):

Speicherort: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Name: DataPersistPath

Wert: String

Sie können den folgenden Befehl ausführen, um diesen Pfad festzulegen:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "DataPersistPath" -d
"your_path"
```

Wenn der konfigurierte Pfad nicht existiert oder nicht zugänglich ist, werden die Daten im Standardpfad gespeichert.

CEIP-Daten, die vom Linux VDA erfasst werden

Die folgende Tabelle zeigt ein Beispiel für die Arten der gesammelten anonymen Informationen. Die Daten enthalten keine Details, 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-Kernel-Version	kernel_version	Textzeichenfolge, die die Kernel-Version 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 angibt, ob das aktuelle Linux VDA-Paket neu installiert oder aktualisiert wird
LVDA-Installationsmethode	install_method	Textzeichenfolge, die angibt, dass das aktuelle Linux VDA-Paket mit MCS, PVS,

DATENPUNKT	SCHLÜSSELNAME	BESCHREIBUNG
		einfacher Installation oder manueller Installation installiert wurde.
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
Systemgebietsschema	system_locale	Textzeichenfolge, die das Gebietsschema dieser Maschine angibt
Letzte Neustartzeit der LVDA-Schlüsseldienste	Ctxhdx Ctxvda	Die letzte Neustartzeit der Dienste `ctxhdx` und `ctxvda` im Format TT-HH:MM:SS, zum Beispiel 10-17:22:19
GPU-Typ	gpu_type	Bezeichnet den GPU-Typ der Maschine
CPU-Kerne	cpu_cores	Ganzzahl, die die Anzahl der CPU-Kerne der Maschine angibt
CPU-Frequenz	cpu_frequency	Gleitkommazahl, die die CPU-Frequenz in MHz angibt
Physische Speichergröße	memory_size	Ganzzahl, die die physische Speichergröße in KB angibt
Anzahl gestarteter Sitzungen	session_launch	Ganzzahl, die die Anzahl der auf der Maschine gestarteten (angemeldeten oder wiederverbundenen) Sitzungen zum Zeitpunkt der Erfassung dieses Datenpunkts angibt

DATENPUNKT	SCHLÜSSELNAME	BESCHREIBUNG
Linux-Betriebssystemname und -Version	os_name_version	Textzeichenfolge, die den Namen und die Version des Linux-Betriebssystems des Computers 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 Sitzungszeit	active_session_time	Wird verwendet, um die aktiven Zeiten der Sitzung zu speichern. Eine Sitzung kann mehrere aktive Zeiten haben, da die Sitzung die Verbindung trennen/trennen/ wiederherstellen kann.
Sitzungsdauer	session_duration_time	Wird verwendet, um die Dauer der Sitzung von der Anmeldung bis zur Abmeldung zu speichern.
Receiver-Clienttyp	receiver_type	Integer, der den Typ der Citrix Workspace-App angibt, die zum Starten der Sitzung verwendet wurde
Receiver-Client-Version	receiver_version	Textzeichenfolge, die die Version der Citrix Workspace-App angibt, die zum Starten der Sitzung verwendet wurde
Druckanzahl	printing_count	Integer, der angibt, wie oft die Sitzung die Druckfunktion verwendet

DATENPUNKT	SCHLÜSSELNAME	BESCHREIBUNG
Anzahl der USB-Umleitungen	usb_redirecting_count	Integer, der angibt, wie oft die Sitzung ein USB-Gerät verwendet
Gfx-Anbietertyp	gfx_provider_type	Textzeichenfolge, die den Grafik-Anbietertyp der Sitzung angibt
Shadowing-Anzahl	shadow_count	Ganzzahl, die angibt, wie oft die Sitzung überwacht wurde
Vom Benutzer ausgewählte Sprache	ctxism_select	Zusammengesetzte lange Zeichenfolge, die alle Sprachen enthält, die Benutzer ausgewählt haben
Anzahl der Smartcard-Umleitungen	scard_redirecting_count	Ganzzahl, die angibt, wie oft die Smartcard-Umleitung für Sitzungsanmeldungen und die Benutzerauthentifizierung für In-Session-Apps verwendet wird

USB-Umleitung konfigurieren

USB-Geräte werden zwischen der Citrix Workspace™-App und dem Linux VDA-Desktop gemeinsam genutzt. Wenn ein USB-Gerät auf den Desktop umgeleitet wird, kann der Benutzer das USB-Gerät so verwenden, als wäre es lokal angeschlossen.

> **Tipp:**

> Wir empfehlen die Verwendung der USB-Umleitung, wenn die Netzwerklatenz unter 100 Millisekunden liegt. Verwenden Sie die USB-Umleitung nicht, wenn die Netzwerklatenz über 200 Millisekunden liegt.

> Die USB-Umleitung umfasst drei Hauptfunktionsbereiche:

- Open-Source-Projektimplementierung (VHCI)

- VHCI-Dienst
- USB-Dienst

Open-Source-VHCI:

Dieser Teil der USB-Umleitungsfunktion entwickelt ein allgemeines System zur gemeinsamen Nutzung von USB-Geräten über ein IP-Netzwerk. Es besteht aus einem Linux-Kernel-Treiber und einigen Benutzermodus-Bibliotheken, die die Kommunikation mit dem Kernel-Treiber ermöglichen, um alle USB-Daten zu erhalten. Bei der Linux VDA-Implementierung verwendet Citrix den Kernel-Treiber von VHCI wieder. Alle USB-Datenübertragungen zwischen dem Linux VDA und der Citrix Workspace-App werden jedoch im Citrix ICA®-Protokollpaket gekapselt.

VHCI-Dienst:

Der VHCI-Dienst ist ein von Citrix bereitgestellter Open-Source-Dienst zur Kommunikation mit dem VHCI-Kernelmodul. Dieser Dienst fungiert als Gateway zwischen VHCI und dem Citrix USB-Dienst.

USB-Dienst:

Der USB-Dienst stellt ein Citrix-Modul dar, das alle Virtualisierungen und Datenübertragungen auf dem USB-Gerät verwaltet.

Funktionsweise der USB-Umleitung

Wenn ein USB-Gerät erfolgreich auf den Linux VDA umgeleitet wird, werden in der Regel ein oder mehrere Geräteknoten im Systempfad /dev erstellt. Manchmal ist das umgeleitete Gerät jedoch für eine aktive Linux VDA-Sitzung nicht verwendbar. USB-Geräte benötigen Treiber, um ordnungsgemäß zu funktionieren, und einige Geräte erfordern spezielle Treiber. Wenn keine Treiber bereitgestellt werden, sind die umgeleiteten USB-Geräte für die aktive Linux VDA-Sitzung nicht zugänglich. Um die USB-Gerätekonnektivität sicherzustellen, installieren Sie die Treiber und konfigurieren Sie das System ordnungsgemäß.

Der Linux VDA unterstützt eine Liste von USB-Geräten, die erfolgreich zum und vom Client umgeleitet werden. Darüber hinaus wird das Gerät, insbesondere die USB-Festplatte, ordnungsgemäß gemountet, sodass der Benutzer ohne zusätzliche Konfiguration auf die Festplatte zugreifen kann.

Unterstützte USB-Geräte

Die folgenden Geräte wurden dahingehend überprüft, dass sie diese Version des Linux VDA unterstützen. Andere Geräte können zwar verwendet werden, dies kann jedoch zu unerwarteten Ergebnissen führen:

Hinweis:

Der Linux VDA unterstützt nur USB 2.0-Protokolle.

USB-MASSENSPEICHERGERÄT	VID:PID	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-Laufwerk	0781:5580	FAT32
WD HDD	1058:10B8	FAT32

USB-3D-MAUS	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

USB-SCANNER	VID:PID
Epson Perfection V330 Photo	04B8: 0142

USB-Umleitung konfigurieren

Eine Citrix-Richtlinie steuert, ob die USB-Geräteumleitung aktiviert oder deaktiviert ist. Darüber hinaus kann der Gerätetyp auch mithilfe einer Delivery Controller™-Richtlinie angegeben werden.

Wenn Sie die USB-Umleitung für den Linux VDA konfigurieren, konfigurieren Sie die folgende Richtlinie und die folgenden Regeln:

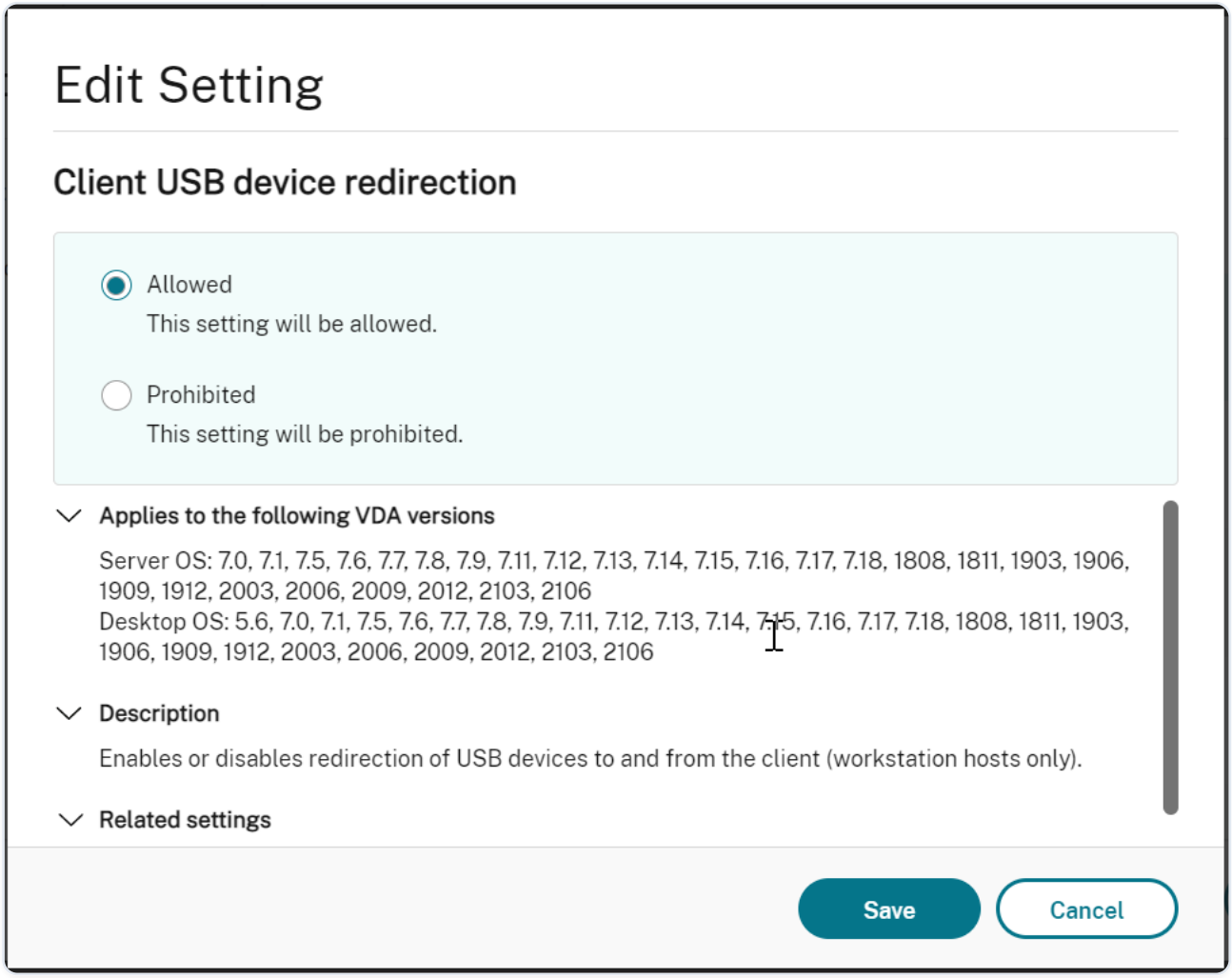
- Client-USB-Geräteumleitungsrichtlinie
- Client-USB-Geräteumleitungsregeln

USB-Umleitung aktivieren

Aktivieren (oder deaktivieren) Sie in Citrix Studio die USB-Geräteumleitung zum und vom Client (nur für Workstation-Hosts).

Im Dialogfeld **Einstellung bearbeiten**:

1. Wählen Sie **Zulässig**.
2. Klicken Sie auf **OK**.

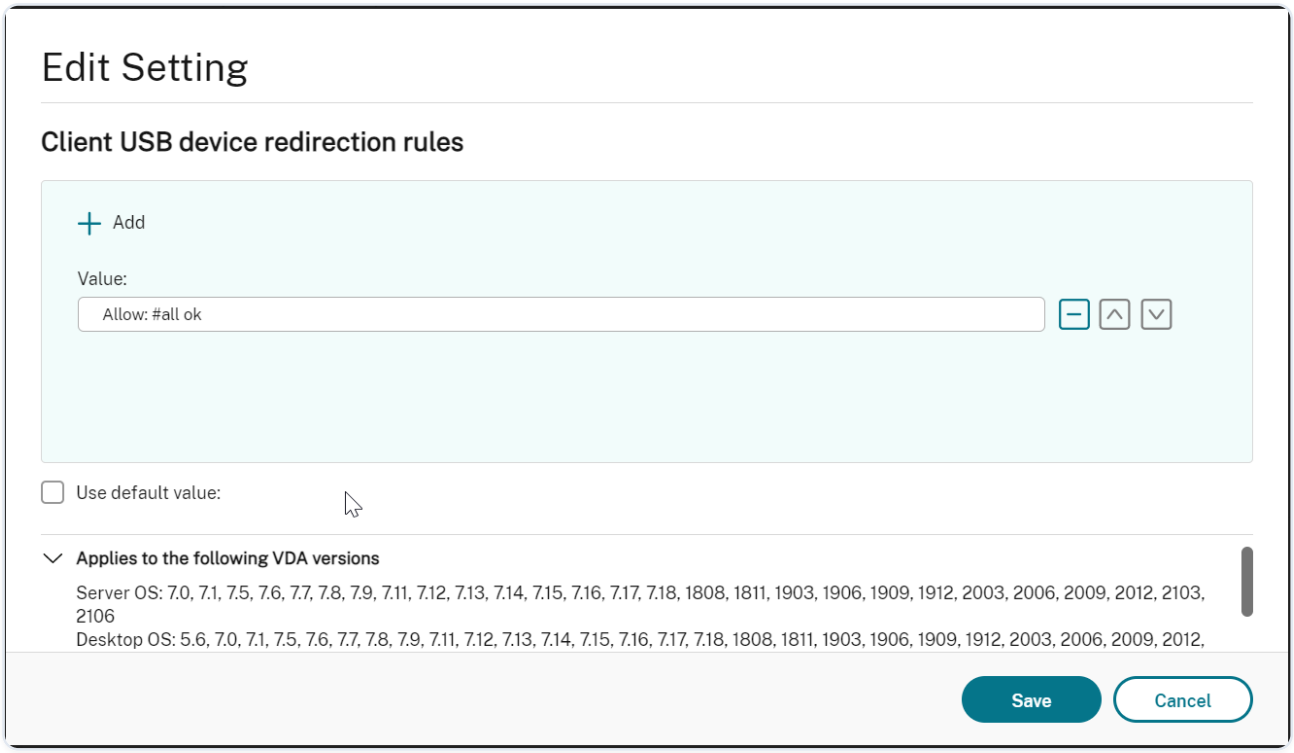


USB-Umleitungsregeln festlegen

Nachdem Sie die USB-Umleitungsrichtlinie aktiviert haben, legen Sie die Umleitungsregeln mithilfe von Citrix Studio fest, indem Sie angeben, welche Geräte auf dem Linux VDA zugelassen (oder verweigert) werden.

Im Dialogfeld „Client-USB-Geräteumleitungsregeln“:

1. Klicken Sie auf **Neu**, um eine Umleitungsregel hinzuzufügen, oder auf **Bearbeiten**, um eine vorhandene Regel zu überprüfen.
2. Klicken Sie nach dem Erstellen (oder Bearbeiten) einer Regel auf **OK**.



VHCI-Kernelmodul erstellen

Die USB-Umleitung hängt von den VHCI-Kernelmodulen (`usb-vhci-hcd.ko` und `usb-vhci-iocif.ko`) ab. Diese Module sind Teil der Linux VDA-Distribution (als Teil des RPM-Pakets). Sie werden basierend auf den offiziellen Linux-Distributions-Kerneln kompiliert und sind in der folgenden Tabelle aufgeführt:

UNTERSTÜTZTE LINUX-DISTRIBUTION	KERNEL-VERSION
RHEL 8.3, CentOS 8.3	4.18.0-240
RHEL 8.2, CentOS 8.2	4.18.0-240

UNTERSTÜTZTE LINUX-DISTRIBUTION	KERNEL-VERSION
RHEL 8.1, CentOS 8.1	4.18.0-240
RHEL 7.9, CentOS 7.9	3.10.0-1160
RHEL 7.8, CentOS 7.8	3.10.0-1160
SUSE 12.5	4.12.14
Ubuntu 20.04	5.4.0-70
Ubuntu 18.04	4.15.0-140
Ubuntu 16.04	4.4.0-206
Debian 10	4.19.0-16

Wichtig:

Wenn der Kernel Ihres Computers nicht mit dem für den Linux VDA erstellten Treiber kompatibel ist, kann der USB-Dienst möglicherweise nicht gestartet werden. In diesem Fall können Sie die USB-Umleitungsfunktion nur verwenden, wenn Sie Ihre eigenen VHCI-Kernelmodule erstellen.

Überprüfen Sie, ob Ihr Kernel mit den von Citrix erstellten Modulen konsistent ist

Führen Sie in der Befehlszeile den folgenden Befehl aus, um zu überprüfen, ob der Kernel konsistent ist:

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

Wenn der Befehl erfolgreich ausgeführt wird, wurde das Kernelmodul erfolgreich geladen und die Version ist mit der von Citrix installierten konsistent.

Wenn der Befehl Fehler meldet, ist der Kernel mit dem Citrix-Modul inkonsistent und muss neu erstellt werden.

VHCI-Kernelmodul neu erstellen

Wenn Ihr Kernelmodul mit der Citrix-Version inkonsistent ist, führen Sie die folgenden Schritte aus:

1. Laden Sie den LVDA-Quellcode von der Citrix-Downloadseite herunter. Wählen Sie die Datei aus, die im Abschnitt „**Linux Virtual Delivery Agent (Quellen)**“ enthalten ist.
2. Extrahieren Sie die Datei **citrix-linux-vda-sources.zip**. Navigieren 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 das Linux VDA-Paket installiert ist, und führen Sie dann einen der folgenden Befehle aus:

   - `sudo bash ctxusbcfg.sh dkms`

     Mit diesem Befehl können Sie das Programm Dynamic Kernel Module Support (DKMS) 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 Ihrem VDA. Bei der Installation der Programme auf RHEL und CentOS installiert und aktiviert der Befehl das Repository Extra Packages for Enterprise Linux (EPEL) auf Ihrem VDA.
     >
     > DKMS kann beim Durchführen eines größeren Kernel-Upgrades, z. B. von Version 4.x.y auf Version 5.x.y, die VHCI-Kernelmodule (`usb-vhci-hcd.ko` und `usb-vhci-iocif.ko`) möglicherweise nicht erstellen. Wenn DKMS fehlschlägt, führen Sie `sudo bash ctxusbcfg.sh dkms` erneut aus.

   - `sudo bash ctxusbcfg.sh build`

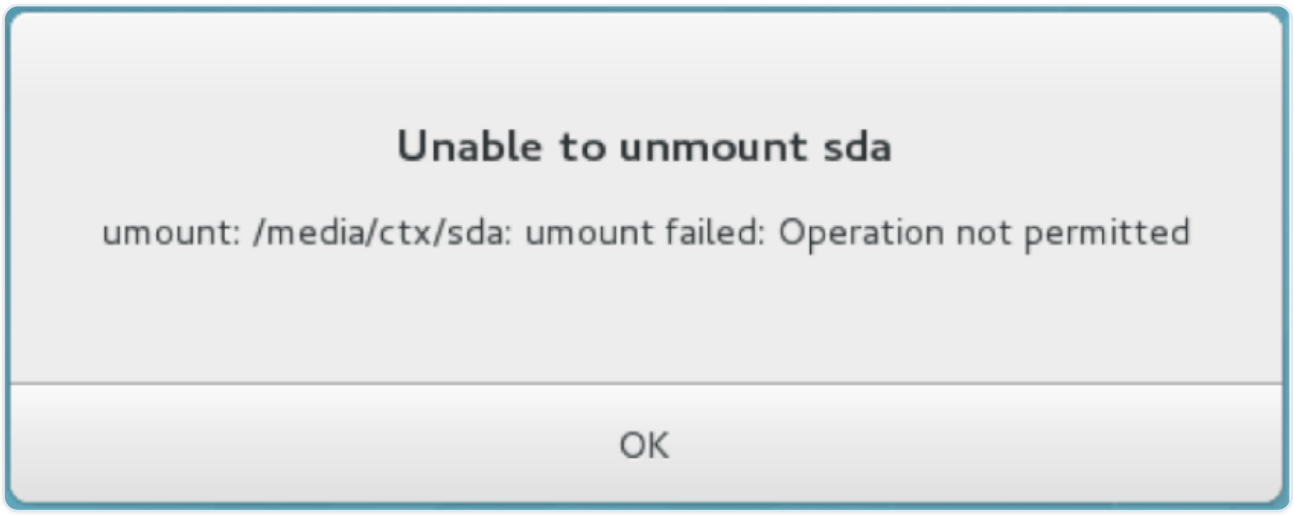
     Dieser Befehl erstellt und installiert die VHCI-Kernelmodule ohne die DKMS-Option.

Beheben von Problemen bei der USB-Umleitung

Verwenden Sie die Informationen in diesem Abschnitt, um verschiedene Probleme zu beheben, die bei der Verwendung des Linux VDA auftreten können.

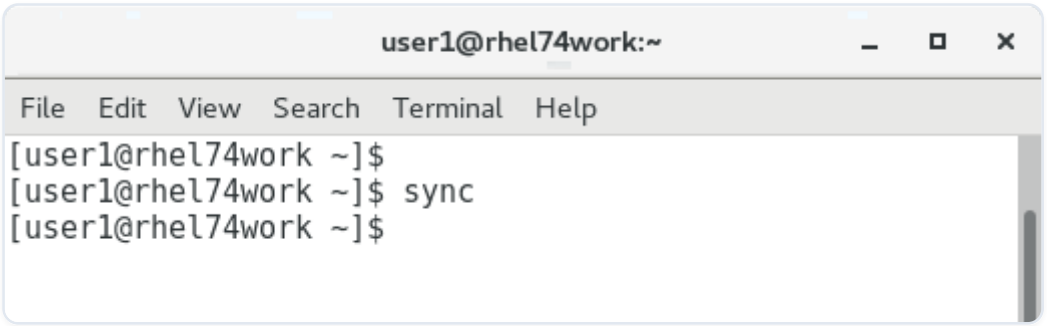
Umgeleitete USB-Festplatte kann nicht ausgeworfen werden

Für die Zugriffssteuerung aller von der Citrix Workspace-App umgeleiteten USB-Festplatten verwaltet der Linux VDA alle diese Geräte mit Administratorrechten, um sicherzustellen, dass nur der Besitzer auf das umgeleitete Gerät zugreifen kann. Folglich kann der Benutzer das Gerät ohne Administratorrechte nicht auswerfen.



Datei geht verloren, wenn Sie die Umleitung einer USB-Festplatte beenden

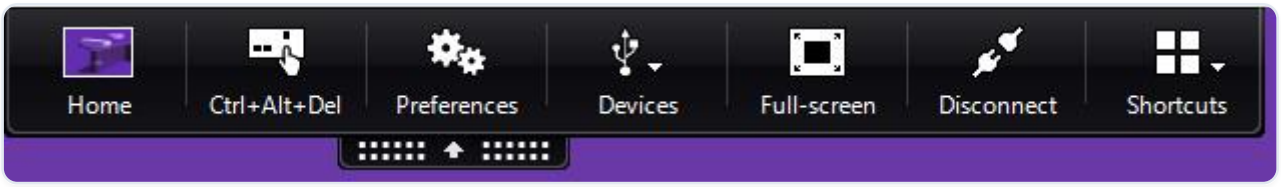
Wenn Sie eine USB-Festplatte an eine Sitzung umleiten und versuchen, sie zu ändern (z. B. einige Dateien auf der Festplatte zu erstellen), und dann die Umleitung sofort über die Symbolleiste der Citrix Workspace-App beenden, kann die von Ihnen geänderte oder erstellte Datei verloren gehen. Dieses Problem tritt auf, weil das System beim Schreiben von Daten in ein Dateisystem den Speicher-Cache im Dateisystem einbindet. Die Daten werden nicht auf die Festplatte selbst geschrieben. Wenn Sie die Umleitung über die Symbolleiste der Citrix Workspace-App beenden, bleibt keine Zeit mehr, die Daten auf die Festplatte zu schreiben, was zu Datenverlust führt. Um dieses Problem zu beheben, verwenden Sie den Befehl sync in einem Terminal, um Daten auf die Festplatte zu schreiben, bevor Sie die USB-Umleitung beenden.



Keine Geräte in der Symbolleiste der Citrix Workspace-App

Manchmal werden Geräte nicht in der Symbolleiste der Citrix Workspace-App angezeigt, was darauf hindeutet, dass keine USB-Umleitung stattfindet. Wenn dieses Problem auftritt, überprüfen Sie Folgendes:

- Die Richtlinie ist so konfiguriert, dass sie die USB-Umleitung zulässt
- Das Kernelmodul ist mit Ihrem Kernel kompatibel



> **Hinweis:**
>
> Die Registerkarte **Geräte** ist in der Citrix Workspace-App für Linux nicht verfügbar.

Fehlgeschlagene Umleitung, wenn USB-Geräte in der Symbolleiste der Citrix Workspace-App sichtbar sind, aber als *richtlinienbeschränkt* gekennzeichnet sind

Wenn das Problem auftritt, gehen Sie wie folgt vor:

- Konfigurieren Sie die Linux VDA-Richtlinie, um die Umleitung zu aktivieren.
- Überprüfen Sie, ob zusätzliche Richtlinieneinschränkungen in der Registrierung der Citrix Workspace-App konfiguriert sind. Überprüfen Sie **DeviceRules** im Registrierungspfad, um sicherzustellen, dass der Zugriff auf das Gerät durch diese Einstellung nicht verweigert wird:

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

Ein USB-Gerät wird erfolgreich umgeleitet, aber ich kann es in meiner Sitzung nicht verwenden

In der Regel können nur unterstützte USB-Geräte umgeleitet werden. Andere Geräte können ebenfalls an eine aktive Linux VDA-Sitzung umgeleitet werden. Für jedes umgeleitete Gerät wird ein dem Benutzer gehörender Knoten im Systempfad **/dev** erstellt. Es sind jedoch die Treiber und die Konfiguration, die bestimmen, ob der Benutzer das Gerät erfolgreich verwenden kann. Wenn Sie ein Gerät finden, das zwar angeschlossen (im Besitz) ist, aber nicht zugänglich ist, fügen Sie das Gerät einer uneingeschränkten Richtlinie hinzu.

Hinweis:

Bei USB-Laufwerken konfiguriert und mountet der Linux VDA die Festplatte. Der Benutzer (und nur der Besitzer, der es installiert hat) kann ohne zusätzliche Konfiguration auf die Festplatte zugreifen. Dies trifft möglicherweise nicht auf Geräte zu, die nicht in der Liste der unterstützten Geräte aufgeführt sind.

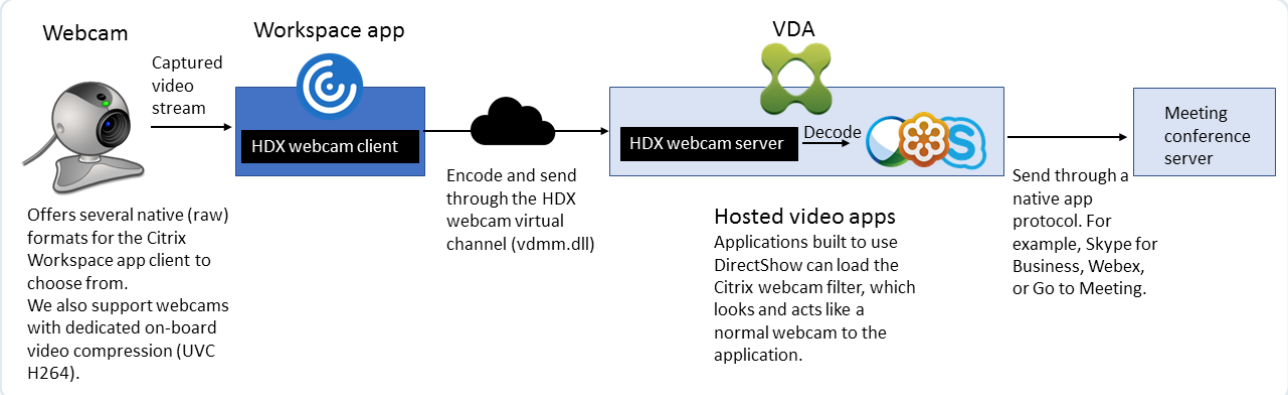
HDX™ Webcam-Videokompression

Übersicht

Benutzer von Videokonferenzanwendungen, die in Linux-VDA-Sitzungen ausgeführt werden, können ihre Webcams jetzt mit HDX-Webcam-Videokompression verwenden. Diese Funktion ist standardmäßig aktiviert. Wir empfehlen, nach Möglichkeit immer die HDX-Webcam-Videokompression zu verwenden.

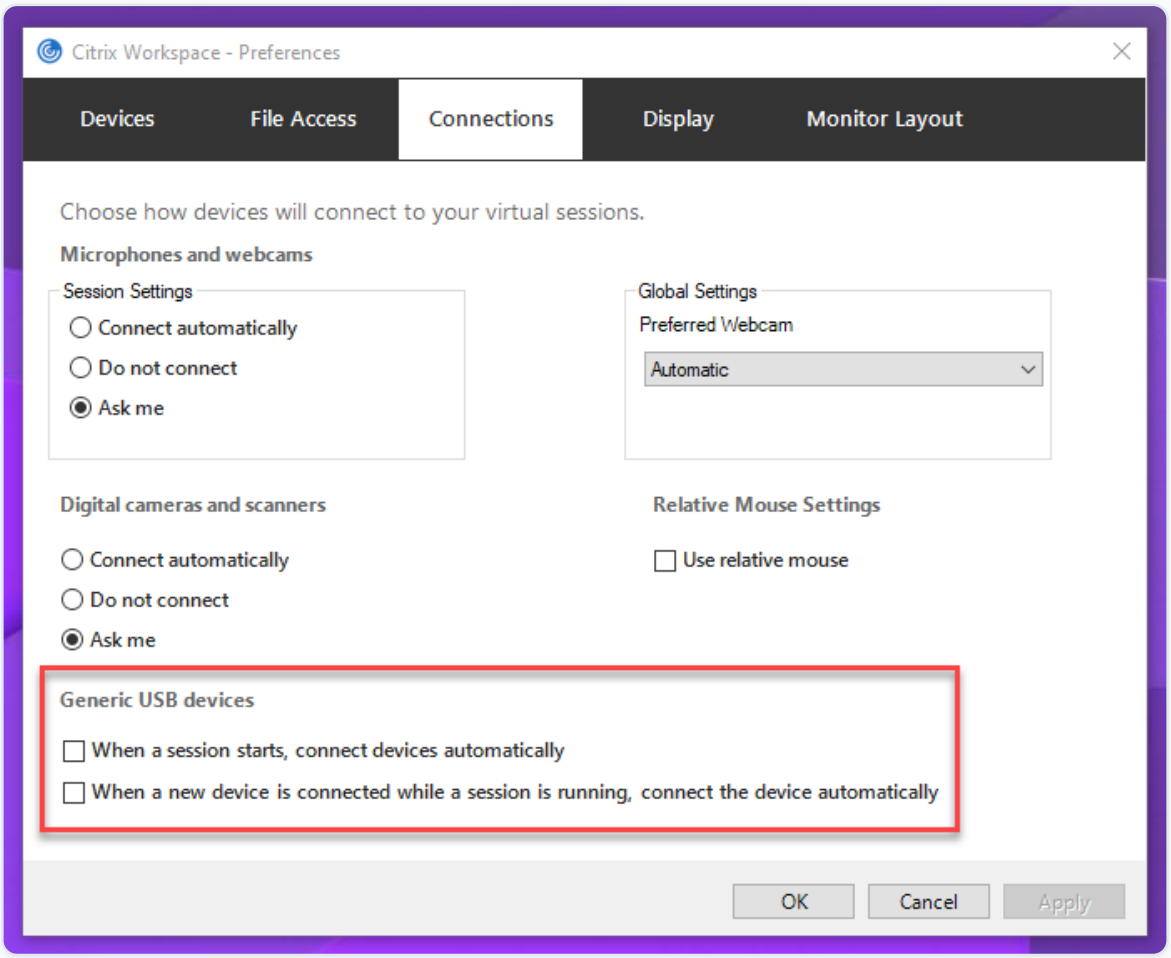
Die HDX-Webcam-Videokompression wird auch als **optimierter** Webcam-Modus bezeichnet. Diese Art der Webcam-Videokompression sendet das H.264-Video direkt an die Videokonferenzanwendung, die in der virtuellen Sitzung ausgeführt wird. Die HDX-Webcam-Videokompression verwendet die Multimedia-Framework-Technologie, die Teil des Clientbetriebssystems ist, um Videos von Erfassungsgeräten abzufangen, zu transkodieren und zu komprimieren. Hersteller von Erfassungsgeräten liefern die Treiber, die in die Kernel-Streaming-Architektur des Betriebssystems integriert werden.

Der Client übernimmt die Kommunikation mit der Webcam. Der Client sendet das Video dann nur an den Server, der es ordnungsgemäß anzeigen kann. Der Server kommuniziert nicht direkt mit der Webcam, aber seine Integration bietet Ihnen dieselbe Erfahrung auf Ihrem Desktop. Die Workspace-App komprimiert das Video, um Bandbreite zu sparen und eine bessere Ausfallsicherheit in WAN-Szenarien zu gewährleisten.



Hinweis:

- Diese Funktion unterstützt nur H.264-Videos von Ihrem Citrix Workspace-App-Client.
- Die unterstützte Webcam-Auflösung liegt zwischen 48x32 und 1920x1080.
- Wählen Sie nicht **Generische USB-Geräte** aus der Symbolleiste Ihrer Citrix Workspace™-App, wenn Sie eine Webcam verwenden. Andernfalls können unerwartete Probleme auftreten.



Unterstützte Linux-Distributionen

- RHEL 8.4/CentOS 8 (2105)
- RHEL 8.3/CentOS 8.3
- RHEL 7.9/CentOS 7.9
- Ubuntu 20.04
- Ubuntu 18.04

- Ubuntu 16.04
- Debian 10

Vollständig getestete Webcams

Verschiedene Webcams bieten unterschiedliche Bildraten und haben unterschiedliche Helligkeits- und Kontraststufen. Citrix® verwendet die folgenden Webcams für die anfängliche Funktionsvalidierung:

- Logitech HD Webcam C270
- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

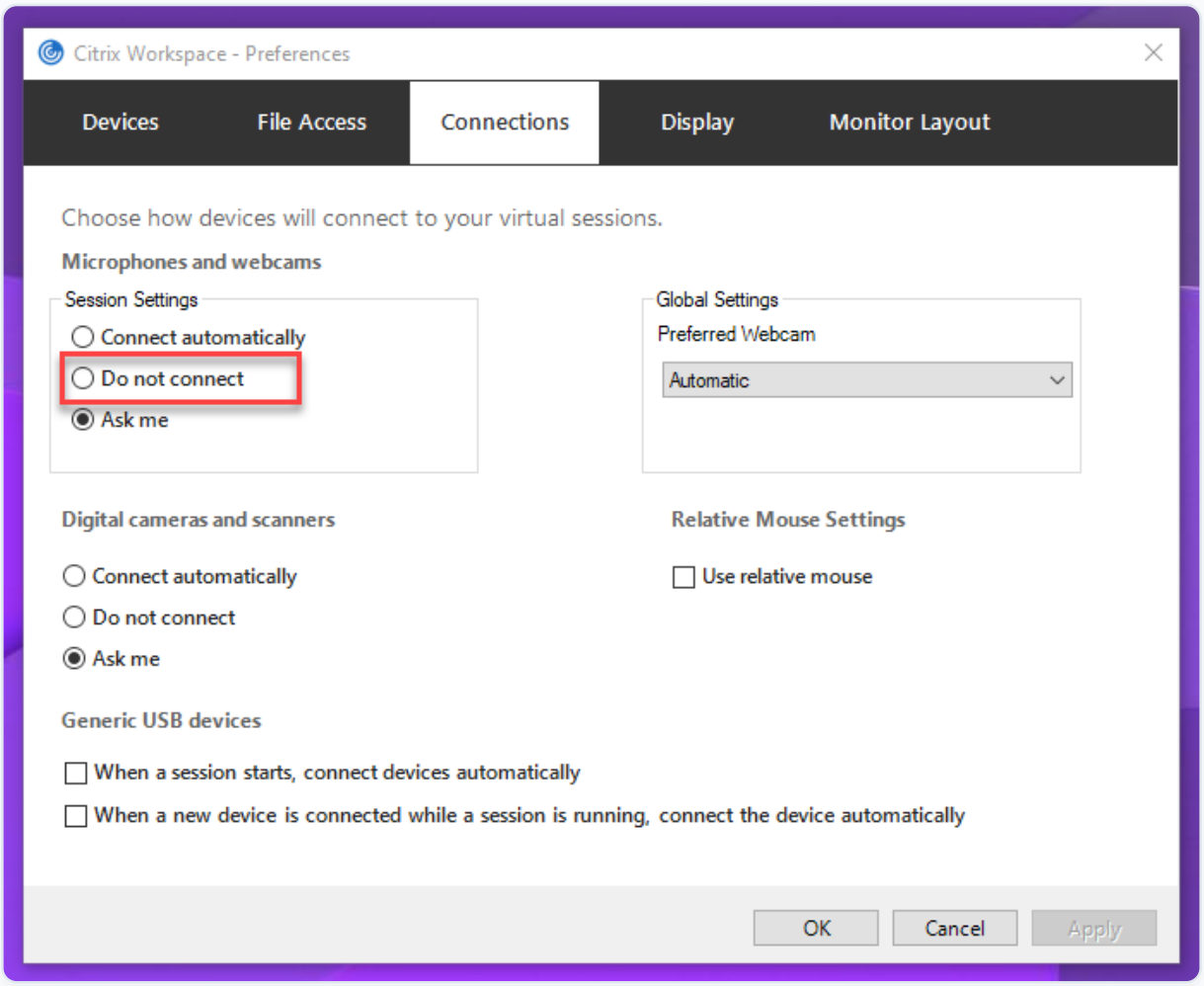
Konfiguration

Diese Funktion ist standardmäßig aktiviert. Um sie zu verwenden, führen Sie die folgende Überprüfung und Konfiguration durch:

> **Tipp:**

> Citrix Workspace app-Benutzer können die Standardeinstellung überschreiben, indem sie in der Desktop Viewer-Einstellung **Mikrofone und Webcams** die Option **Nicht verbinden**

wählen.



1. Nach Abschluss der VDA-Installation überprüfen Sie, ob Ihr VDA sich beim Delivery Controller™ registrieren kann und die veröffentlichten Linux-Desktopsitzungen erfolgreich mit Windows-Anmeldeinformationen gestartet werden können.
2. Stellen Sie sicher, dass Ihr VDA über Internetzugang verfügt, und führen Sie dann den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um Ihre Webcam-Konfigurationen abzuschließen. Wenn Ihr VDA keinen Internetzugang hat, fahren Sie mit Schritt 3 fort.

   Wenn Ihr VDA auf Debian 10 bereitgestellt wird, stellen Sie sicher, dass er mit der neuesten Kernel-Version läuft. Andernfalls führen Sie die folgenden Befehle aus, um auf die neueste Kernel-Version zu aktualisieren:

   ```
   sudo apt-get update

   sudo apt-get dist-upgrade
   ```

```
sudo reboot
```

Das Skript ctxwcamcfg.sh hilft dabei, Folgendes zu tun:

a. Die Programme `FFmpeg`, `kernel-devel` und Dynamic Kernel Module Support (DKMS) auf Ihrem VDA zu installieren.

- `FFmpeg` wird für die Videodekodierung verwendet.
- `kernel-devel` wird verwendet, um ein virtuelles Webcam-Kernelmodul der entsprechenden Version zu erstellen.
- DKMS wird verwendet, um das virtuelle Webcam-Kernelmodul dynamisch zu verwalten.

> **Hinweis:**
>
> Bei der Installation der vorhergehenden Programme auf RHEL und CentOS installiert und aktiviert das `ctxwcamcfg.sh`-Skript die folgenden Repositorys auf Ihrem VDA:
>
> - Zusätzliche 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 Webcam-Dienst des Linux VDA – `ctxwcamsd` – wird neu gestartet und lädt das Kernelmodul `v4l2loopback` für die HDX-Webcam-Videokomprimierungsfunktion.

3. Wenn Ihr VDA keinen Internetzugang hat, erstellen Sie das v4l2loopback-Kernelmodul auf einem anderen Computer und kopieren Sie es dann auf Ihren VDA.

a. Bereiten Sie einen Build-Computer vor, der Internetzugang hat und dieselbe Kernelversion wie Ihr VDA aufweist. Der Befehl `uname -r` hilft, Kernelversionen zu finden.

b. Auf dem Build-Computer führen Sie den Befehl `sudo mkdir -p /var/xdl` aus.

c. Kopieren Sie `/var/xdl/configure_*` von Ihrem VDA auf den Build-Computer unter `/var/xdl/`.

d. Auf dem Build-Computer führen Sie den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um das Kernelmodul zu erstellen. Wenn der Befehl erfolgreich ausgeführt wird, wird eine Datei v4l2loopback.ko unter dem Pfad `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/` erstellt. Ignorieren Sie Fehler, die beim Ausführen des Skripts ctxwcamcfg.sh auftreten können.

e. Kopieren Sie v4l2loopback.ko vom Build-Computer auf Ihren VDA und legen Sie es unter `/opt/Citrix/VDA/lib64/` ab.

f. Auf Ihrem VDA führen Sie den Befehl `sudo service ctxwcamsd restart` aus, um den Webcam-Dienst neu zu starten und das v4l2loopback-Kernelmodul zu laden.

g. Stellen Sie sicher, dass Sie das FFmpeg-Programm auf Ihrem VDA installieren, bevor Sie die HDX-Webcam-Videokomprimierungsfunktion verwenden können.

Sitzungszuverlässigkeit konfigurieren

Citrix® führt die Funktion zur Sitzungszuverlässigkeit für alle unterstützten Linux-Plattformen ein. Die Sitzungszuverlässigkeit ist standardmäßig aktiviert.

Die Sitzungszuverlässigkeit stellt ICA-Sitzungen bei Netzwerkunterbrechungen nahtlos wieder her. Weitere Informationen zur Sitzungszuverlässigkeit finden Sie unter Automatisches Client-Reconnect und Sitzungszuverlässigkeit.

Hinweis: Daten, die über eine Sitzungszuverlässigkeitsverbindung übertragen werden, liegen standardmäßig im Klartext vor. Aus Sicherheitsgründen empfehlen wir Ihnen, die TLS-Verschlüsselung zu aktivieren. Weitere Informationen zur TLS-Verschlüsselung finden Sie unter Benutzersitzungen mit TLS sichern.

Konfiguration

Richtlinieneinstellungen in Citrix Studio

Sie können die folgenden Richtlinien für die Sitzungszuverlässigkeit in Citrix Studio festlegen:

- Sitzungszuverlässigkeitsverbindungen
- Timeout für Sitzungszuverlässigkeit

- Portnummer für Sitzungszuverlässigkeit
- Transparenzstufe der Benutzeroberfläche für die Wiederverbindung

Weitere Informationen finden Sie unter Richtlinieneinstellungen für die Sitzungszuverlässigkeit und Richtlinieneinstellungen für das automatische Client-Reconnect.

Hinweis: Nachdem Sie die Richtlinie **Sitzungszuverlässigkeitsverbindungen** oder **Sitzungszuverlässigkeits-Portnummer** festgelegt haben, starten Sie den VDA-Dienst und den HDX™-Dienst in dieser Reihenfolge neu, damit Ihre Einstellungen wirksam werden.

Einstellungen auf dem Linux VDA

- **TCP-Listener für Sitzungszuverlässigkeit aktivieren/deaktivieren**

Standardmäßig ist der TCP-Listener für die Sitzungszuverlässigkeit aktiviert und lauscht auf Port 2598. Um den Listener zu deaktivieren, führen Sie den folgenden Befehl aus.

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cg
p"   -v  "fEnableWinStation" -d "0x00000000"
```

Hinweis: Starten Sie den HDX-Dienst neu, damit Ihre Einstellungen wirksam werden. Das Deaktivieren des TCP-Listeners deaktiviert die Sitzungszuverlässigkeit nicht. Die Sitzungszuverlässigkeit ist weiterhin über andere Listener (z. B. SSL) verfügbar, wenn die Funktion über die Richtlinie **Sitzungszuverlässigkeitsverbindungen** aktiviert ist.

- **Sitzungszuverlässigkeits-Portnummer**

Sie können die Sitzungszuverlässigkeits-Portnummer auch mit dem folgenden Befehl festlegen (Portnummer 2599 als Beispiel).

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cg
p"   -v  "PortNumber" -d  "2599"
```

Hinweis: Starten Sie den HDX-Dienst neu, damit Ihre Einstellung wirksam wird. Wenn die Portnummer über die Richtlinieneinstellung in Citrix Studio festgelegt wurde, wird Ihre Einstellung auf dem Linux VDA ignoriert. Stellen Sie sicher, dass die Firewall auf dem VDA so konfiguriert ist, dass sie den Netzwerkverkehr über den festgelegten Port nicht blockiert.

- **Keep-Alive-Intervall Server-zu-Client**

Keep-Alive-Meldungen für die Sitzungszuverlässigkeit werden zwischen dem Linux VDA und dem ICA®-Client gesendet, wenn in der Sitzung keine Aktivität stattfindet (z. B. keine Mausbewegung, keine Bildschirmaktualisierung). Die Keep-Alive-Meldungen werden verwendet, um zu erkennen, ob der Client noch reagiert. Wenn keine Antwort vom Client erfolgt, wird die Sitzung angehalten, bis der Client die Verbindung wiederherstellt. Diese Einstellung gibt die Anzahl der Sekunden zwischen aufeinanderfolgenden Keep-Alive-Meldungen an. Standardmäßig ist diese Einstellung nicht konfiguriert. Um sie zu konfigurieren, führen Sie den folgenden Befehl aus (als Beispiel werden 10 Sekunden verwendet).

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig"  -t "REG_DWORD"  -v
"CgpServerToClientKeepAlive"  -d  "10"  --force
```

- **Keep-Alive-Intervall Client-zu-Server**

Diese Einstellung gibt die Anzahl der Sekunden zwischen aufeinanderfolgenden Keep-Alive-Meldungen an, die vom ICA-Client an den Linux VDA gesendet werden. Standardmäßig ist diese Einstellung nicht konfiguriert. Um sie zu konfigurieren, führen Sie den folgenden Befehl aus (als Beispiel werden 10 Sekunden verwendet).

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig"  -t "REG_DWORD"  -v
"CgpClientToServerKeepAlive"  -d  "10"  --force
```

Problembehandlung

Sitzungen können nach dem Aktivieren der Sitzungszuverlässigkeit über die Richtlinieneinstellung nicht gestartet werden.

Gehen Sie wie folgt vor, um dieses Problem zu umgehen:

1. Stellen Sie sicher, dass der VDA-Dienst und der HDX-Dienst in dieser Reihenfolge neu gestartet werden, nachdem Sie die Sitzungszuverlässigkeit über die Richtlinieneinstellung in Citrix Studio aktiviert haben.
2. Führen Sie auf dem VDA den folgenden Befehl aus, um zu überprüfen, ob der TCP-Listener für die Sitzungszuverlässigkeit ausgeführt wird (als Beispiel wird Port 2598 verwendet).

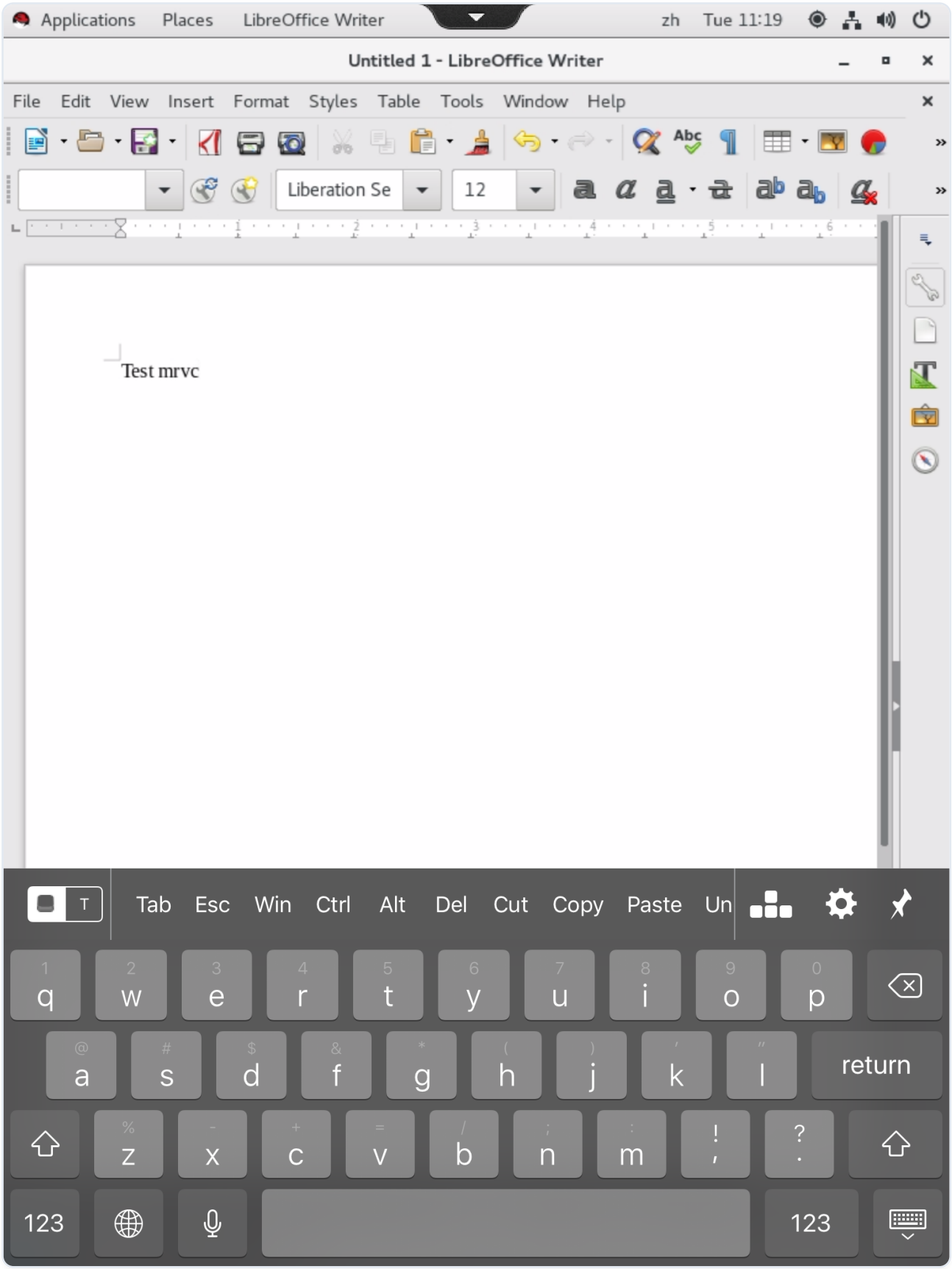
   ```
   netstat -an | grep 2598
   ```

Wenn kein TCP-Listener am Port für die Sitzungszuverlässigkeit vorhanden ist, aktivieren Sie den Listener, indem Sie den folgenden Befehl ausführen.

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations
\cgp"   -v  "fEnableWinStation" -d "0x00000001"
```

Bildschirmtastatur

Die Bildschirmtastaturfunktion ist in einer virtuellen Linux-Desktop- oder Anwendungssitzung verfügbar. Die Bildschirmtastatur wird automatisch ein- oder ausgeblendet, wenn Sie ein Eingabefeld aufrufen oder verlassen.


Applications
Places
LibreOffice Writer
zh
Tue 11:19
Untitled 1 - LibreOffice Writer
File
Edit
View
Insert
Format
Styles
Table
Tools
Window
Help
Liberation Se
12
Test mrvc
Tab
Esc
Win
Ctrl
Alt
Del
Cut
Copy
Paste
Un
return
123
123

Hinweis:

> Die Funktion ist für RHEL 7.8, RHEL 7.9, RHEL 8.1, RHEL 8.2, RHEL 8.3, SUSE 12.5, Ubuntu 16.04, Ubuntu 18.04 und Ubuntu 20.04 verfügbar. Sie wird von der Citrix Workspace-App für iOS und Android unterstützt.

Funktion aktivieren und deaktivieren

Die Funktion ist standardmäßig deaktiviert. Verwenden Sie das Dienstprogramm **ctxreg**, um die Funktion zu aktivieren oder zu deaktivieren. Die Funktionskonfiguration auf einem bestimmten Linux-VDA gilt für alle Sitzungen auf diesem VDA.

So aktivieren Sie die Funktion:

1. Führen Sie den Befehl aus:

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
   "Enabled" -d "0x00000001"
   ```

2. Legen Sie in Citrix Studio die Richtlinie **Automatische Tastaturanzeige** auf **Zulässig** fest.
3. (Optional) Führen Sie für RHEL 7 und CentOS 7 den folgenden Befehl aus, um Intelligent Input Bus (`IBus`) als Standard-IM-Dienst zu konfigurieren:

   ```
   echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
   ```

Um die Funktion zu deaktivieren, führen Sie den Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000000"
```

Hinweis:

> Die vorstehenden Einstellungen werden wirksam, wenn Sie sich bei einer neuen Sitzung anmelden oder sich von der aktuellen Sitzung ab- und wieder anmelden.

Einschränkungen

- Die Funktion funktioniert möglicherweise nicht wie erwartet mit Google Chrome, LibreOffice und anderen Apps.
- Um die Bildschirmtastatur nach dem manuellen Ausblenden wieder anzuzeigen, klicken Sie auf ein Nicht-Eingabefeld und dann erneut auf das aktuelle Eingabefeld.
- Die Bildschirmtastatur wird möglicherweise nicht angezeigt, wenn Sie in einem Webbrowser von einem Eingabefeld zu einem anderen klicken. Um dieses Problem zu umgehen, klicken Sie auf ein Nicht-Eingabefeld und dann auf das Ziel-Eingabefeld.
- Die Funktion unterstützt keine Unicode-Zeichen und Doppelbyte-Zeichen (wie chinesische, japanische und koreanische Zeichen).
- Die Bildschirmtastatur ist für Passworteingabefelder nicht verfügbar.
- Die Bildschirmtastatur kann das aktuelle Eingabefeld überlappen. Verschieben Sie in diesem Fall das App-Fenster oder scrollen Sie auf Ihrem 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, selbst wenn eine physische Tastatur angeschlossen ist.

Client-Eingabemethoden-Editor (IME)

Übersicht

Doppelbyte-Zeichen wie chinesische, japanische und koreanische Zeichen müssen über einen IME eingegeben werden. Geben Sie solche Zeichen mit einem beliebigen IME ein, der mit der Citrix Workspace™-App auf Clientseite kompatibel ist, z. B. dem nativen Windows-CJK-IME.

Installation

Diese Funktion wird automatisch installiert, wenn Sie den Linux VDA installieren.

Verwendung

Öffnen Sie eine Citrix Virtual Apps- oder Citrix Virtual Desktops™-Sitzung wie gewohnt.

Ändern Sie Ihre Eingabemethode nach Bedarf auf Clientseite, um die Client-IME-Funktion zu verwenden.

Bekannte Probleme

- Ein Doppelklick auf eine Zelle in einer Google-Tabelle ist erforderlich, bevor Sie die Client-IME-Funktion verwenden können, um Zeichen in die Zelle einzugeben.
- Die Client-IME-Funktion wird in Kennwortfeldern nicht automatisch deaktiviert.
- Die IME-Benutzeroberfläche folgt dem Cursor im Eingabebereich nicht.

Unterstützung für mehrere Spracheingaben

Ab Linux VDA Version 1.4 hat Citrix Unterstützung für veröffentlichte Anwendungen hinzugefügt. Benutzer können auf eine gewünschte Linux-Anwendung zugreifen, ohne die Linux-Desktop-Umgebung zu benötigen.

Die native Sprachleiste auf dem Linux VDA war jedoch für die veröffentlichte Anwendung nicht verfügbar, da die Sprachleiste stark in die Linux-Desktop-Umgebung integriert ist. Infolgedessen konnten Benutzer keinen Text in einer Sprache eingeben, die IME erfordert, wie z. B. Chinesisch, Japanisch oder Koreanisch. Es war auch nicht möglich, dass Benutzer während einer Anwendungssitzung zwischen Tastaturlayouts wechselten.

Um diese Probleme zu beheben, bietet diese Funktion eine Sprachleiste für veröffentlichte Anwendungen, die Texteingaben akzeptieren. Die Sprachleiste ermöglicht es Benutzern, ein serverseitiges IME auszuwählen und während einer Anwendungssitzung zwischen Tastaturlayouts zu wechseln.

Konfiguration

Sie können das Dienstprogramm **ctxreg** verwenden, um diese Funktion zu aktivieren oder zu deaktivieren (standardmäßig deaktiviert). Die Funktionskonfiguration auf einem bestimmten Linux VDA-Server gilt für alle auf diesem VDA veröffentlichten Anwendungen.

Der Konfigurationsschlüssel ist „HKEY_LOCAL_MACHINE \\SYSTEM\\CurrentControlSet\ \Control\\Citrix\\LanguageBar“ und der Typ ist DWORD.

Um diese Funktion zu aktivieren, führen Sie den Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d
"0x00000001"
```

Um diese Funktion zu deaktivieren, führen Sie den Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d
"0x00000000"
```

Verwendung

Die Verwendung ist unkompliziert.

1. Aktivieren Sie die Funktion.
2. Greifen Sie auf eine veröffentlichte Anwendung zu, die Texteingaben akzeptiert. Eine Sprachleiste erscheint in der Sitzung, neben der Anwendung.
3. Wählen Sie im Dropdown-Menü **Region & Sprache** aus, um die gewünschte Sprache (Eingabequelle) hinzuzufügen.

   Abbildung von Region und Sprache(/en-us/linux-virtual-delivery-agent/2107/media/select-region-language-dialog-box.png)
4. Wählen Sie das IME oder Tastaturlayout aus dem Dropdown-Menü aus.
5. Geben Sie eine Sprache unter Verwendung des ausgewählten IME oder Tastaturlayouts ein.

> **Hinweis:**
>
> - Wenn Sie ein Tastaturlayout in der Sprachleiste auf der VDA-Seite ändern, stellen Sie sicher, dass dasselbe Tastaturlayout auf der Clientseite (auf der die Citrix Workspace™-App ausgeführt wird) verwendet wird.
> - Das Paket **accountsservice** muss auf Version 0.6.37 oder höher aktualisiert werden, bevor Sie Einstellungen im Dialogfeld **Region & Sprache** vornehmen können.

> Abbildung der Auswahl von IME oder Tastaturlayout(/en-us/linux-virtual-delivery-agent/2107/media/region-language-dialog-box.png)

Dynamische Tastaturlayout-Synchronisierung

Bisher mussten die Tastaturlayouts auf dem Linux-VDA und auf dem Clientgerät identisch sein. Wenn sich beispielsweise das Tastaturlayout auf dem Clientgerät von Englisch auf Französisch

änderte, aber nicht auf dem VDA, konnten Zuordnungsprobleme auftreten und bestehen bleiben, bis der VDA ebenfalls auf Französisch umgestellt wurde.

Citrix® behebt das Problem, indem es das Tastaturlayout des VDA automatisch mit dem Tastaturlayout des Clientgeräts synchronisiert. Jedes Mal, wenn sich das Tastaturlayout auf dem Clientgerät ändert, passt sich das Layout auf dem VDA entsprechend an.

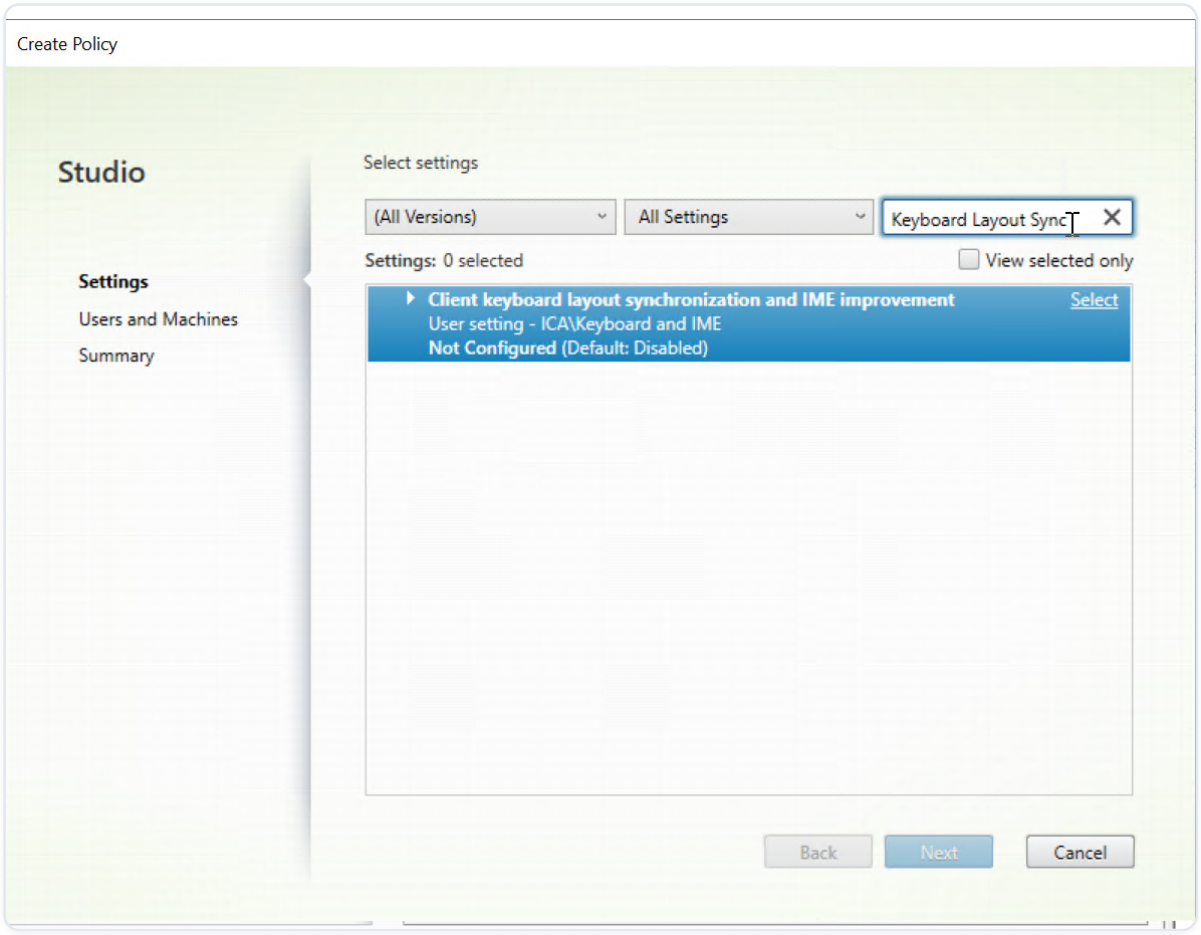
> **Hinweis:**
>
> Die Citrix Workspace™-App für HTML5 unterstützt die Funktion zur dynamischen Tastaturlayoutsynchronisierung nicht.

Konfiguration

Die Funktion zur dynamischen Tastaturlayoutsynchronisierung ist standardmäßig deaktiviert. Um die Funktion zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client Keyboard Layout Sync and IME Improvement** fest oder bearbeiten Sie die Registrierung über das Dienstprogramm `ctxreg`.

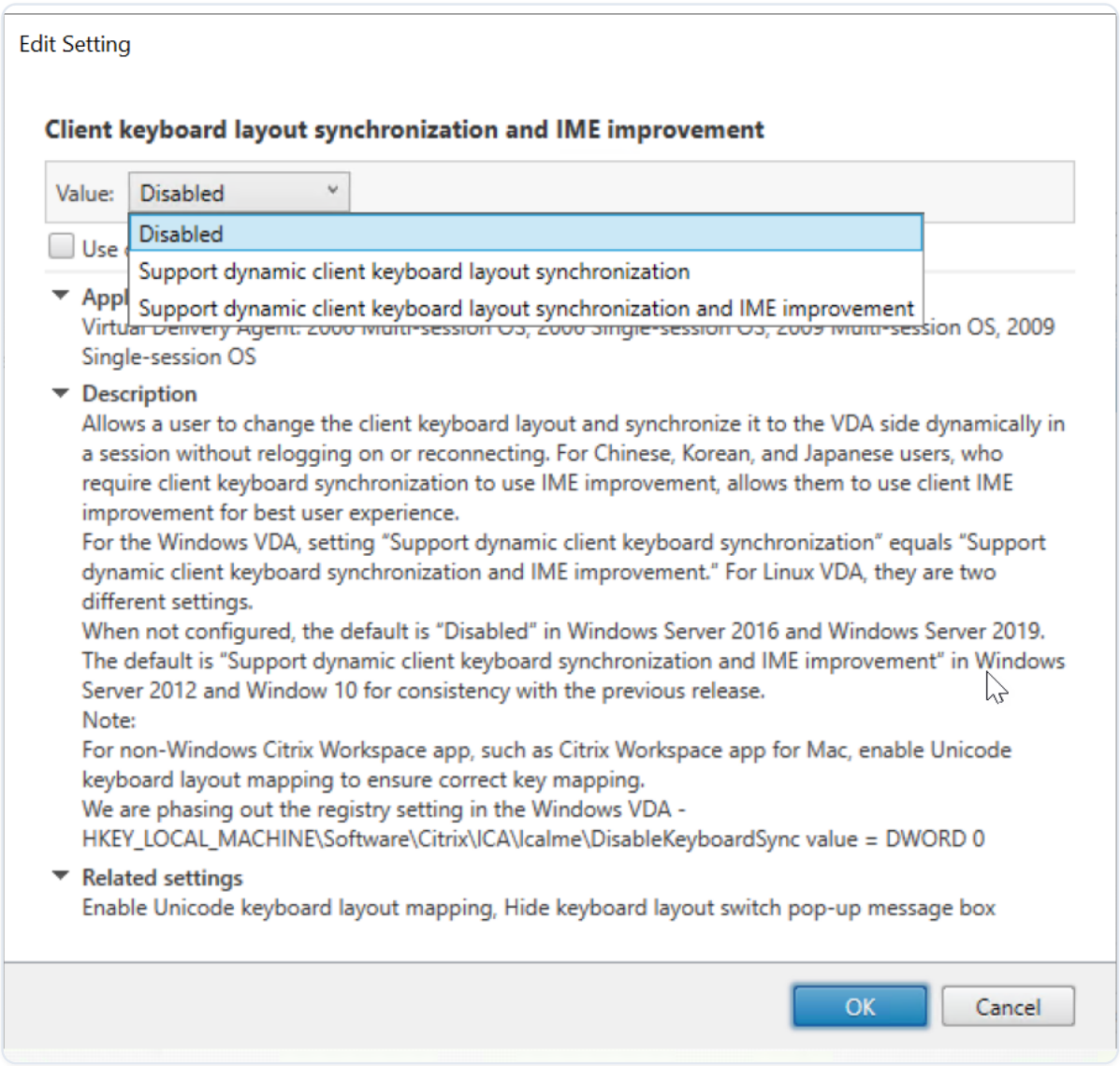
> **Hinweis:**
>
> Die Richtlinie **Client Keyboard Layout Sync and IME Improvement** hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Maschinenobjekte oder alle Objekte in Ihrer Site angewendet werden. Registrierungseinstellungen auf einem bestimmten Linux-VDA gelten für alle Sitzungen auf diesem VDA.

- Legen Sie die Richtlinie **Client Keyboard Layout Sync and IME Improvement** fest, um die Funktion zur dynamischen Tastaturlayoutsynchronisierung zu aktivieren oder zu deaktivieren:
  a. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.
  b. Suchen Sie nach der Richtlinie **Client Keyboard Layout Sync and IME Improvement**.



c. Klicken Sie neben dem Richtliniennamen auf **Auswählen**.

d. 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`.
- **Unterstützung der dynamischen Synchronisierung des Client-Tastaturlayouts und IME-Verbesserung**: Ermöglicht sowohl die dynamische Synchronisierung des Tastaturlayouts 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 mit dem Dienstprogramm `ctxreg`, um die dynamische Tastaturlayout-Synchronisierungsfunktion zu aktivieren oder zu deaktivieren:

  Um diese Funktion zu aktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncKeyboardLayout" -d "0x00000001"
  ```

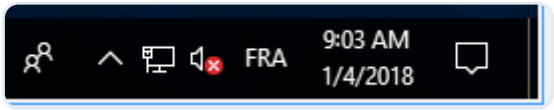
  Um diese Funktion zu deaktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncKeyboardLayout" -d "0x00000000"
  ```

Verwendung

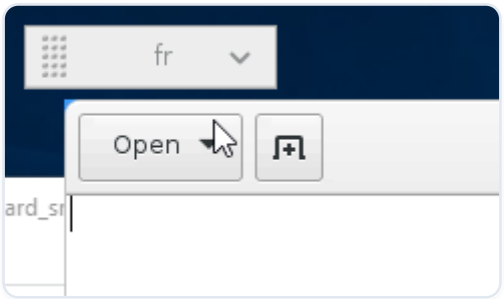
Wenn diese Funktion aktiviert ist, ändert sich das Tastaturlayout der Sitzung entsprechend, wenn sich das Tastaturlayout auf dem Clientgerät während einer Sitzung ändert.

Wenn Sie beispielsweise das Tastaturlayout auf einem Clientgerät auf Französisch (FR) ändern:



Dann ändert sich das Tastaturlayout der Linux VDA-Sitzung ebenfalls auf „fr“.

In einer Anwendungssitzung können Sie diese automatische Änderung sehen, wenn Sie die Sprachleiste aktiviert haben:



In einer Desktopsitzung können Sie diese automatische Änderung in der Taskleiste sehen:



Client-IME-Benutzeroberflächensynchronisierung

Übersicht

Bisher wurde die Client-IME-Benutzeroberfläche (einschließlich des Kompositionsfensters und des Kandidatenfensters) in der oberen linken Ecke des Bildschirms positioniert. Sie folgte dem Cursor nicht und befand sich manchmal weit vom Cursor entfernt im Texteingabebereich:

Abbildung der vorherigen Client-IME-Benutzeroberfläche(/en-us/linux-virtual-delivery-agent/2107/media/composition-and-candidate-windows.png)

Citrix® verbessert die Benutzerfreundlichkeit und optimiert die Benutzererfahrung mit dem Client-IME wie folgt:

Abbildung der aktuellen Client-IME-Benutzeroberfläche(/en-us/linux-virtual-delivery-agent/2107/media/synced-composition-and-candidate-windows.png)

> **Hinweis:**

> Die Funktion ist verfügbar für RHEL 7.x, CentOS 7.x, Ubuntu 16.04, Ubuntu 18.04 und SUSE 12.x. Sie wird von der Citrix Workspace-App für Windows und für Mac unterstützt.

> Um die Funktion in RHEL 7.x Desktopsitzungen zu verwenden, müssen Sie `IBus` aktivieren. Stellen Sie zum Beispiel die Benutzeroberflächensprache auf eine Sprache ein, die eine IME-Eingabe erfordert, oder fügen Sie **GTK_IM_MODULE=ibus** zur Datei **${HOME}/.config/imsettings/xinputrc** hinzu.

> Die Funktion wird automatisch installiert, aber Sie müssen sie aktivieren, bevor Sie sie verwenden können.

Aktivieren und Deaktivieren der Funktion

Die Client-IME-Benutzeroberflächensynchronisierungsfunktion ist standardmäßig deaktiviert. Um die Funktion zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client Keyboard Layout Sync and IME Improvement** fest oder bearbeiten Sie die Registrierung über das `ctxreg` Dienstprogramm.

> **Hinweis:**

> Die Richtlinie **Client Keyboard Layout Sync and IME Improvement** 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 Keyboard Layout Sync and IME Improvement** fest, um die Client-IME-Benutzeroberflächensynchronisierungsfunktion zu aktivieren oder zu deaktivieren:

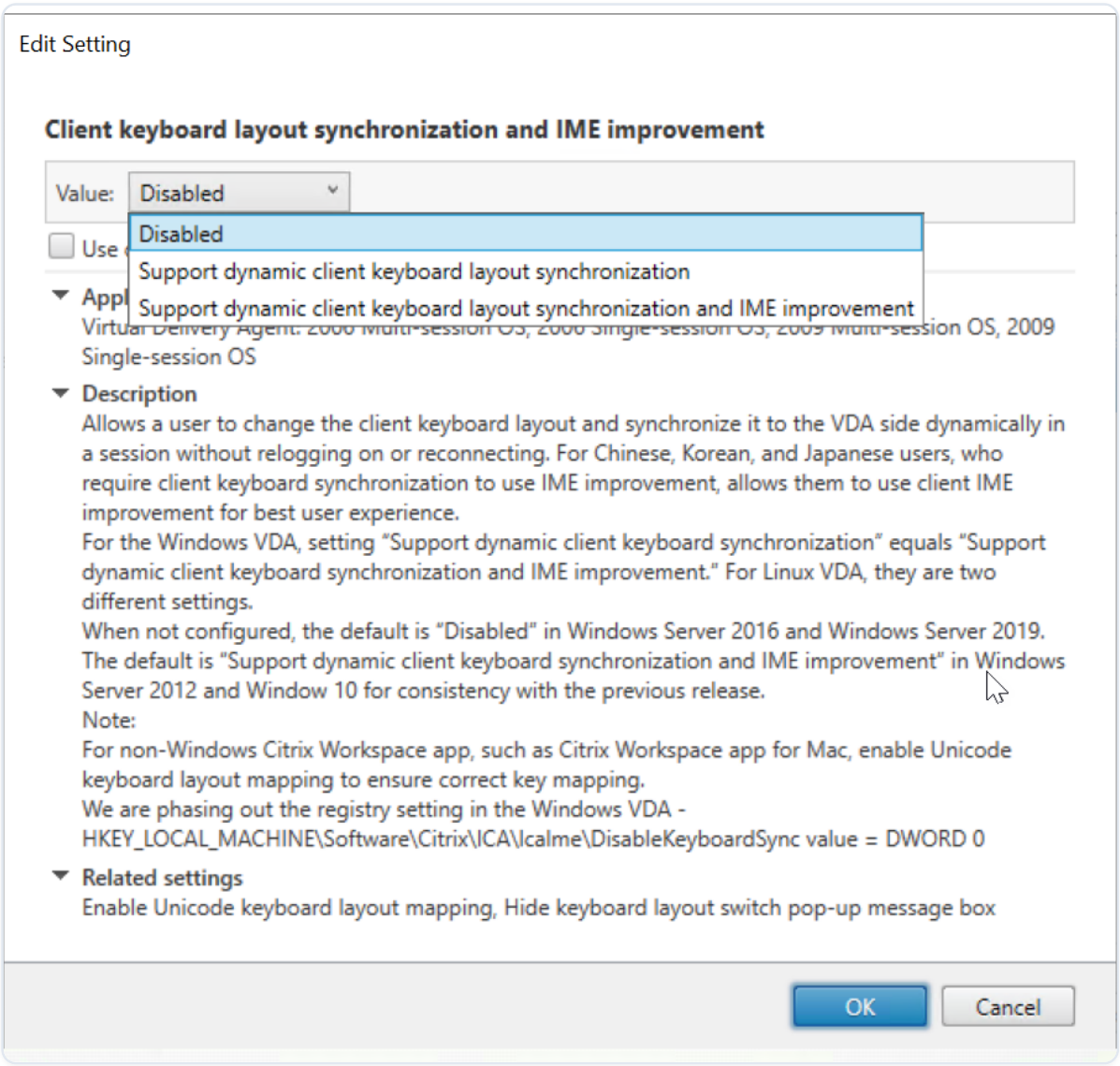
  a. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.

  b. Suchen Sie nach der Richtlinie **Client Keyboard Layout Sync and IME Improvement**.

     Abbildung der Richtlinie zur Client-Tastaturlayout-Synchronisierung und IME-Verbesserung(/en-us/linux-virtual-delivery-agent/2107/media/client-keyboard-and-ime-policy.png)

  c. Klicken Sie auf **Auswählen** neben dem Richtliniennamen.

  d. Legen Sie die Richtlinie fest.



Es stehen drei Optionen zur Verfügung:

- **Deaktiviert**: Deaktiviert die dynamische Tastaturlayoutsynchronisierung und die Synchronisierung der Client-IME-Benutzeroberfläche.
- **Unterstützung der dynamischen Clients-Tastaturlayoutsynchronisierung**: Aktiviert die dynamische Tastaturlayoutsynchronisierung, unabhängig vom DWORD-Wert des Registrierungsschlüssels **SyncKeyboardLayout** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
- **Unterstützung der dynamischen Clients-Tastaturlayoutsynchronisierung und IME-Verbesserung**: 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 Dienstprogramm `ctxreg`, um die Funktion zur Synchronisierung der Client-IME-Benutzeroberfläche zu aktivieren oder zu deaktivieren:

  Um die Funktion zu aktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v  "SyncClientIME" -d "0x00000001"
  ```

  Um die Funktion zu deaktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncClientIME" -d "0x00000000"
  ```

HDX™ Insight

Übersicht

Der Linux VDA unterstützt die HDX Insight-Funktion teilweise. HDX Insight ist Teil von Citrix Application Delivery Management (ADM) und basiert auf dem beliebten Industriestandard AppFlow. Es ermöglicht der IT, eine außergewöhnliche Benutzererfahrung zu bieten, indem es eine beispiellose End-to-End-Transparenz des Citrix ICA-Datenverkehrs bietet, der über das Citrix ADC- oder Citrix SD-WAN-Anwendungsnetzwerk fließt. Weitere Informationen finden Sie unter HDX Insight

Installation

Es müssen keine abhängigen Pakete installiert werden.

Verwendung

HDX Insight analysiert die ICA®-Nachrichten, die über den Citrix ADC zwischen der Citrix Workspace™-App und dem Linux VDA übertragen werden. Alle HDX Insight-Daten stammen vom virtuellen NSAP-Kanal und werden unkomprimiert gesendet. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert.

Die folgenden Befehle deaktivieren bzw. aktivieren den virtuellen NSAP-Kanal:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000000" --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000001" --force
```

Problembehandlung

Es werden keine Datenpunkte angezeigt

Es kann zwei Ursachen geben:

- HDX Insight ist nicht korrekt konfiguriert.

  Beispielsweise ist AppFlow® auf dem Citrix ADC nicht aktiviert oder eine falsche Citrix ADC-Instanz ist auf dem Citrix ADM konfiguriert.

- Der virtuelle ICA-Steuerungskanal ist auf dem Linux VDA nicht gestartet.

  `ps aux | grep -i ctxctl`

  Wenn `ctxctl` nicht ausgeführt wird, wenden Sie sich an Ihren Administrator, um einen Fehler an Citrix zu melden.

Es werden keine Anwendungsdatenpunkte angezeigt

Stellen Sie sicher, dass der nahtlose virtuelle Kanal aktiviert ist und eine nahtlose Anwendung für eine Weile gestartet wurde.

Rendezvous-Protokoll

In Umgebungen, die den Citrix Gateway-Dienst verwenden, ermöglicht das Rendezvous-Protokoll HDX-Sitzungen, den Citrix Cloud Connector™ zu umgehen und sich direkt und sicher mit dem Citrix Gateway-Dienst zu verbinden.

Anforderungen:

- Zugriff auf die Umgebung unter Verwendung von Citrix Workspace™ und dem Citrix Gateway-Dienst.
- Steuerungsebene: Citrix Virtual Apps and Desktops™ Service (Citrix Cloud).

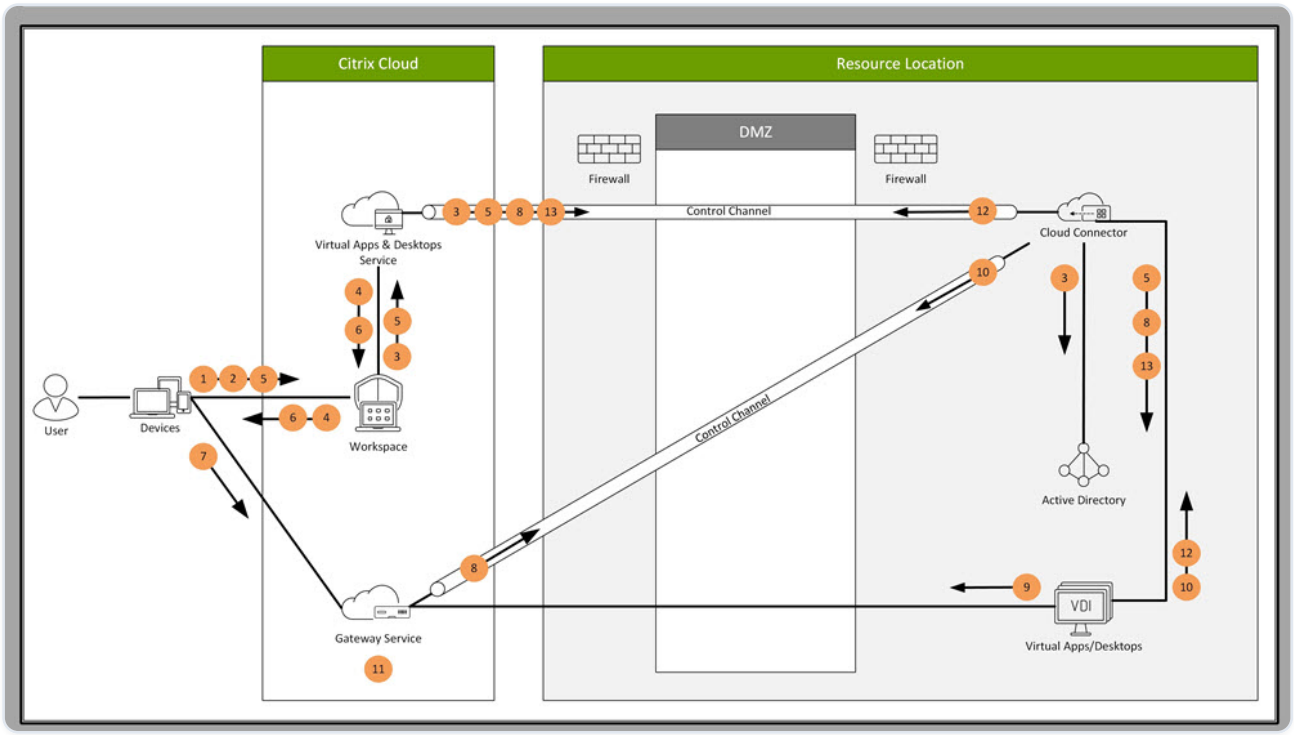
- Linux VDA Version 2012 oder höher.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix-Richtlinie. Weitere Informationen finden Sie unter Rendezvous-Protokoll-Richtlinieneinstellung.
- Die VDAs müssen Zugriff auf `https://*.nssvc.net` haben, einschließlich aller Subdomains. Wenn Sie nicht alle Subdomains auf diese Weise auf die Whitelist setzen können, verwenden Sie stattdessen `https://*.c.nssvc.net` und `https://*.g.nssvc.net`. Weitere Informationen finden Sie im Abschnitt Internet Connectivity Requirements der Citrix Cloud-Dokumentation (unter Virtual Apps and Desktop Service) und im Knowledge Center-Artikel CTX270584.
- Cloud Connectors müssen die FQDNs der VDAs abrufen, wenn sie eine Sitzung vermitteln. Um dies zu erreichen, aktivieren Sie die DNS-Auflösung für die Site: Verwenden Sie das Citrix Virtual Apps and Desktops Remote PowerShell SDK und führen Sie den Befehl `Set-BrokerSite -DnsResolutionEnabled $true` aus. Weitere Informationen zum Citrix Virtual Apps and Desktops Remote PowerShell SDK finden Sie unter SDKs und APIs.

> **Wichtig:**
>
> Das Rendezvous-Protokoll unterstützt keine transparenten oder expliziten Proxys. Um Proxys zu verwenden, nutzen Sie weiterhin den Cloud Connector für den ICA®-Datenverkehr.
>
> Wenn Sie Rendezvous aktivieren und der VDA den Citrix Gateway-Dienst nicht direkt erreichen kann, fällt der VDA auf die Proxy-Verbindung der HDX™-Sitzung über den Cloud Connector zurück.

Wenn Sie alle Anforderungen erfüllen, führen Sie die folgenden Schritte aus, um zu überprüfen, ob Rendezvous verwendet wird:

1. Starten Sie ein Terminal auf dem VDA.
2. Führen Sie `su root -c "/opt/Citrix/VDA/bin/ctxquery -f iuStdP"` aus.
3. Die TRANSPORT PROTOCOLS geben den Verbindungstyp an:
   - TCP Rendezvous: TCP - SSL - CGP - ICA
   - EDT Rendezvous: UDP - DTLS - CGP - ICA
   - Proxy über Cloud Connector: TCP - CGP - ICA

Dieses Diagramm bietet einen Überblick über den Rendezvous-Verbindungsfluss. Befolgen Sie die Schritte, um den Ablauf zu verstehen.



1. Navigieren Sie zu Citrix Workspace.
2. Geben Sie die Anmeldeinformationen in Citrix Workspace ein.
3. Bei Verwendung eines lokalen Active Directory authentifiziert der Citrix Virtual Apps™ and Desktops-Dienst die Anmeldeinformationen mit Active Directory über den Cloud Connector-Kanal.
4. Citrix Workspace zeigt die aufgelisteten Ressourcen vom Citrix Virtual Apps and Desktops-Dienst an.
5. Wählen Sie Ressourcen in Citrix Workspace aus. Der Citrix Virtual Apps and Desktops-Dienst sendet eine Nachricht an den VDA, um sich auf eine eingehende Sitzung vorzubereiten.
6. Citrix Workspace sendet eine ICA-Datei an den Endpunkt, die ein von Citrix Cloud generiertes STA-Ticket enthält.
7. Der Endpunkt stellt eine Verbindung zum Citrix Gateway-Dienst her, stellt das Ticket für die Verbindung zum VDA bereit, und Citrix Cloud validiert das Ticket.
8. Der Citrix Gateway-Dienst sendet Verbindungsinformationen an den Cloud Connector. Der Cloud Connector ermittelt, ob die Verbindung eine Rendezvous-Verbindung sein soll, und sendet die Informationen an den VDA.
9. Der VDA stellt eine direkte Verbindung zum Citrix Gateway-Dienst her.

10. Wenn eine direkte Verbindung zwischen dem VDA und dem Citrix Gateway-Dienst nicht möglich ist, leitet der VDA seine Verbindung über den Cloud Connector weiter.
11. Der Citrix Gateway-Dienst stellt eine Verbindung zwischen dem Endpunktgerät und dem VDA her.
12. Der VDA überprüft seine Lizenz mit dem Citrix Virtual Apps and Desktops-Dienst über den Cloud Connector.
13. Der Citrix Virtual Apps and Desktops-Dienst sendet Sitzungsrichtlinien über den Cloud Connector an den VDA. Diese Richtlinien werden angewendet.

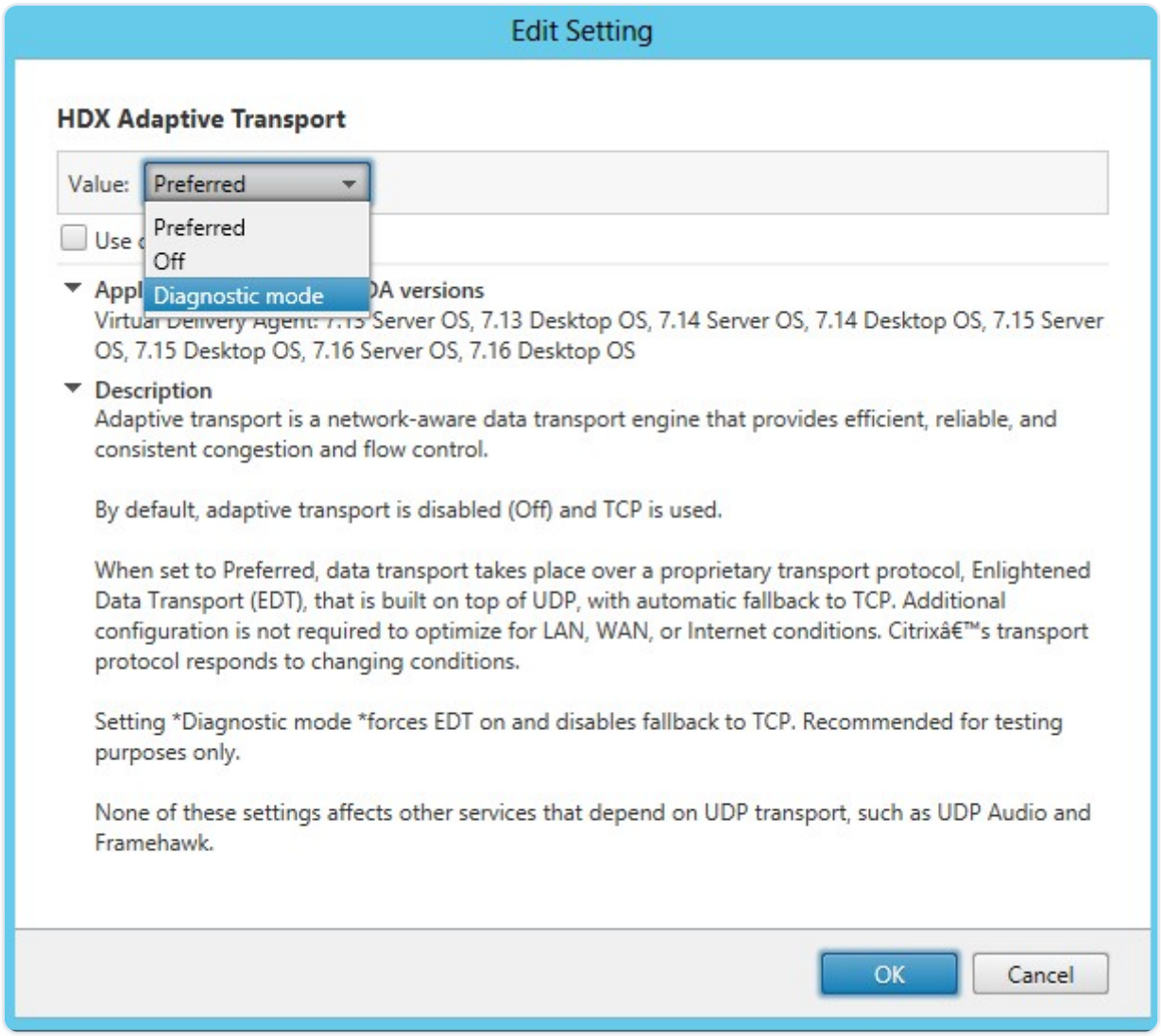
Adaptiver Transport

Adaptiver Transport ist ein Datentransportmechanismus für Citrix Virtual Apps and Desktops. Er ist schneller, skalierbarer, verbessert die Anwendungsinteraktivität und ist interaktiver bei anspruchsvollen WAN- und Internetverbindungen über große Entfernungen. Weitere Informationen zum adaptiven Transport finden Sie unter Adaptiver Transport.

Adaptiven Transport aktivieren

Stellen Sie in Citrix Studio sicher, dass die Richtlinie **HDX™ Adaptive Transport** auf **Bevorzugt** oder **Diagnosemodus** eingestellt ist. **Bevorzugt** ist standardmäßig ausgewählt.

- **Bevorzugt**: Adaptiver Transport über Enlightened Data Transport (EDT) wird nach Möglichkeit verwendet, mit Fallback auf TCP.
- **Diagnose Modus**: EDT wird erzwungen und der Fallback auf TCP ist deaktiviert.



Adaptiven Transport deaktivieren

Um den adaptiven Transport zu deaktivieren, setzen Sie die Richtlinie **HDX Adaptive Transport** in Citrix Studio auf **Aus**.

Überprüfen, ob adaptiver Transport aktiviert ist

Um zu überprüfen, ob UDP-Listener ausgeführt werden, führen Sie den folgenden Befehl aus.

```
netstat -an | grep "1494\|2598"
```

Unter normalen Umständen ist die Ausgabe ähnlich der folgenden.

```
udp        0      0 0.0.0.0:2598            0.0.0.0:*
```

```
udp        0      0 :::1494                 :::*
```

EDT MTU-Erkennung

EDT ermittelt automatisch die Maximum Transmission Unit (MTU) beim Aufbau einer Sitzung. Dadurch wird eine EDT-Paketfragmentierung verhindert, die zu einer Leistungsverschlechterung oder einem Fehler beim Aufbau einer Sitzung führen könnte.

Mindestanforderungen:

- Linux VDA 2012
- Citrix Workspace™ App 1911 für Windows
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- Sitzungszuverlässigkeit muss aktiviert sein

Wenn Sie Clientplattformen oder -versionen verwenden, die diese Funktion nicht unterstützen, siehe Knowledge Center-Artikel CTX231821 für Details zur Konfiguration einer benutzerdefinierten EDT-MTU, die für Ihre Umgebung geeignet ist.

WARNUNG:

Eine falsche Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen, die möglicherweise eine Neuinstallation Ihres Betriebssystems erfordern. Citrix kann nicht garantieren, dass Probleme, die aus der falschen Verwendung des Registrierungs-Editors resultieren, gelöst werden können. Verwenden Sie den Registrierungs-Editor auf eigenes Risiko. Sichern Sie die Registrierung unbedingt, bevor Sie sie bearbeiten.

EDT MTU-Erkennung auf dem VDA aktivieren oder deaktivieren

Die EDT MTU-Erkennung ist standardmäßig deaktiviert.

- Um die EDT MTU-Erkennung zu aktivieren, legen Sie den Registrierungsschlüssel `MtuDiscovery` mit dem folgenden Befehl fest, starten Sie den VDA neu und warten Sie, bis sich der VDA registriert hat:

`/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd" -t "REG_DWORD" -v "MtuDiscovery" -d "0x00000001" --force`

- Um die EDT MTU-Erkennung zu deaktivieren, löschen Sie den Registrierungswert `MtuDiscovery`.

Diese Einstellung gilt maschinenweit und betrifft alle Sitzungen, die von einem unterstützten Client aus verbunden werden.

EDT MTU-Erkennung auf dem Client steuern

Sie können die EDT MTU-Erkennung selektiv auf dem Client steuern, indem Sie den Parameter `MtuDiscovery` in der ICA®-Datei hinzufügen. Um die Funktion zu deaktivieren, legen Sie Folgendes im Abschnitt `Application` fest:

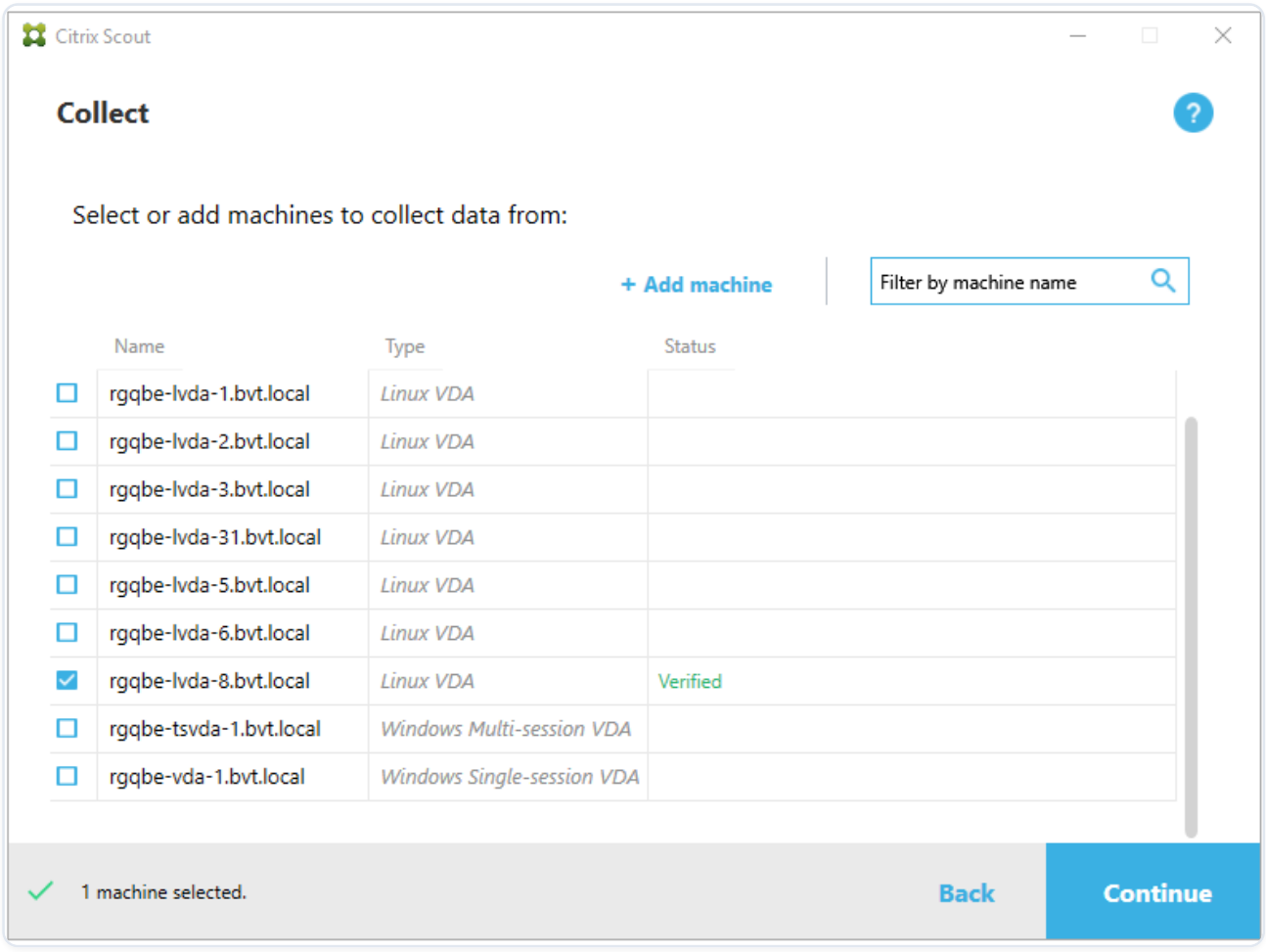
`MtuDiscovery=Off`

Um die Funktion wieder zu aktivieren, entfernen Sie den Parameter `MtuDiscovery` aus der ICA-Datei.

> **WICHTIG:**
>
> Damit dieser ICA-Dateiparameter funktioniert, aktivieren Sie die EDT MTU-Erkennung auf dem VDA. Wenn die EDT MTU-Erkennung auf dem VDA nicht aktiviert ist, hat der ICA-Dateiparameter keine Auswirkung.

Integration mit dem Citrix Telemetry Service

Wenn der Citrix Telemetry Service (ctxtelemetry) in die Linux VDA-Software integriert ist, können Sie Citrix Scout ausführen, das dann das Skript /opt/Citrix/VDA/bin/xdlcollect.sh verwendet, um Protokolle über den Linux VDA zu sammeln.



Hinweis:

Nach dem Upgrade von Linux VDA 1912 und früheren Versionen müssen Sie /opt/Citrix/VDA/sbin/ctxsetup.sh erneut ausführen, um die Variablen für den Citrix Telemetry Service (ctxtelemetry) zu konfigurieren. Weitere Informationen zu den Variablen finden Sie unter Einfache Installation.

Citrix Telemetry Service aktivieren und deaktivieren

- 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 Telemetry Service (ctxtelemetry) verwendet standardmäßig den TCP/IP-Port 7503, um auf Citrix Scout zu lauschen. Er verwendet den TCP/IP-Port 7502 auf dem Delivery Controller, um mit Citrix Scout zu kommunizieren.

Sie können die Standardports verwenden oder die Ports während der Installation des Linux VDA über die folgenden Variablen ändern.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Lauschen auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT** – Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

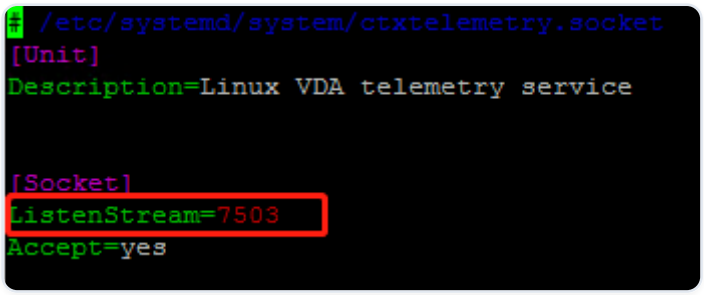
Um Ports nach der Installation Ihres VDA zu ändern, gehen Sie wie folgt vor:

1. Um einen Port für die Kommunikation mit Scout zu ändern, führen Sie den folgenden Befehl aus.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\Software\Citrix\VirtualDesktopAgent" -v "TelemetryServicePort" -d
   <port number> -t REG_DWORD
   ```

2. Um den Socket-Port zum Lauschen auf Scout zu ändern, führen Sie den folgenden Befehl aus, um die Datei ctxtelemetry.socket zu öffnen und zu bearbeiten.

   ```
   sudo vi /etc/systemd/system/ctxtelemetry.socket
   ```

3. Führen Sie die folgenden Befehle aus, um den Socket-Port neu zu starten.

   ```
   sudo systemctl daemon-reload

   sudo systemctl stop ctxtelemetry.socket

   sudo systemctl start ctxtelemetry.socket
   ```

4. Aktivieren Sie die neuen Ports in Ihrer Firewall-Konfiguration.

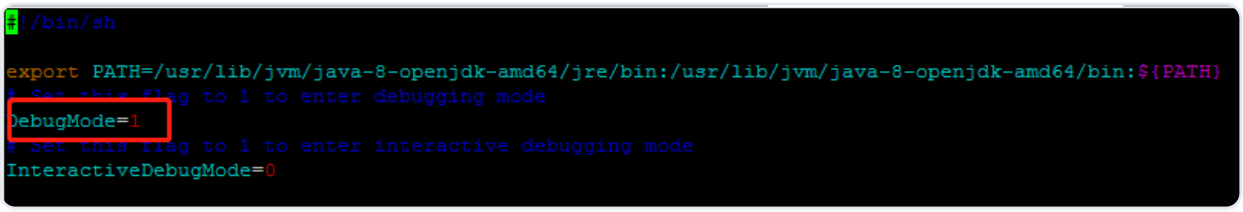
   Wenn Sie beispielsweise eine Ubuntu-Distribution verwenden, führen Sie den Befehl **sudo ufw allow 7503** aus, um Port 7503 zu aktivieren.

Debug-Modus

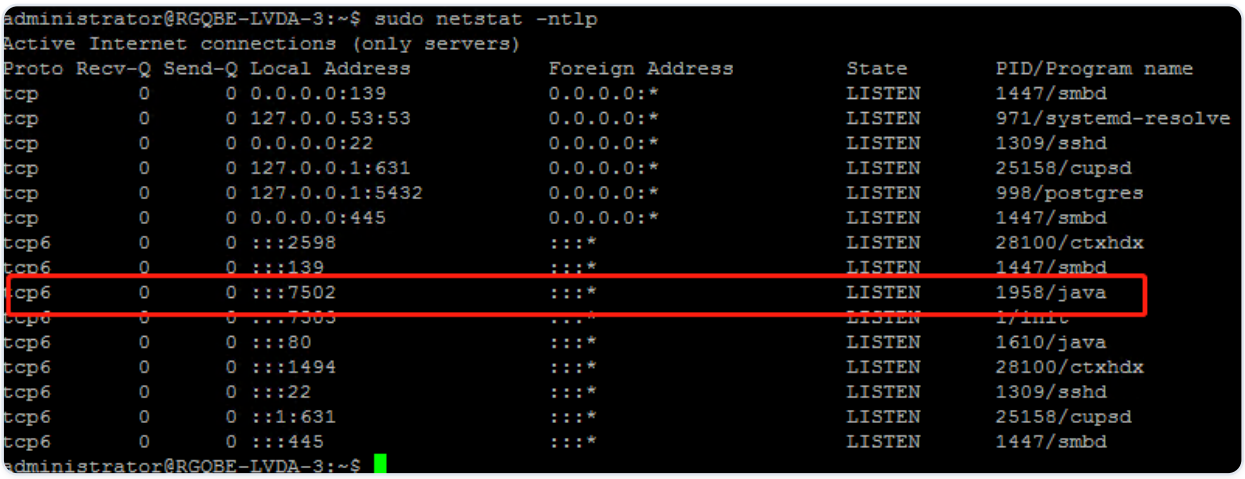
Wenn der Citrix Telemetry Service nicht wie erwartet funktioniert, können Sie den Debug-Modus aktivieren, um die Ursachen zu ermitteln.

1. Um den Debug-Modus zu aktivieren, führen Sie den folgenden Befehl aus, um die Datei ctxtelemetry zu öffnen und anschließend den Wert von DebugMode auf 1 zu ändern.

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
```



2. Stoppen Sie den Citrix Telemetry Service manuell, oder warten Sie 15 Minuten, bis der Dienst automatisch stoppt.



In diesem Beispiel können Sie die folgenden Befehle ausführen, um den Citrix Telemetry Service zu stoppen.

```
sudo netstat -ntlp

Kill -9 1958
```

3. Um den Citrix Telemetry Service neu zu starten, wählen Sie Ihr Linux VDA in Scout aus und suchen Sie telemetry-debug.log unter /var/log/xdl/.

Dienstwartezeit

Der `systemd`-Daemon, der den Socket-Port öffnet, startet standardmäßig und verbraucht nur wenige Ressourcen. Der Citrix Telemetry Service stoppt standardmäßig und startet nur, wenn eine Protokollsammlungsanforderung vom Delivery Controller vorliegt. Nach Abschluss der Protokollsammlung wartet der Dienst 15 Minuten lang auf neue Sammlungsanforderungen und stoppt erneut, wenn keine vorhanden sind. Sie können die Wartezeit mit dem folgenden Befehl konfigurieren. Der Mindestwert beträgt 10 Minuten. Wenn Sie einen Wert unter 10 Minuten festlegen, wird der Mindestwert von 10 Minuten wirksam. Nachdem Sie die Wartezeit festgelegt haben, stoppen und starten Sie den Dienst neu.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v
"TelemetryServiceIdleTimeoutInMinutes" -d <number> -t REG_DWORD
```

Überprüfungstests

Bevor eine Sammlung beginnt, werden für jede ausgewählte Maschine automatisch Überprüfungstests ausgeführt. Diese Tests stellen sicher, dass die Anforderungen erfüllt werden. Wenn ein Test für eine Maschine fehlschlägt, zeigt Scout eine Meldung mit vorgeschlagenen Korrekturmaßnahmen an. Weitere Informationen zu Überprüfungstests finden Sie im Abschnitt Überprüfungstests in der Citrix Scout-Dokumentation.

Tracing aktivieren

Übersicht

Das Sammeln von Protokollen und das Reproduzieren von Problemen verlangsamen die Diagnose und beeinträchtigen die Benutzerfreundlichkeit. Die Funktion „Tracing aktivieren“ erleichtert solche Bemühungen. Tracing ist für den Linux VDA standardmäßig aktiviert.

Konfiguration

Der `ctxlogd`-Daemon und das `setlog`-Dienstprogramm sind jetzt im Linux VDA-Releasepaket enthalten. Standardmäßig startet der `ctxlogd`-Daemon, nachdem Sie den Linux VDA installiert und konfiguriert haben.

ctxlogd-Daemon

Alle anderen Dienste, die verfolgt werden, hängen vom `ctxlogd`-Daemon ab. Sie können den `ctxlogd`-Daemon stoppen, wenn Sie den Linux VDA nicht verfolgt lassen möchten.

setlog-Dienstprogramm

Tracing aktivieren wird mit dem `setlog`-Dienstprogramm konfiguriert, das sich unter dem Pfad **/opt/Citrix/VDA/bin/** befindet. Nur der Root-Benutzer hat die Berechtigung, es auszuführen. Sie können die GUI verwenden oder Befehle ausführen, um die Konfigurationen anzuzeigen und zu ändern. Führen Sie den folgenden Befehl aus, um Hilfe zum `setlog`-Dienstprogramm zu erhalten:

```
setlog help
```

Werte

Standardmäßig ist der **Protokollausgabepfad** auf **/var/log/xdl/hdx.log** festgelegt, die **maximale Protokollgröße** ist auf 200 MB festgelegt, und Sie können bis zu zwei alte Protokolldateien unter dem **Protokollausgabepfad** speichern.

Zeigen Sie die aktuellen `setlog`-Werte an:

```
setlog values



log_path (Log Output Path) = /var/log/xdl/hdx.log



log_size (Max Log Size (MiB)) = 200



log_count (Max Old Log Files) = 2
```

Einen einzelnen `setlog`-Wert anzeigen oder festlegen:

```
setlog value <name> [<value>]
```

Zum Beispiel:

```
setlog value log_size 100
```

Ebenen

Standardmäßig sind die Protokollebenen auf **warning** (Groß-/Kleinschreibung wird nicht beachtet) festgelegt.

Um die für verschiedene Komponenten festgelegten Protokollebenen anzuzeigen, führen Sie den folgenden Befehl aus:

```
setlog levels
```

Um Protokollebenen festzulegen (einschließlich Deaktiviert, Geerbt, Ausführlich, Informationen, Warnungen, Fehler und Schwerwiegende Fehler), führen Sie den folgenden Befehl aus:

```
setlog level <class> [<level>]
```

PROTOKOLLSTUFE	BEFEHLSPARAMETER (GROSS-/KLEINSCHREIBUNG WIRD NICHT BEACHTET)
Deaktiviert	keine
Geerbt	erben
Ausführlich	ausführlich
Informationen	Info
Warnungen	Warnung
Fehler	Fehler
Schwerwiegende Fehler	Fatal

Die Variable `<class>` gibt eine Komponente des Linux VDA an. Um alle Komponenten abzudecken, setzen Sie sie auf all. Zum Beispiel:

```
setlog level all error
```

Flags

Standardmäßig sind die Flags wie folgt eingestellt:

```
setlog flags



DATE = true



TIME = true



NAME = true



PID = true



TID = false



SID = true



UID = false



GID = false



CLASS = false
```

```
LEVEL = false

FUNC = true

FILE = false
```

Aktuelle Flags anzeigen:

```
setlog flags
```

Ein einzelnes Protokoll-Flag anzeigen oder festlegen:

```
setlog flag <flag> [<state>]
```

Standardeinstellungen wiederherstellen

Alle Ebenen, Flags und Werte auf die Standardeinstellungen zurücksetzen:

```
setlog default
```

Wichtig:

Der `ctxlogd`-Dienst wird über die Datei **/var/xdl/.ctxlog** konfiguriert, die nur Root-Benutzer erstellen können. Andere Benutzer haben keine Schreibberechtigung für diese Datei. Wir empfehlen, dass Root-Benutzer anderen Benutzern keine Schreibberechtigung erteilen. Die Nichteinhaltung kann dazu führen, dass die beliebige oder bösartige Konfiguration `ctxlogd` wird, was die Serverleistung und damit die Benutzererfahrung beeinträchtigen kann.

Problembehandlung

Der `ctxlogd`-Daemon schlägt fehl, und Sie können den `ctxlogd`-Dienst nicht neu starten, wenn die Datei **/var/xdl/.ctxlog** fehlt (z. B. versehentlich gelöscht wurde).

/var/log/messages:

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
configuration file.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited,
code=exited, status=1/FAILURE



Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
```

Um dieses Problem zu beheben, führen Sie `setlog` als Root-Benutzer aus, um die Datei **/var/xdl/.ctxlog** neu zu erstellen. Starten Sie anschließend den `ctxlogd`-Dienst neu, von dem andere Dienste abhängen.

Sitzungen überwachen

Die Sitzungsüberwachungsfunktion ermöglicht Domänenadministratoren, die ICA-Sitzungen von Benutzern in einem Intranet anzuzeigen. Die Funktion verwendet noVNC, um eine Verbindung zu den ICA-Sitzungen herzustellen, und wird nur mit RHEL 7.x und Ubuntu 16.04 unterstützt.

> **Hinweis:**

> Um die Sitzungsüberwachungsfunktion zu verwenden, muss die Version von Citrix Director 7.16 oder höher sein.

Installation und Konfiguration

Abhängigkeiten

Für die Sitzungsüberwachung sind zwei neue Abhängigkeiten, `python-websockify` und `x11vnc`, erforderlich. Die Abhängigkeiten `python-websockify` und `x11vnc` werden automatisch installiert, wenn Sie den Linux VDA unter Ubuntu 16.04 installieren. Unter RHEL 7.x müssen Sie `python-websockify` und `x11vnc` nach der Installation des Linux VDA manuell installieren.

Führen Sie den folgenden Befehl unter RHEL 7.x aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren.

```
sudo yum install -y python-websockify x11vnc
```

Um `python-websockify` und `x11vnc` aufzulösen, aktivieren Sie die folgenden Repositorys unter RHEL 7.x:

- Zusätzliche Pakete für Enterprise Linux (EPEL)

  Das EPEL-Repository ist sowohl für `python-websockify` als auch für `x11vnc` erforderlich. Führen Sie den folgenden Befehl aus, um das EPEL-Repository zu aktivieren:

  ```
  sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-$(rpm -E '%{rhel}').noarch.rpm
  ```

- Optionale RPMs

  Führen Sie einen der folgenden Befehle aus, um das Repository für optionale RPMs zu aktivieren, um einige Abhängigkeitspakete von `x11vnc` zu installieren:

  Für Workstation:

  ```
  subscription-manager repos --enable=rhel-7-workstation-optional-rpms
  ```

  Für Server:

  ```
  subscription-manager repos --enable=rhel-7-server-optional-rpms
  ```

Port

Die Sitzungsüberwachungsfunktion wählt automatisch verfügbare Ports im Bereich 6001-6099 aus, um Verbindungen vom Linux VDA zu Citrix Director aufzubauen. Daher ist die Anzahl der ICA®-Sitzungen, die Sie gleichzeitig überwachen können, auf 99 begrenzt. Stellen Sie sicher, dass genügend Ports verfügbar sind, um Ihre Anforderungen zu erfüllen, insbesondere für die Überwachung mehrerer Sitzungen.

Registrierung

Die folgende Tabelle listet die zugehörigen Registrierungen auf:

REGISTRIERUNG	BESCHREIBUNG	STANDARDWERT
EnableSessionShadowing	Aktiviert oder deaktiviert die Sitzungsschattenfunktion	1 (Aktiviert)
ShadowingUseSSL	Legt fest, ob die Verbindung zwischen dem 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 Sitzenschattenfunktion zu deaktivieren, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v "EnableSessionShadowing" -d
0x00000000
```

SSL

Die noVNC-Verbindung zwischen dem Linux VDA und Citrix Director verwendet das WebSocket-Protokoll. Für die Sitzungsschattenfunktion wird die Wahl zwischen `ws://` und `wss://` durch den zuvor erwähnten Registrierungseintrag „ShadowingUseSSL“ bestimmt. Standardmäßig wird `ws://` gewählt. Aus Sicherheitsgründen empfehlen wir jedoch, `wss://` zu verwenden und Zertifikate auf jedem Citrix Director-Client und auf jedem Linux VDA-Server zu installieren. Citrix lehnt jegliche Sicherheitsverantwortung für die Linux VDA-Sitzungsschattenfunktion bei Verwendung von `ws://` ab.

Server- und Root-SSL-Zertifikate abrufen

Zertifikate müssen von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert sein.

Für jeden Linux VDA-Server, auf dem Sie SSL konfigurieren möchten, ist ein separates Serverzertifikat (einschließlich des Schlüssels) erforderlich. Ein Serverzertifikat identifiziert einen bestimmten Computer, daher müssen Sie den vollqualifizierten Domänennamen (FQDN) jedes Servers kennen. Der Einfachheit halber können Sie stattdessen ein Wildcard-Zertifikat für die gesamte Domäne verwenden. In diesem Fall müssen Sie mindestens den Domänennamen kennen.

Zusätzlich zur Installation eines Serverzertifikats auf jedem Server müssen Sie ein Root-Zertifikat derselben CA auf jedem Citrix Director-Client installieren, der mit dem Linux VDA-Server kommuniziert. Root-Zertifikate sind von denselben CAs erhältlich, die die Serverzertifikate ausstellen. Sie können Server- und Clientzertifikate von einer CA installieren, die mit Ihrem Betriebssystem gebündelt ist, von einer Unternehmens-CA (einer CA, die Ihre Organisation Ihnen zugänglich macht) oder von einer CA, die nicht mit Ihrem Betriebssystem gebündelt ist. Wenden Sie sich an das Sicherheitsteam Ihrer Organisation, um herauszufinden, welche Methoden sie für den Erhalt von Zertifikaten vorschreiben.

Wichtig:

- Der allgemeine Name für ein Serverzertifikat muss der exakte FQDN des Linux VDA-Servers oder zumindest die korrekten Wildcard- und Domänenzeichen sein. Beispiel: vda1.basedomain.com oder *.basedomain.com.
- Hashing-Algorithmen wie SHA1 und MD5 sind für Signaturen in digitalen Zertifikaten zu schwach, um von einigen Browsern unterstützt zu werden. Daher ist SHA-256 als Mindeststandard festgelegt.

Installieren Sie ein Stammzertifikat auf jedem Citrix Director-Client

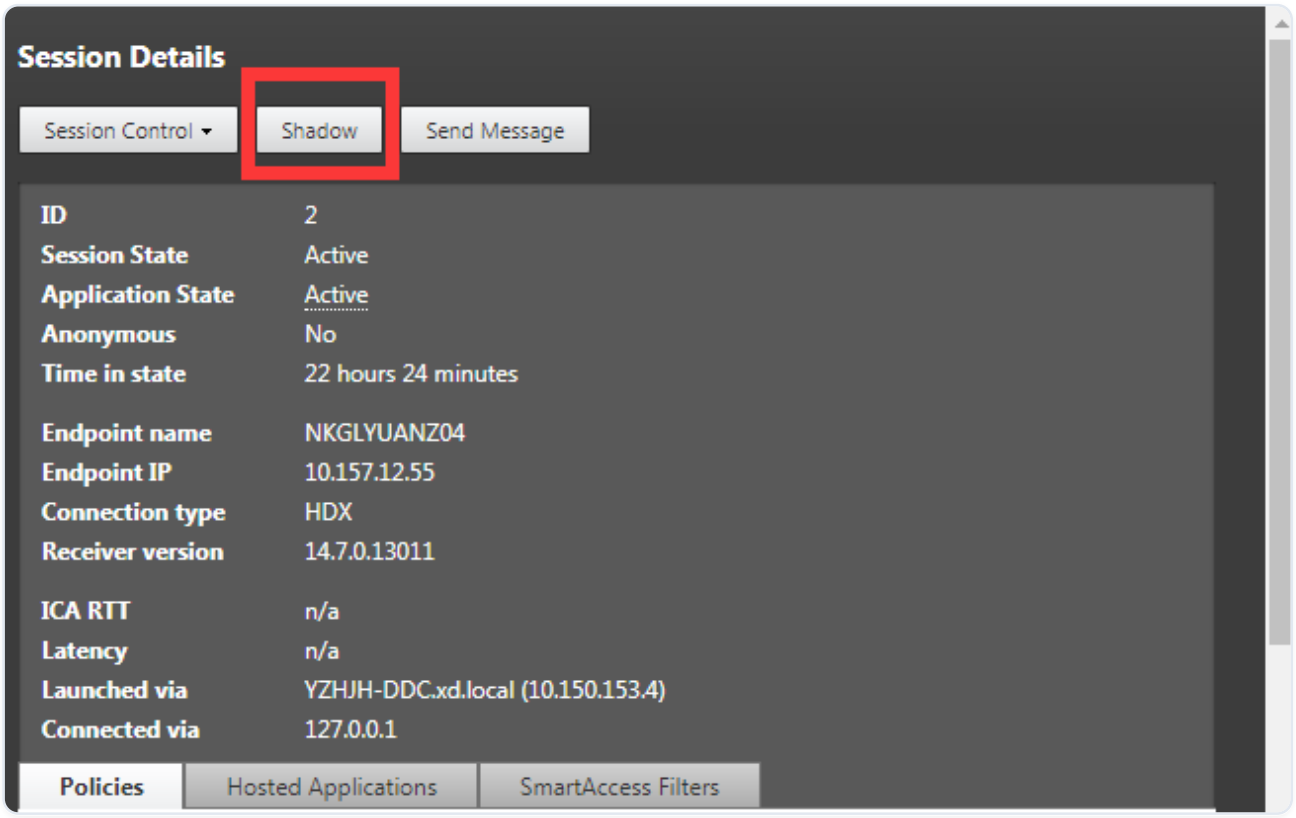
Die Sitzungsschattenfunktion verwendet denselben registrierungsbasierten Zertifikatspeicher wie IIS, sodass Sie Stammzertifikate mit IIS oder dem Microsoft Management Console (MMC)-Zertifikats-Snap-In installieren können. Wenn Sie ein Zertifikat von einer Zertifizierungsstelle erhalten, können Sie den Webserver-Zertifikatsassistenten in IIS neu starten, und der Assistent installiert das Zertifikat. Alternativ können Sie Zertifikate auf dem Computer mit der MMC anzeigen und importieren und das Zertifikat als eigenständiges Snap-In hinzufügen. Internet Explorer und Google Chrome importieren die auf Ihrem Betriebssystem installierten Zertifikate standardmäßig. Für Mozilla Firefox müssen Sie Ihre SSL-Stammzertifikate auf der Registerkarte **Zertifizierungsstellen** des Zertifikatsmanagers importieren.

Installieren Sie ein Serverzertifikat und dessen Schlüssel auf jedem Linux VDA-Server

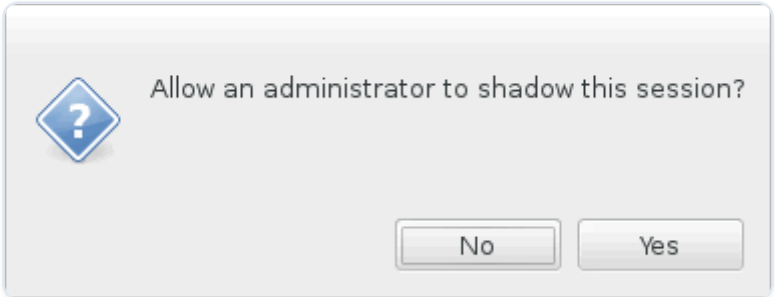
Benennen Sie die Serverzertifikate „shadowingcert.*“ und die Schlüsseldatei „shadowingkey.*“ (* kann das Format angeben, z. B. shadowingcert.csr und shadowingkey.key). Legen Sie Serverzertifikate und Schlüsseldateien unter dem Pfad **/etc/xdl/shadowingssl** ab und schützen Sie sie ordnungsgemäß mit eingeschränkten Berechtigungen. Ein falscher Name oder Pfad führt dazu, dass der Linux VDA ein bestimmtes Zertifikat oder eine Schlüsseldatei nicht finden kann und somit die Verbindung mit Citrix Director fehlschlägt.

Verwendung

Suchen Sie in Citrix Director die Zielsession und klicken Sie in der Ansicht **Sitzungsdetails** auf **Schatten**, um eine Shadowing-Anfrage an den Linux VDA zu senden.



Nach der Initialisierung der Verbindung erscheint eine Bestätigung auf dem ICA-Sitzungsclient (nicht dem Citrix Director-Client), um den Benutzer um Erlaubnis zum Shadowing der Sitzung zu bitten.



Wenn der Benutzer auf **Ja** klickt, erscheint auf der Citrix Director-Seite ein Fenster, das anzeigt, dass die ICA-Sitzung geschattet wird.

Weitere Informationen zur Verwendung finden Sie in der Citrix Director-Dokumentation.

Einschränkungen

- Die Sitzungsschattenfunktion ist nur für die Verwendung in einem Intranet konzipiert. Sie funktioniert nicht für externe Netzwerke, selbst wenn die Verbindung über Citrix Gateway erfolgt. Citrix lehnt jegliche Verantwortung für das Shadowing von Linux VDA-Sitzungen in einem externen Netzwerk ab.
- Wenn die Sitzungsschattenfunktion aktiviert ist, kann ein Domänenadministrator die ICA-Sitzungen nur anzeigen, hat aber keine Berechtigung, sie zu schreiben oder zu steuern.
- Nachdem ein Administrator in Citrix Director auf **Schatten** geklickt hat, erscheint eine Bestätigung, die den Benutzer um Erlaubnis zum Shadowing der Sitzung bittet. Eine Sitzung kann nur geschattet werden, wenn der Sitzungsbenutzer die Erlaubnis erteilt.
- Die zuvor erwähnte Bestätigung hat eine Zeitüberschreitung von 20 Sekunden. Eine Shadowing-Anfrage schlägt fehl, wenn die Zeit abläuft.
- Eine ICA-Sitzung kann von nur einem Administrator in einem Citrix Director-Fenster überwacht werden. Wenn eine ICA-Sitzung von Administrator A überwacht wurde und Administrator B in der Zwischenzeit eine Überwachungsanfrage sendet, wird die Bestätigung zur Einholung der Benutzerberechtigung auf dem Benutzergerät erneut angezeigt. Wenn der Benutzer zustimmt, wird die Überwachungsverbindung für Administrator A beendet und eine neue Überwachungsverbindung für Administrator B aufgebaut. Dies gilt auch, wenn dieselbe Überwachungsanfrage für dieselbe ICA-Sitzung vom selben Administrator gesendet wird.
- Um die Sitzungsüberwachung zu verwenden, installieren Sie Citrix Director 7.16 oder höher.
- Ein Citrix Director-Client verwendet einen FQDN anstelle einer IP-Adresse, um eine Verbindung zum Ziel-Linux-VDA-Server herzustellen. Daher muss der Citrix Director-Client den FQDN des Linux-VDA-Servers auflösen können.

Problembehandlung

Wenn die Sitzungsüberwachung fehlschlägt, führen Sie das Debugging sowohl auf dem Citrix Director-Client als auch auf dem Linux-VDA durch.

Auf dem Citrix Director-Client

Überprüfen Sie in den Entwicklertools des Browsers die Ausgabeprotokolle auf der Registerkarte **Konsole**. Oder überprüfen Sie die Antwort der ShadowLinuxSession-API auf der Registerkarte

Netzwerk. Wenn die Bestätigung zur Einholung der Benutzerberechtigung angezeigt wird, die Verbindung aber nicht aufgebaut werden kann, pingen Sie den FQDN des Linux-VDA manuell an, um zu überprüfen, ob Citrix Director den FQDN auflösen kann. Wenn es ein Problem mit der `wss://` Verbindung gibt, überprüfen Sie Ihre Zertifikate.

Auf dem Linux-VDA

Vergewissern Sie sich, dass die Bestätigung zur Einholung der Benutzerberechtigung als Reaktion auf eine Überwachungsanfrage angezeigt wird. Ist dies nicht der Fall, überprüfen Sie die Dateien vda.log und hdx.log auf Hinweise. Um die Datei vda.log zu erhalten, gehen Sie wie folgt vor:

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“ in „trace“ wie folgt:

   ```
   <!-- Broker Agent Plugin - Director VDA plugin Logger -->


    <logger name="com.citrix.dmc">


      <level value="trace"/>


    </logger>
   ```

3. Führen Sie den Befehl `service ctxvda restart` aus, um den Dienst `ctxvda` neu zu starten.

Wenn beim Verbindungsaufbau ein Fehler auftritt:

1. Überprüfen Sie, ob eine Firewall-Einschränkung die Sitzungsüberwachung daran hindert, den Port zu öffnen.
2. Vergewissern Sie sich, dass Zertifikate und Schlüsseldateien korrekt benannt und im richtigen Pfad abgelegt sind, falls es sich um ein SSL-Szenario handelt.

3. Vergewissern Sie sich, dass zwischen 6001 und 6099 genügend Ports für neue Überwachungsanfragen verfügbar sind.

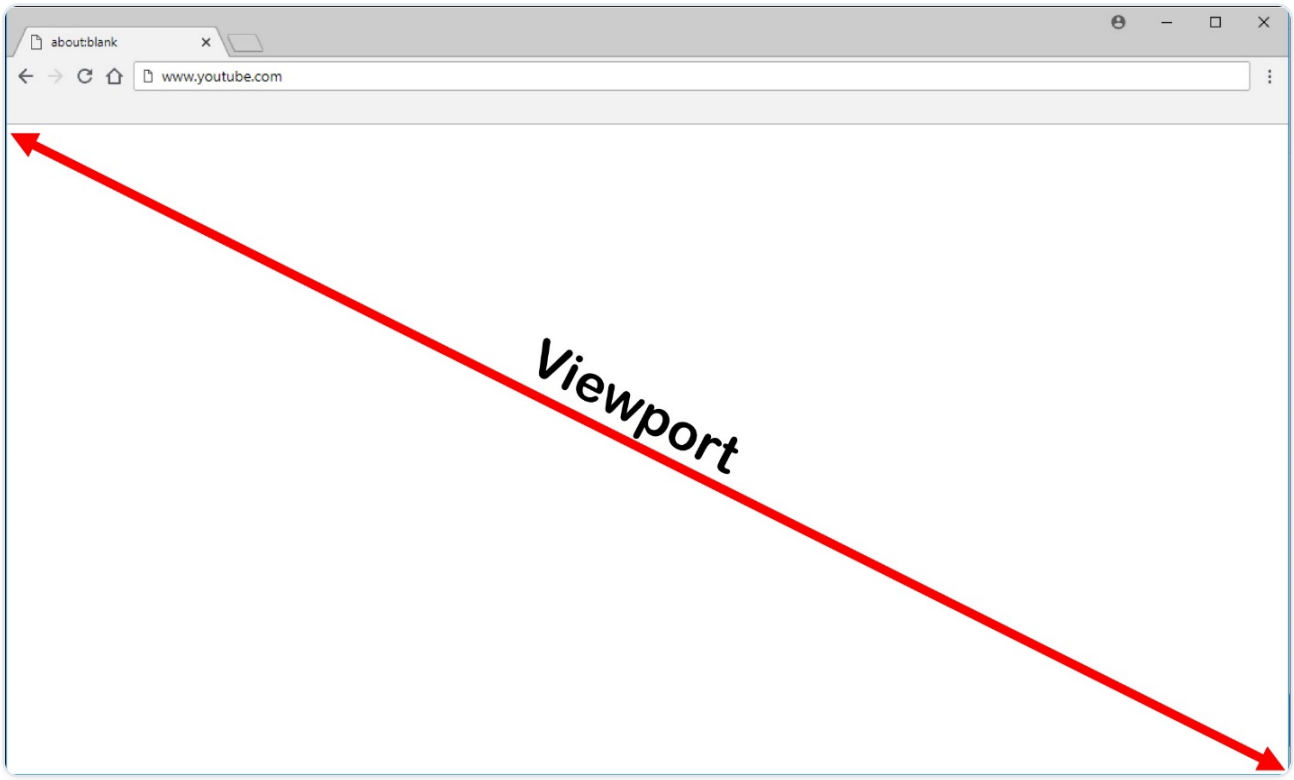
Browserinhaltsumleitung

Übersicht

Der Linux-VDA unterstützt die Browserinhaltsumleitung in Google Chrome. Die Browserinhaltsumleitung ermöglicht das Rendern von Webseiten auf der Zulassungsliste auf der Clientseite. Diese Funktion verwendet die Citrix Workspace™-App, um eine entsprechende Rendering-Engine auf der Clientseite zu instanziieren, die die HTTP- und HTTPS-Inhalte von der URL abruft.

> **Hinweis:**
>
> Sie können mithilfe einer Zulassungsliste festlegen, welche Webseiten auf die Clientseite umgeleitet werden. Umgekehrt können Sie mithilfe einer Sperrliste festlegen, welche Webseiten nicht auf die Clientseite umgeleitet werden.
>
> Diese Overlay-Web-Layout-Engine läuft auf dem Client anstatt auf dem VDA und verwendet die Client-CPU, GPU, RAM und das Netzwerk.

Nur der Browser-Viewport wird umgeleitet. Der Viewport ist der rechteckige Bereich in Ihrem Browser, in dem Inhalte angezeigt werden. Der Viewport umfasst keine Elemente wie die Adressleiste, die Favoritenleiste und die Statusleiste. Diese Elemente werden weiterhin im Browser auf dem VDA ausgeführt.



Systemanforderungen

Windows-Client:

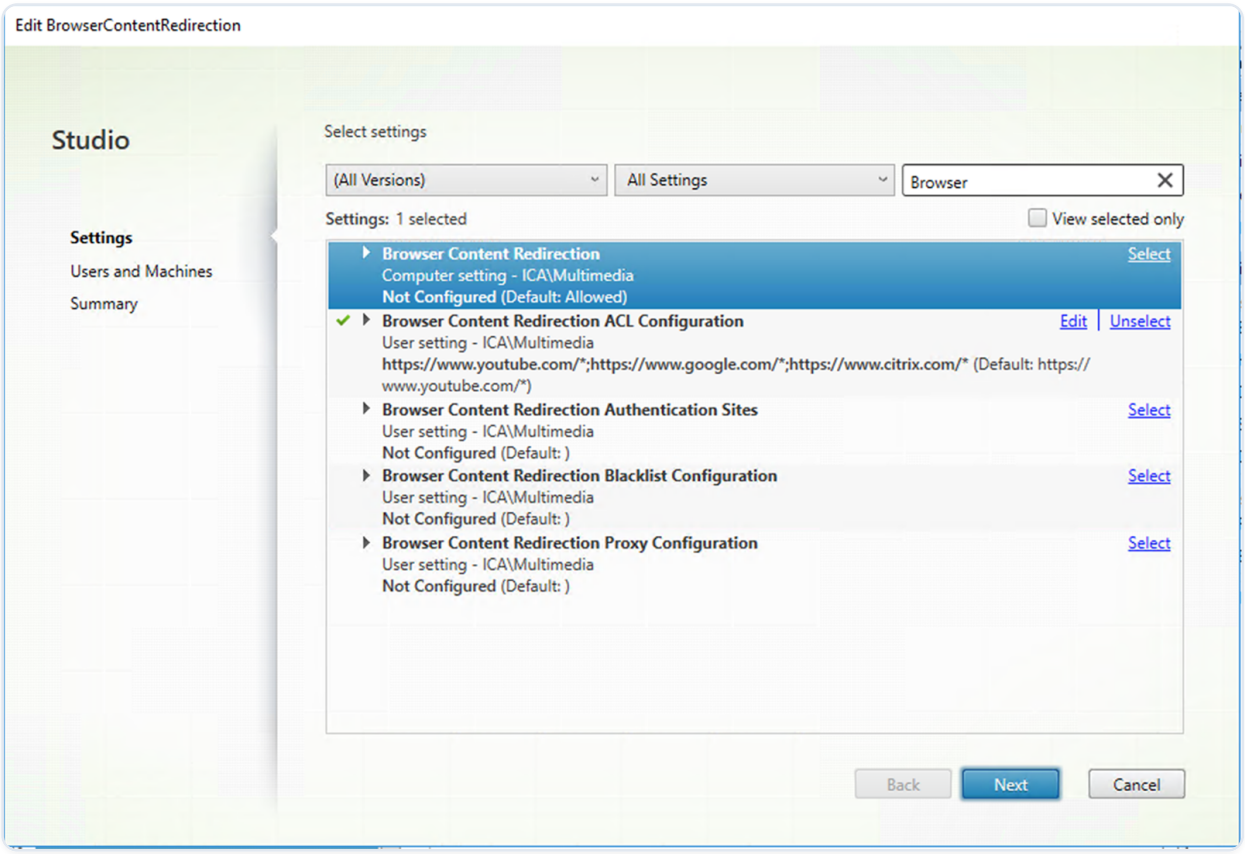
- Citrix Workspace-App 1809 für Windows oder höher

Linux-VDA:

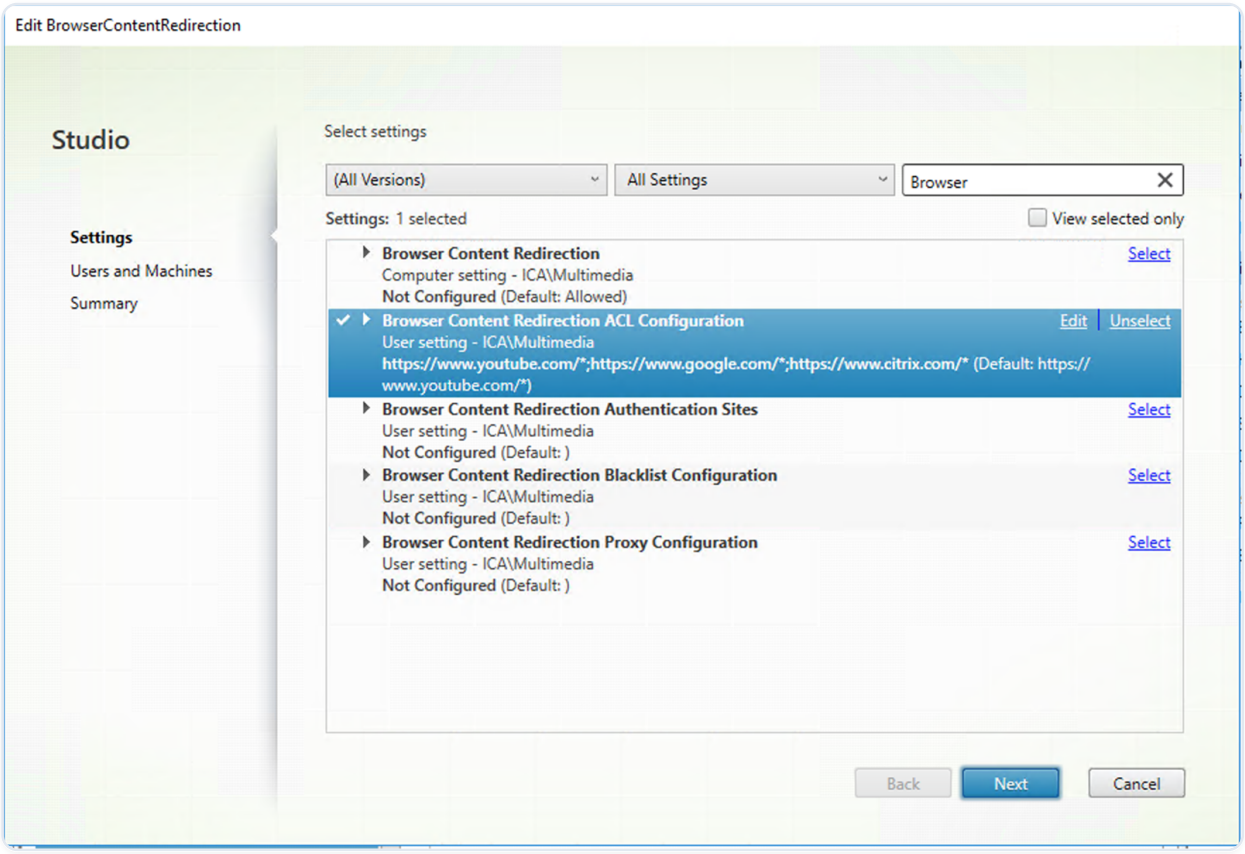
- VDA-Betriebssystem: Ubuntu 16.04, Ubuntu 18.04, RHEL 7.8, RHEL 8.2, RHEL 8.1, SLES 12.5
- Browser auf dem VDA: Google Chrome v66 oder höher mit installierter Citrix® Browser Content Redirection-Erweiterung

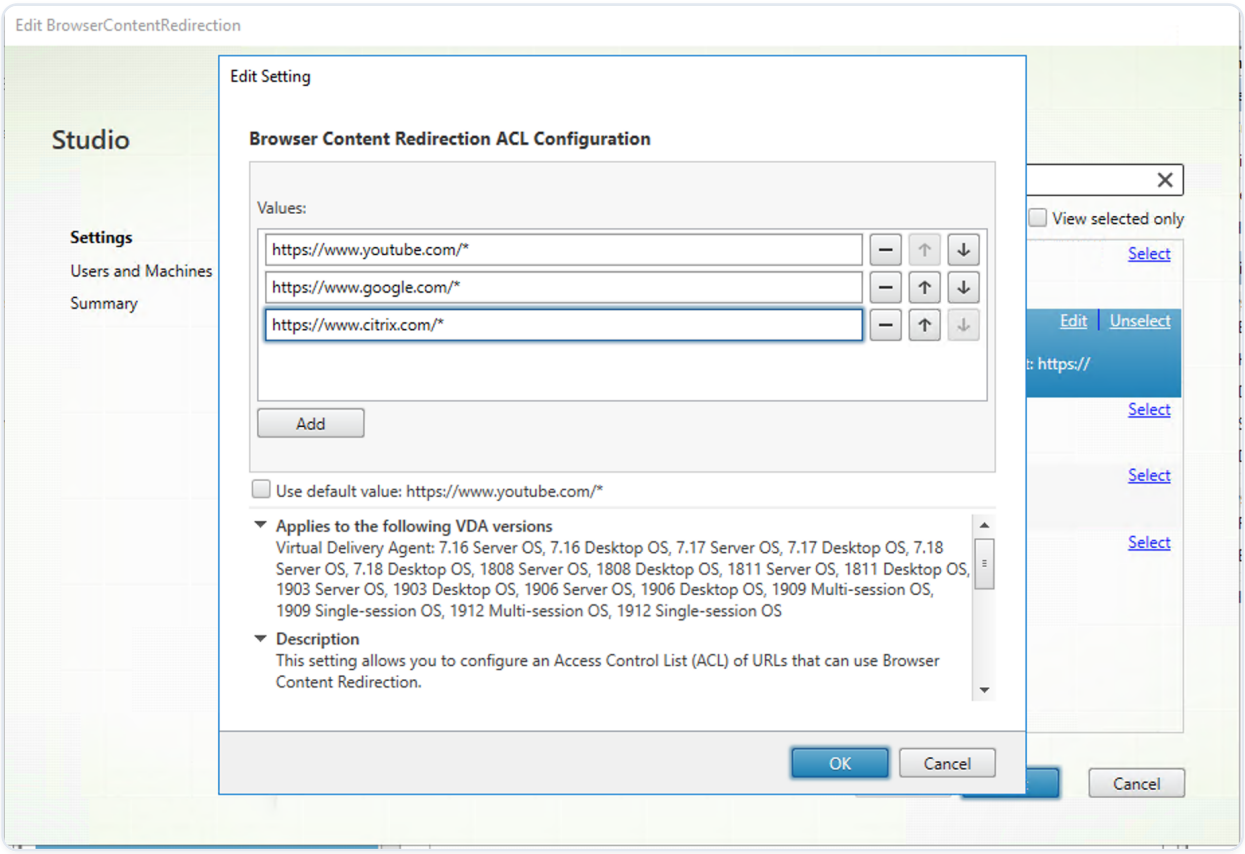
Browserinhaltsumleitung konfigurieren

1. Konfigurieren Sie in Citrix Studio eine Richtlinie, die eine Zulassungsliste von URLs, die die Browserinhaltsumleitung verwenden dürfen, und eine Sperrliste von URLs, die dies nicht dürfen, festlegt. Die Browserinhaltsumleitung ist standardmäßig auf **Zulässig** eingestellt.

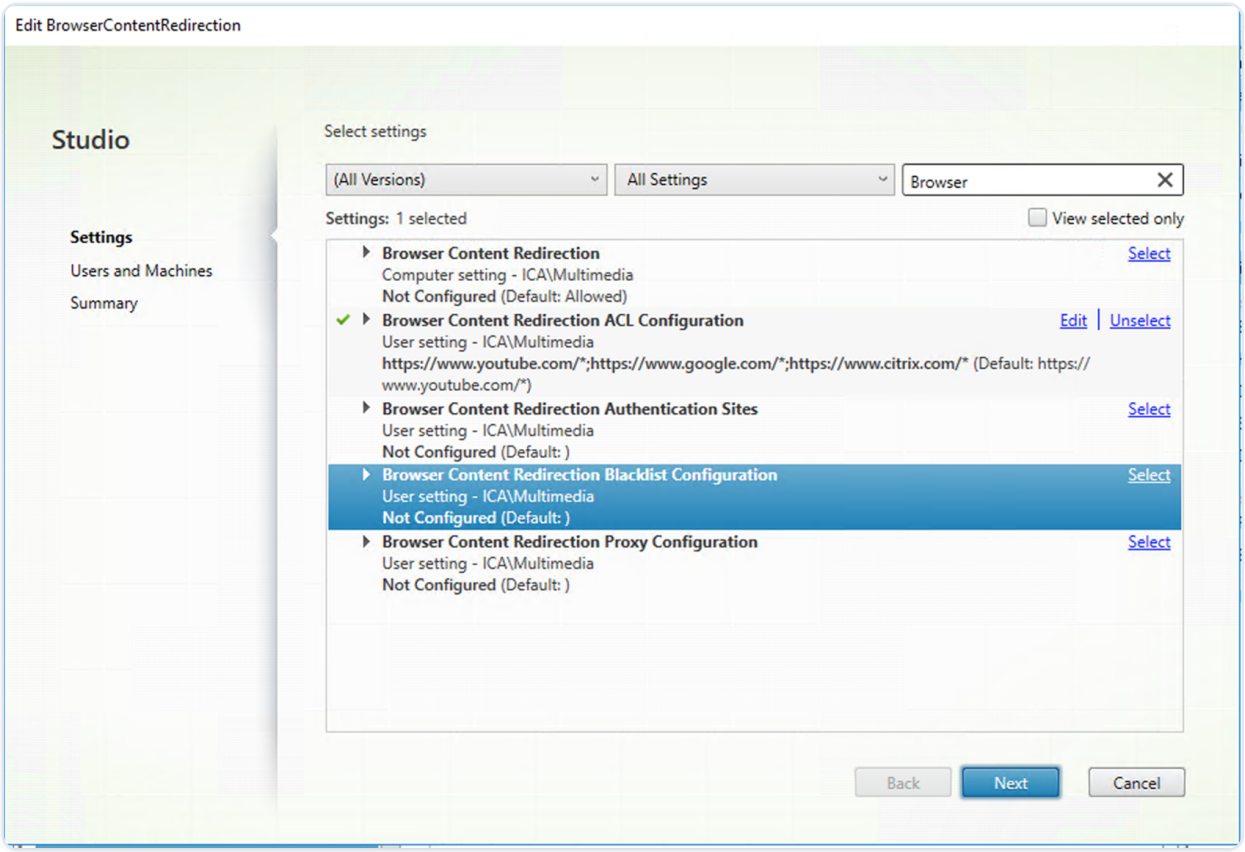


Die Einstellung **Browser Content Redirection ACL Configuration** gibt eine Zulassungsliste von URLs an, die die Browserinhaltsumleitung verwenden dürfen.





Die Einstellung **Browser Content Redirection Blacklist Configuration** gibt eine Sperrliste von URLs an, die keine Browserinhaltsumleitung verwenden können.



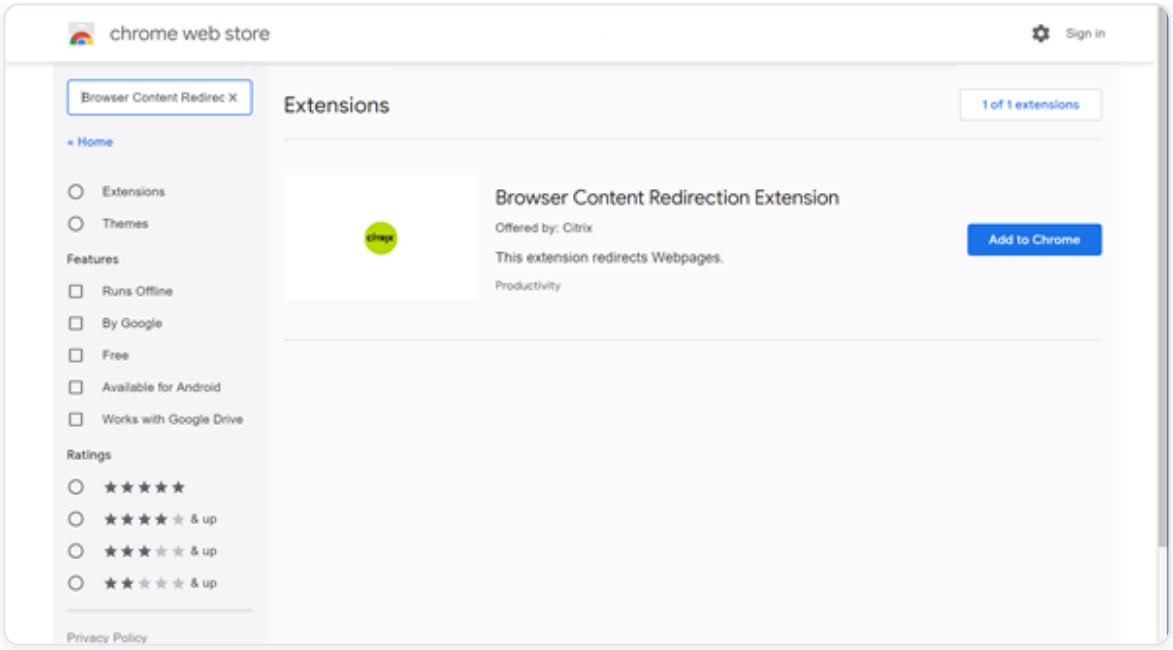
> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit die Einstellung **Browser Content Redirection Proxy Configuration** nicht.

2. Damit der Browser auf dem VDA erkennen kann, ob eine URL (zu der navigiert wird) mit einer Zulassungsliste oder einer Sperrliste übereinstimmt, fügen Sie die Citrix Browserinhaltsumleitungs-Erweiterung aus dem Chrome Web Store hinzu. Klicken Sie auf dem VDA auf **Zu Chrome hinzufügen**.

> **Wichtig:**
>
> Die Erweiterung ist auf dem Client nicht erforderlich. Fügen Sie sie nur auf dem VDA hinzu.

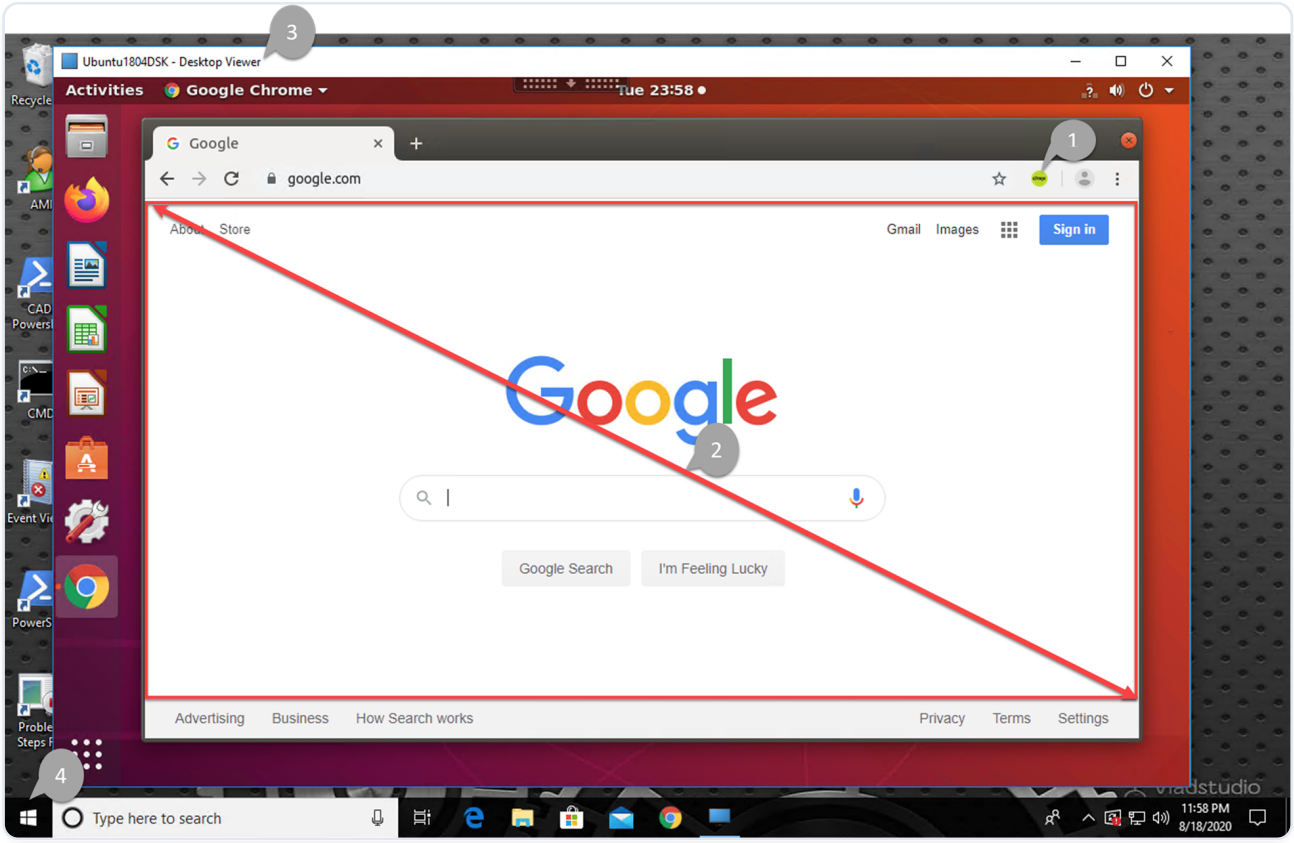
\>

> Chrome-Erweiterungen werden pro Benutzer installiert. Eine Aktualisierung eines Golden Image zum Hinzufügen oder Entfernen einer Erweiterung ist nicht erforderlich.



Wenn eine Übereinstimmung mit einer URL in einer Zulassungsliste (z. B. `https://www.mycompany.com/`) gefunden wird, aber 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 instanziiert dann eine lokale Rendering-Engine und zeigt die Website an.

Die Citrix Workspace-App fügt die Website dann nahtlos wieder in den Inhaltsbereich des virtuellen Desktop-Browsers ein.



1. Symbol der Citrix Browserinhaltsumleitungs-Erweiterung

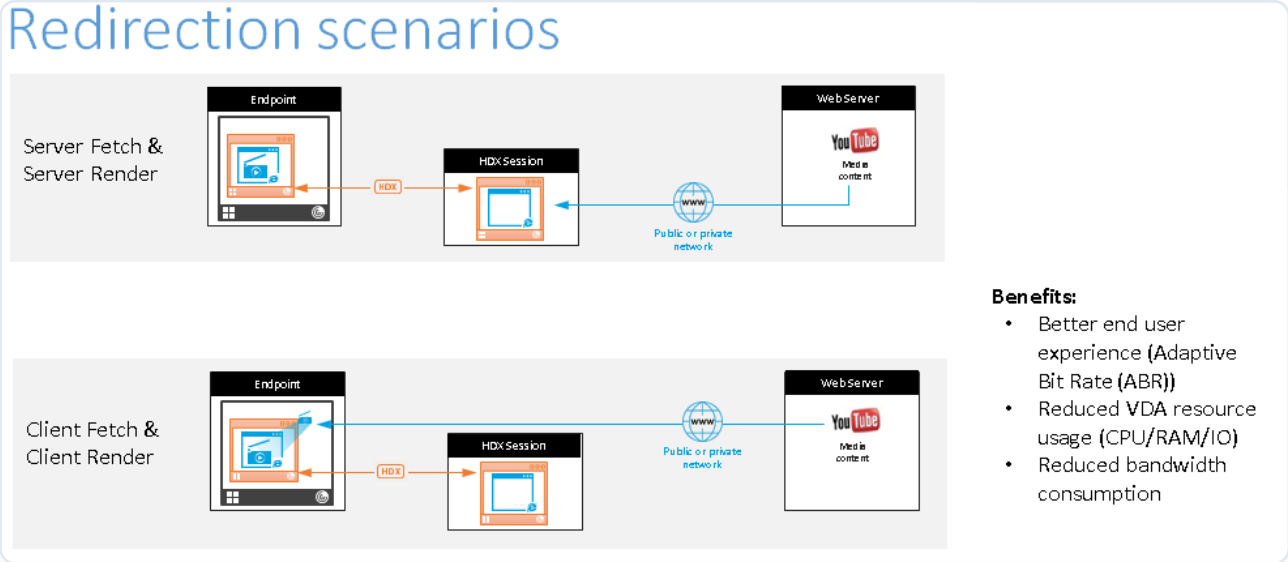
   Die Farbe des Erweiterungssymbols gibt den Status der Chrome-Erweiterung an. Es ist eine der drei Farben:

   - Grün: Aktiv und verbunden
   - Grau: Nicht aktiv/im Leerlauf auf der aktuellen Registerkarte
   - Rot: Defekt/Funktioniert nicht

2. Viewport auf dem Client gerendert oder in den virtuellen Desktop zurückgemischt
3. Linux VDA
4. Windows-Client

Umleitungsszenarien

Hier sind Szenarien, wie die Citrix Workspace-App Inhalte abruft:



- **Server-Abruf und Server-Rendering:** Es erfolgt keine Umleitung, da Sie die Site nicht zur Zulassungsliste hinzugefügt haben oder die Umleitung fehlgeschlagen ist. Wir greifen auf das Rendern der Webseite auf dem VDA zurück und verwenden Thinwire, um die Grafiken remote bereitzustellen. Verwenden Sie Richtlinien, um das Fallback-Verhalten zu steuern. Dieses Szenario verursacht einen hohen CPU-, RAM- und Bandbreitenverbrauch auf dem VDA.
- **Client-Abruf und Client-Rendering:** Da die Citrix Workspace-App direkt mit dem Webserver kommuniziert, erfordert sie Internetzugriff. Dieses Szenario verlagert die gesamte Netzwerk-, CPU- und RAM-Nutzung von Ihrer Citrix Virtual Apps and Desktops™-Site.

Fallback-Mechanismus

Es kann vorkommen, dass die Clientumleitung fehlschlägt. Wenn die Clientmaschine beispielsweise keinen direkten Internetzugriff hat, könnte eine Fehlermeldung an den VDA zurückgesendet werden. In solchen Fällen kann der Browser auf dem VDA die Seite dann neu laden und auf dem Server rendern.

Unterstützung der Citrix Workspace™ App für HTML5

Ab dieser Version können Sie die Citrix Workspace App für HTML5 verwenden, um direkt auf virtuelle Linux-Apps und -Desktops zuzugreifen, ohne Ihren Client mit Citrix Gateway zu verbinden. Informationen zur Citrix Workspace App für HTML5 finden Sie in der Citrix-Dokumentation.

Diese Funktion aktivieren

Diese Funktion ist standardmäßig deaktiviert. Um sie zu aktivieren, gehen Sie wie folgt vor:

1. Aktivieren Sie in Citrix StoreFront™ die Citrix Workspace App für HTML5.

   Die detaillierte Vorgehensweise finden Sie in Schritt 1 des Knowledge Center-Artikels CTX208163.

2. WebSocket-Verbindungen aktivieren.

   a. Legen Sie in Citrix Studio die Richtlinie **WebSockets-Verbindungen** auf **Zulässig** 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 Dienst `ctxvda` und den Dienst `ctxhdx` in dieser Reihenfolge neu, damit Ihre Einstellung wirksam wird.

   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, sieht die Befehlsausgabe wie folgt aus:

      ```
      tcp 0 0 :::8008 :::* LISTEN
      ```

   Hinweis: Sie können auch die TLS-Verschlüsselung aktivieren, um WebSocket-Verbindungen zu sichern. Informationen zum Aktivieren der TLS-Verschlüsselung finden Sie unter Sichern von Benutzersitzungen mit TLS.

Linux-VMs und Linux-Sitzungen in Citrix Director überwachen

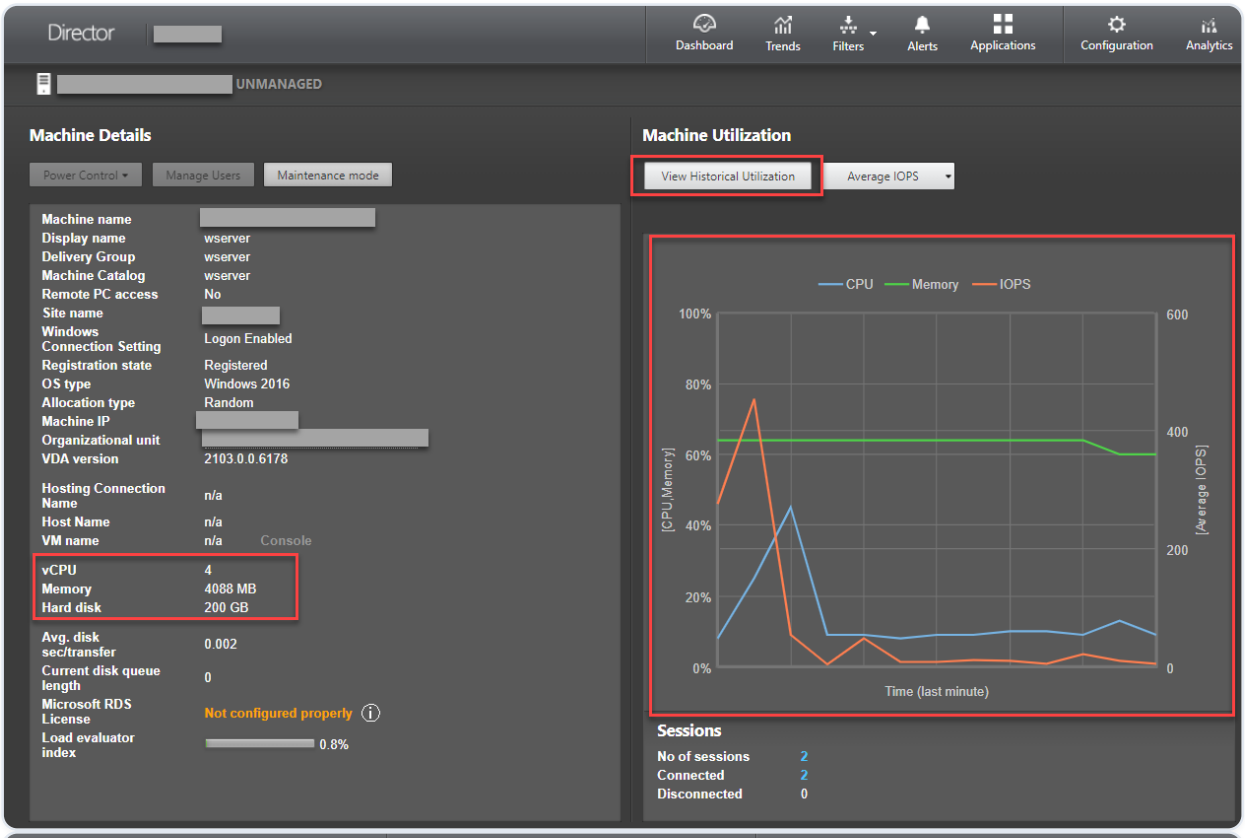
Dieser Artikel listet einige der Metriken auf, die für Linux-VMs und Linux-Sitzungen in Citrix Director verfügbar sind.

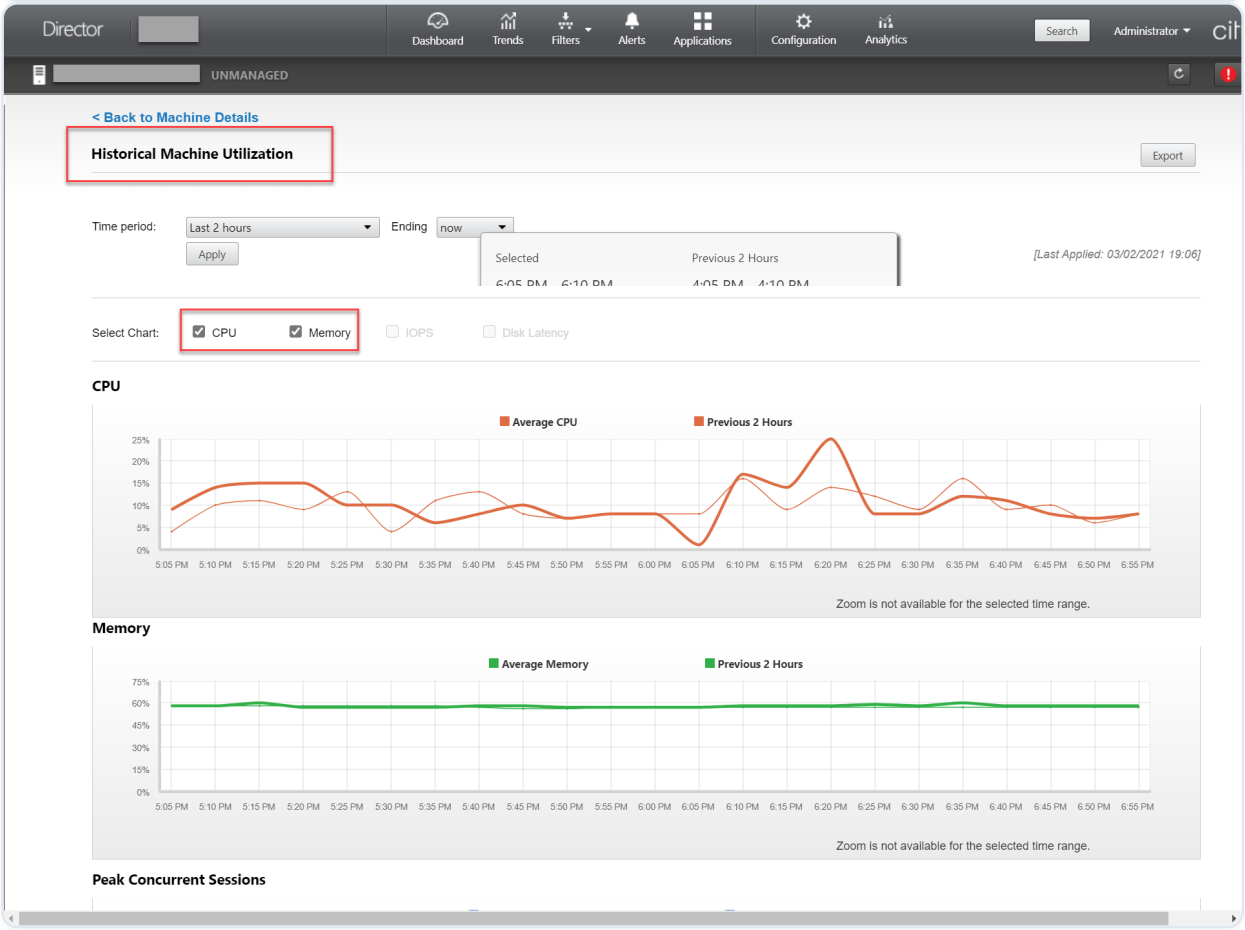
Metriken für Linux-VMs

Um auf die Metriken einer Linux-VM zuzugreifen, suchen Sie die VM in Citrix Director und überprüfen Sie den Bereich **Maschinendetails**.

Ab Linux VDA Version 2103 sind die folgenden Metriken für Linux-VMs in Citrix Director verfügbar.

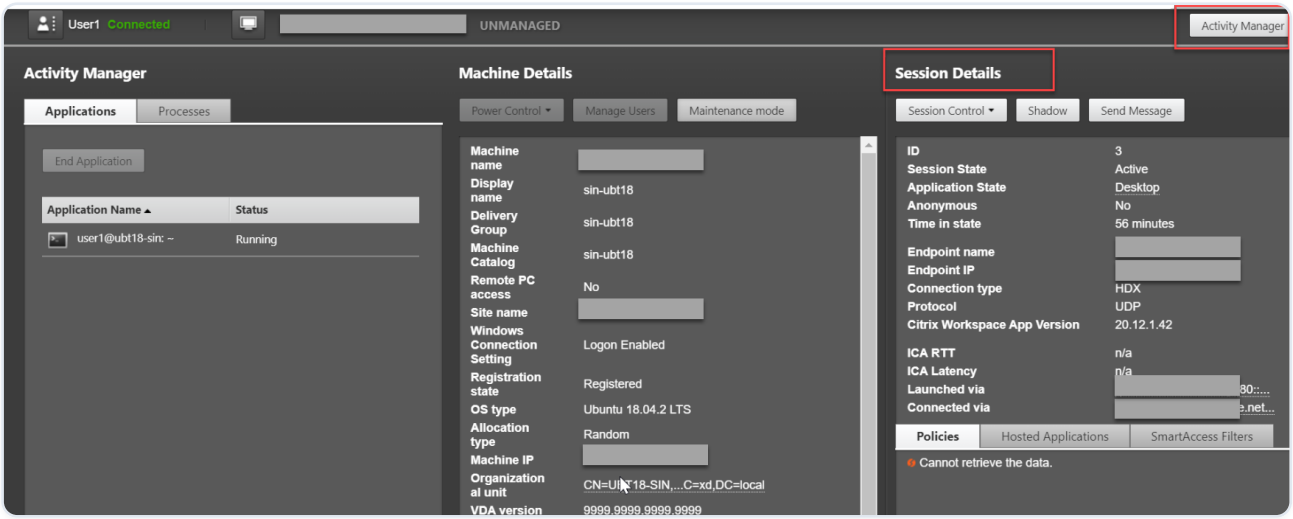
- Anzahl der CPU-Kerne
- Speichergröße
- Festplattenkapazität
- Aktuelle und historische CPU- und Speicherauslastung


Director
Dashboard
Trends
Filters
Alerts
Applications
Configuration
Analytics
UNMANAGED
Machine Details
Power Control
Manage Users
Maintenance mode
Machine name
Display name wserver
Delivery Group wserver
Machine Catalog wserver
Remote PC access No
Site name
Windows Connection Setting Logon Enabled
Registration state Registered
OS type Windows 2016
Allocation type Random
Machine IP
Organizational unit
VDA version 2103.0.0.6178
Hosting Connection Name n/a
Host Name n/a
VM name n/a Console
vCPU 4
Memory 4088 MB
Hard disk 200 GB
Avg. disk sec/transfer 0.002
Current disk queue length 0
Microsoft RDS License Not configured properly
Load evaluator index 0.8%
Machine Utilization
View Historical Utilization
Average IOPS
CPU
Memory
IOPS
100%
80%
60%
40%
20%
0%
600
400
200
0
[CPU,Memory]
[Average IOPS]
Time (last minute)
Sessions
No of sessions 2
Connected 2
Disconnected 0


Director
Dashboard
Trends
Filters
Alerts
Applications
Configuration
Analytics
Search
Administrator
UNMANAGED
< Back to Machine Details
Historical Machine Utilization
Export
Time period: Last 2 hours
Ending now
Apply
Selected
Previous 2 Hours
[Last Applied: 03/02/2021 19:06]
Select Chart: CPU Memory IOPS Disk Latency
CPU
Average CPU
Previous 2 Hours
Zoom is not available for the selected time range.
Memory
Average Memory
Previous 2 Hours
Zoom is not available for the selected time range.
Peak Concurrent Sessions

Metriken für Linux-Sitzungen

Um die Metriken einer Linux-Sitzung anzuzeigen, öffnen Sie die Seite **Alle Sitzungen**, indem Sie **Filter > Sitzungen > Alle Sitzungen** auswählen, 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 deren Ansicht **Aktivitätsmanager** aufzurufen. Zum Beispiel:



- ICA® RTT

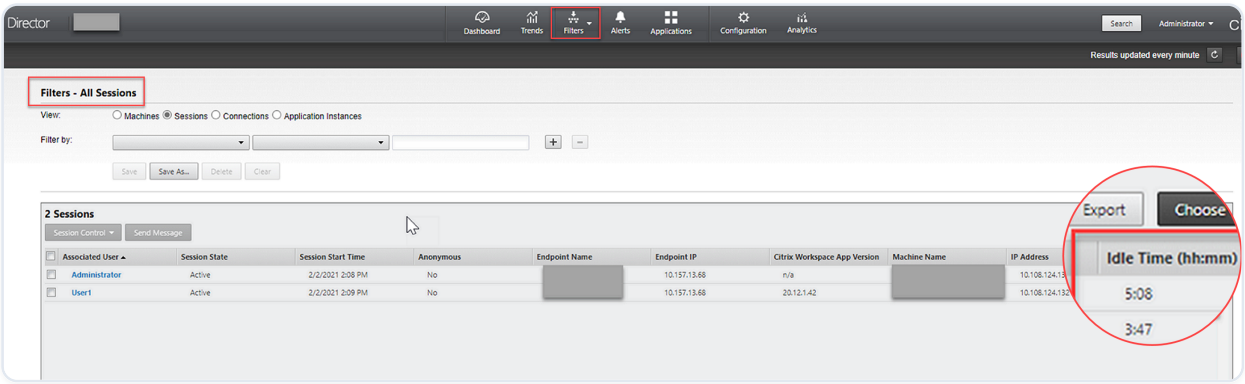
  Ab Linux VDA Version 1903 sind ICA-RTT-Metriken verfügbar. Um ICA-RTT-Metriken anzuzeigen, verwenden Sie Citrix Director 1903 oder höher und erstellen Sie die Richtlinien **ICA-Roundtrip-Berechnung** und **ICA-Roundtrip-Berechnungsintervall** in Citrix Studio. Informationen zur Richtlinienerstellung finden Sie unter Erstellen einer Richtlinie mit Studio.

- Protokoll

  Ab Linux VDA Version 1909 sind Protokollinformationen verfügbar. Das Transportprotokoll einer Linux-Sitzung wird im Bereich **Sitzungsdetails** als **UDP** oder **TCP** angezeigt.

- Leerlaufzeit

  Ab Linux VDA Version 2103 ist die Leerlaufzeitmetrik für Linux-Sitzungen verfügbar. Um auf diese Metrik zuzugreifen, öffnen Sie die Seite **Alle Sitzungen**, indem Sie **Filter > Sitzungen > Alle Sitzungen** auswählen.



Überwachungsdienst-Daemon

Der Überwachungsdienst-Daemon überwacht wichtige Dienste durch regelmäßige Scans. Beim Erkennen von Ausnahmen startet der Daemon Dienstprozesse neu oder beendet sie und bereinigt Prozessreste zur Freigabe von Ressourcen. Die erkannten Ausnahmen werden in der Datei **/var/log/xdl/ms.log** protokolliert.

Konfiguration

Der Überwachungsdienst-Daemon startet automatisch, wenn Sie den VDA starten.

Sie können die Funktion über die Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** mit Administratorrechten konfigurieren. Die Konfigurationsdateien befinden sich unter **/opt/Citrix/VDA/sbin**.

Damit Ihre Änderungen in den Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** wirksam werden, führen Sie den folgenden Befehl aus, um den Überwachungsdienst-Daemon neu zu starten.

```
service ctxmonitorservice restart
```

- **scanningpolicy.conf**

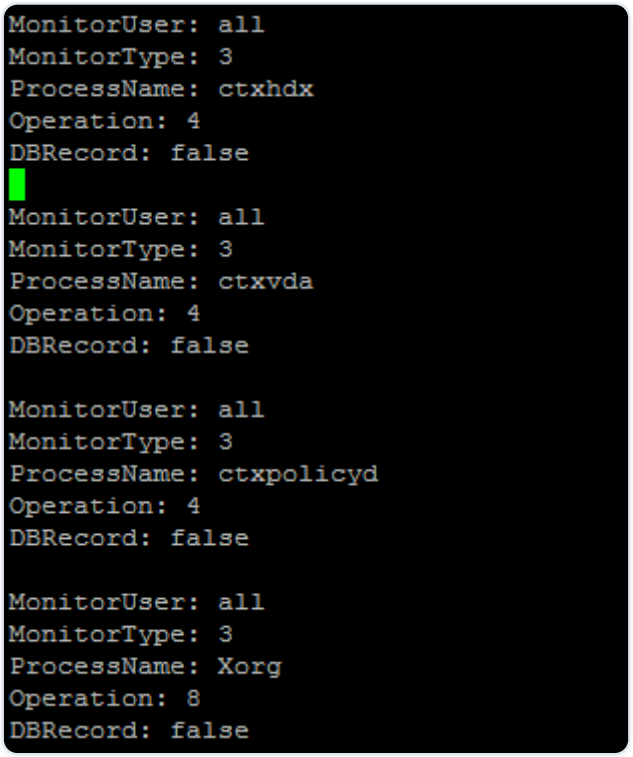
  Diese Konfigurationsdatei aktiviert oder deaktiviert den Überwachungsdienst-Daemon. Sie legt das Dienst-Erkennungsintervall fest und gibt an, ob erkannte Ausnahmen repariert werden sollen.

  - MonitorEnable: true/false (standardmäßig true)
  - DetectTime: 20 (Einheit: Sekunden, Standardwert: 20, Mindestwert: 5)
  - AutoRepair: true/false (standardmäßig true)
  - MultBalance: falsch

- ReportAlarm: falsch

- **rulesets.conf**

  Diese Konfigurationsdatei gibt die zu überwachenden Zieldienste an. Standardmäßig werden vier Dienste überwacht, wie im folgenden Screenshot gezeigt.



  Um jeden zu überwachenden Dienst zu konfigurieren, legen Sie die folgenden Felder fest.

  - MonitorUser: alle
  - MonitorType: 3
  - ProcessName: <> (Der Prozessname darf nicht leer sein und muss exakt übereinstimmen.)
  - Operation: 1/2/4/8 (1 = Dienst beenden, wenn Ausnahmen erkannt werden. 2 = Dienst beenden (kill), wenn Ausnahmen erkannt werden. 4 = Dienst neu starten. 8 = Xorg-Prozessreste bereinigen.)
  - DBRecord: falsch

- **whitelist.conf**

  Die in der Datei **rulesets.conf** angegebenen Zieldienste müssen auch in der Datei **whitelist.conf** konfiguriert werden. Die Whitelist-Konfiguration ist ein sekundärer Filter für die Sicherheit.

  Um die Whitelist zu konfigurieren, fügen Sie nur die Prozessnamen (die exakt übereinstimmen müssen) in die Datei **whitelist.conf** ein. Ein Beispiel finden Sie im folgenden Screenshot.

```
ctxcdmd
ctxcdmmount
ctxcdmstat
ctxceip
ctxclipboard
ctxconnect
ctxcredentialctl
ctxctl
ctxcupsd
ctxdisconnect
ctxeuem
ctxfiletransfer
ctxgfx
ctxhdx
ctxism
ctxlogd
ctxlogin
ctxmonitorservice
ctxmrvc
ctxpolicyd
ctxscardsd
ctxvhcid
ctxvda
Xorg
```

Hinweis:

Bevor Sie die Dienste `ctxvda`, `ctxhdx` und `ctxpolicyd` beenden, führen Sie den Befehl `service ctxmonitorservice stop` aus, um den Monitor-Dienst-Daemon zu beenden. Andernfalls startet der Monitor-Dienst-Daemon die von Ihnen beendeten Dienste neu.

Sichere Benutzersitzungen mit TLS

Ab Version 7.16 unterstützt der Linux VDA die TLS-Verschlüsselung für sichere Benutzersitzungen. Die TLS-Verschlüsselung ist standardmäßig deaktiviert.

TLS-Verschlüsselung aktivieren

Um die TLS-Verschlüsselung für sichere Benutzersitzungen zu aktivieren, besorgen Sie sich Zertifikate und aktivieren Sie die TLS-Verschlüsselung sowohl auf dem Linux VDA als auch auf dem Delivery Controller™ (dem Controller).

Zertifikate abrufen

Besorgen Sie sich Serverzertifikate im PEM-Format und Stammzertifikate im CRT-Format von einer vertrauenswürdigen Zertifizierungsstelle (CA). Ein Serverzertifikat enthält die folgenden Abschnitte:

- Zertifikat
- Unverschlüsselter privater Schlüssel
- Zwischenzertifikate (optional)

Ein Beispiel für ein Serverzertifikat:

```
-----BEGIN CERTIFICATE-----

MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV

BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU

MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0

MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL

MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE

ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G

A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD

gY0AMIGJAoGBALCTTOdxcivbI0L0F66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9

t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEw13YxM6COyBf7L6psrsCDNnBP1q8TJH

4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+0FQ2Bq3NhwsRhnAgMBAAGj

gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8y0w

gZkGA1UdIwSBkTCBjoAU85kN1EPJ0cVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV

BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU

MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0

ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB

AD5axBYHwIxJCJzNt2zdXnbp2O0yUToWElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68

VelBu1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbu0IjOtr3pkxAe

b6CFJtNLudHUrwF6l0rB72zbyz3PiIx+HEwt1j0j8z4K

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q

fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy

R+MaDyF1HmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB

AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea

FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSx0Yb/lAdck/
```

TLS-Verschlüsselung aktivieren

TLS-Verschlüsselung auf dem Linux VDA aktivieren

Verwenden Sie auf dem Linux VDA das Tool `enable_vdassl.sh`, um die TLS-Verschlüsselung zu aktivieren (oder zu deaktivieren). Das Tool befindet sich im Verzeichnis **/opt/Citrix/VDA/sbin**. Informationen zu den im Tool verfügbaren Optionen erhalten Sie, indem Sie den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help` ausführen.

Tipp: Ein Serverzertifikat muss auf jedem Linux VDA-Server installiert sein, und Stammzertifikate müssen auf jedem Linux VDA-Server und -Client installiert sein.

TLS-Verschlüsselung auf dem Controller aktivieren

> **Hinweis:**

> Sie können die TLS-Verschlüsselung nur für ganze Bereitstellungsgruppen aktivieren. Sie können die TLS-Verschlüsselung nicht für bestimmte Anwendungen aktivieren.

> Führen Sie in einem PowerShell-Fenster auf dem Controller die folgenden Befehle nacheinander aus, um die TLS-Verschlüsselung für die Zielbereitstellungsgruppe zu aktivieren.

1. `Add-PSSnapin citrix.*`.
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule –HdxSslEnabled $true`

> **Hinweis:**

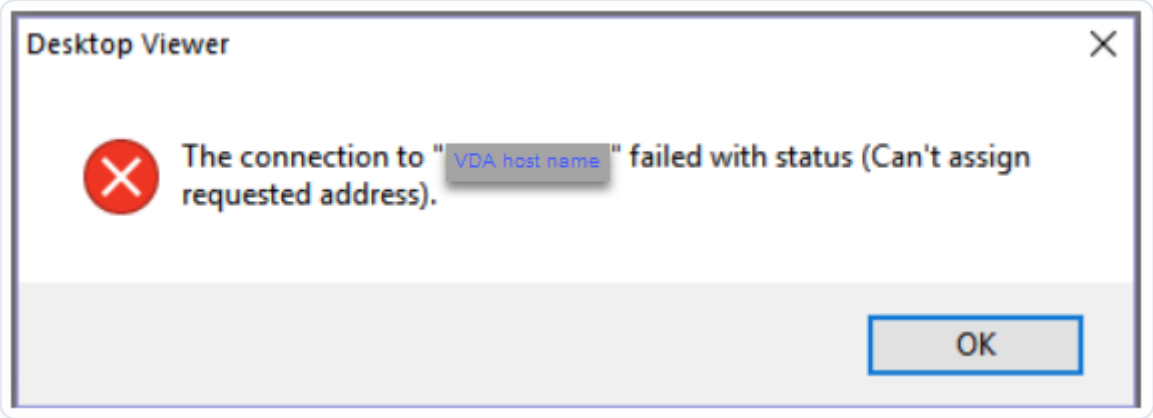
> Um sicherzustellen, dass eine ICA®-Sitzungsdatei nur VDA-FQDNs enthält, können Sie auch den Befehl `Set-BrokerSite –DnsResolutionEnabled $true` ausführen. Der Befehl aktiviert die DNS-Auflösung. Wenn Sie die DNS-Auflösung deaktivieren, werden in einer ICA-Sitzungsdatei VDA-IP-Adressen offengelegt und FQDNs nur für TLS-bezogene Elemente wie SSLProxyHost und UDPDTLSPort bereitgestellt.

> Um die TLS-Verschlüsselung auf dem Controller zu deaktivieren, 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 „Can't assign requested address“ (Angeforderte Adresse kann nicht zugewiesen werden) kann in der Citrix Workspace™-App für Windows auftreten, wenn Sie versuchen, auf eine veröffentlichte Desktopsitzung zuzugreifen:



Fügen Sie als Problemumgehung einen Eintrag zur Datei **hosts** hinzu, der dem folgenden ähnelt:

```
<IP address of the Linux VDA>      <FQDN of the Linux VDA>
```

Auf Windows-Computern befindet sich die Datei **hosts** normalerweise unter `C:\Windows\System32\drivers\etc\hosts`.

Benutzersitzungen mit DTLS sichern

Die DTLS-Verschlüsselung ist ab Release 7.18 ein vollständig unterstütztes Feature. Standardmäßig ist dieses Feature auf dem Linux VDA aktiviert. Weitere Informationen finden Sie unter Transport Layer Security.

DTLS-Verschlüsselung aktivieren

Überprüfen, ob adaptiver Transport aktiviert ist

Vergewissern Sie sich in Citrix Studio, dass die Richtlinie **HDX™ Adaptive Transport** auf **Bevorzugt** oder **Diagnosemodus** eingestellt ist.

SSL-Verschlüsselung auf dem Linux VDA aktivieren

Verwenden Sie auf dem Linux VDA das Tool `enable_vdassl.sh`, um die SSL-Verschlüsselung zu aktivieren (oder zu deaktivieren). Das Tool befindet sich unter **/opt/Citrix/VDA/sbin**. Informationen zu den im Tool verfügbaren Optionen erhalten Sie, indem Sie den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh -h` ausführen.

> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit DTLS 1.0 und DTLS 1.2. DTLS 1.2 erfordert Citrix Receiver für Windows 4.12 oder Citrix Workspace-App 1808 für Windows oder höher. Wenn Ihr Client nur DTLS 1.0 unterstützt (z. B. Citrix Receiver für Windows 4.11), stellen Sie `SSLMinVersion` mit dem Tool `enable_vdassl.sh` auf `TLS_1.0` und `SSLCipherSuite` auf `COM` oder `ALL` ein.

Textbasiertes Sitzungswasserzeichen

Textbasierte Sitzungswasserzeichen helfen, Datendiebstahl zu verhindern und die Nachverfolgung zu ermöglichen. Diese nachverfolgbaren Informationen erscheinen auf dem Sitzungsdesktop als Abschreckung für diejenigen, die Fotos und Bildschirmaufnahmen verwenden, um Daten zu stehlen. Sie können ein Wasserzeichen als Textebene angeben, das über dem gesamten Sitzungsbildschirm angezeigt wird, ohne den Inhalt des Originaldokuments zu ändern.

> **Wichtig:**
>
> Textbasierte Sitzungswasserzeichen sind keine Sicherheitsfunktion. Die Lösung verhindert Datendiebstahl nicht vollständig, bietet aber ein gewisses Maß an Abschreckung und Nachverfolgbarkeit. Wir garantieren keine vollständige Nachverfolgbarkeit von Informationen bei Verwendung dieser Funktion. Wir empfehlen jedoch, diese Funktion gegebenenfalls mit anderen Sicherheitslösungen zu kombinieren.

> Das Sitzungswasserzeichen ist Text und wird auf die dem Benutzer bereitgestellte Sitzung angewendet. Das Sitzungswasserzeichen enthält Informationen zur Nachverfolgung von Datendiebstahl. Die wichtigsten Daten sind die Identität des angemeldeten Benutzers der aktuellen Sitzung, in der der Screenshot erstellt wurde. Um Datenlecks effektiver

> nachzuverfolgen, fügen Sie weitere Informationen hinzu, wie z. B. die Internetprotokolladresse des Servers oder Clients und eine Verbindungszeit.

Um die Benutzererfahrung anzupassen, verwenden Sie die Richtlinieneinstellungen für Sitzungswasserzeichen, um die Platzierung und das Erscheinungsbild des Wasserzeichens auf dem Bildschirm zu konfigurieren.

Einschränkungen

- Sitzungswasserzeichen werden in Sitzungen, in denen die Browserinhaltsumleitung verwendet wird, nicht unterstützt. Um die Sitzungswasserzeichenfunktion zu verwenden, stellen Sie sicher, dass die Browserinhaltsumleitung deaktiviert ist.
- Sitzungswasserzeichen werden nicht unterstützt und erscheinen nicht, wenn die Sitzung im Vollbildmodus mit hardwarebeschleunigter H.264- oder H.265-Kodierung mit älteren NVIDIA-Treibern ausgeführt wird (in diesem Fall ist NvCaptureType in der Registrierung auf 2 gesetzt).
- Wasserzeichen sind bei der Sitzungsschattenfunktion nicht sichtbar.
- Wenn Sie die Drucktaste drücken, um einen Bildschirm aufzunehmen, enthält der auf der VDA-Seite aufgenommene Bildschirm die Wasserzeichen nicht. Wir empfehlen Ihnen, Maßnahmen zu ergreifen, um das Kopieren von Bildschirmaufnahmen zu vermeiden.

Smartcard-Unterstützung

Sie können eine mit dem Clientgerät verbundene Smartcard zur Authentifizierung bei der Anmeldung an einer virtuellen Linux-Desktopsitzung verwenden. Diese Funktion wird durch Smartcard-Umleitung über den virtuellen ICA® Smartcard-Kanal implementiert. Sie können die Smartcard auch innerhalb der Sitzung verwenden. Anwendungsfälle sind das Hinzufügen einer digitalen Signatur zu einem Dokument, das Verschlüsseln oder Entschlüsseln einer E-Mail und die Authentifizierung bei einer Website, die eine Smartcard-Authentifizierung erfordert.

Der Linux VDA verwendet für diese Funktion dieselbe Konfiguration wie der Windows VDA. Weitere Informationen finden Sie im Abschnitt Smartcard-Umgebung konfigurieren in diesem Artikel.

> **Hinweis:**

> Die Verwendung einer zugeordneten Smartcard innerhalb einer Linux VDA-Sitzung zur Anmeldung bei Citrix Gateway wird nicht offiziell unterstützt.

Voraussetzungen

Die Verfügbarkeit der Smartcard-Pass-Through-Authentifizierung ist von den folgenden Bedingungen abhängig:

- Ihr Linux VDA ist auf einer der folgenden Distributionen installiert:
  - RHEL 8/CentOS 8
  - RHEL 7/CentOS 7
  - Ubuntu 20.04
  - Ubuntu 18.04
  - Ubuntu 16.04
  - Debian 10.7

  Nach Abschluss der VDA-Installation überprüfen Sie, ob sich Ihr VDA beim Delivery Controller™ registrieren kann und die veröffentlichten Linux-Desktopsitzungen erfolgreich mit Windows-Anmeldeinformationen gestartet werden können.
- Es werden von OpenSC unterstützte Smartcards verwendet. Weitere Informationen finden Sie unter Sicherstellen, dass OpenSC Ihre Smartcard unterstützt.
- Citrix Workspace™-App für Windows wird verwendet.

Stellen Sie sicher, dass OpenSC Ihre Smartcard unterstützt

OpenSC ist ein weit verbreiteter Smartcard-Treiber unter RHEL 7.4+. Als vollständig kompatibler Ersatz für CoolKey unterstützt OpenSC viele Arten von Smartcards (siehe Smartcard-Unterstützung in Red Hat Enterprise Linux).

In diesem Artikel wird die Smartcard YubiKey 4 als Beispiel zur Veranschaulichung der Konfiguration verwendet. YubiKey 4 ist ein All-in-One-USB-CCID-PIV-Gerät, das einfach bei Amazon oder anderen Einzelhändlern erworben werden kann. Der OpenSC-Treiber unterstützt YubiKey 4.



Wenn Ihr Unternehmen eine andere, fortschrittlichere Smartcard benötigt, bereiten Sie eine physische Maschine mit einer unterstützten Linux-Distribution und dem installierten OpenSC-Paket vor. Informationen zur OpenSC-Installation finden Sie unter Smartcard-Treiber installieren. Legen Sie Ihre Smartcard ein und führen Sie den folgenden Befehl aus, um zu überprüfen, ob OpenSC Ihre Smartcard unterstützt:

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
```

Konfiguration

Root-Zertifikat vorbereiten

Ein Root-Zertifikat wird verwendet, um das Zertifikat auf der Smartcard zu überprüfen. Führen Sie die folgenden Schritte aus, um ein Root-Zertifikat herunterzuladen und zu installieren.

1. Besorgen Sie sich ein Root-Zertifikat im PEM-Format, typischerweise von Ihrem CA-Server.

   Sie können einen ähnlichen Befehl wie den folgenden ausführen, um eine DER-Datei (*.crt, *.cer, *.der) in PEM zu konvertieren. Im folgenden Befehlsbeispiel ist **certnew.cer** eine DER-Datei.

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   ```

2. Installieren Sie das Root-Zertifikat im Verzeichnis `openssl`. Die Datei **certnew.pem** wird als Beispiel verwendet.

   ```
   cp certnew.pem <path where you install the root certificate>
   ```

Um einen Pfad für die Installation des Root-Zertifikats zu erstellen, führen Sie `sudo mdkir -p <path where you install the root certificate>` aus.

Das pam_krb5-Modul unter RHEL 8/CentOS 8 erstellen

Die Smartcard-Authentifizierung hängt vom pam_krb5-Modul ab, das unter RHEL 8/CentOS 8 veraltet ist. Um die Smartcard-Authentifizierung unter RHEL 8/CentOS 8 zu verwenden, erstellen Sie das pam_krb5-Modul wie folgt:

1. Laden Sie den Quellcode pam_krb5-2.4.8-6 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 pam_krb5-Modul unter RHEL 8/CentOS 8.

```
yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools

yum install gcc krb5-devel pam-devel autoconf libtool

rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio –div

tar xvzf pam_krb5-2.4.8.tar.gz

cd pam_krb5-2.4.8

./configure --prefix=/usr

make

make install
```

3. Stellen Sie sicher, dass pam_krb5.so unter /usr/lib64/security/ vorhanden ist.

```
ls -l /usr/lib64/security | grep pam_krb5
```

Smartcard-Umgebung konfigurieren

Sie können das Skript ctxsmartlogon.sh verwenden, um die Smartcard-Umgebung zu konfigurieren, oder die Konfiguration manuell abschließen.

(Option 1) Verwenden Sie das Skript ctxsmartlogon.sh, um die Smartcard-Umgebung zu konfigurieren

Hinweis:

Das Skript ctxsmartlogon.sh fügt PKINIT-Informationen zum Standard-Realm hinzu. Sie können diese Einstellung über die Konfigurationsdatei **/etc/krb5.conf** ändern.

Bevor Sie Smartcards zum ersten Mal verwenden, führen Sie das Skript ctxsmartlogon.sh aus, um die Smartcard-Umgebung zu konfigurieren.

Tipp:

Wenn Sie SSSD für den Domänenbeitritt verwendet haben, starten Sie den SSSD-Dienst neu, nachdem Sie ctxsmartlogon.sh ausgeführt haben.

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

Die Ergebnisse sehen wie folgt aus:

```
#*******************************************************************************
# 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:

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

Die Ergebnisse sehen wie folgt aus:

```
#*******************************************************************************
# 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) Smartcard-Umgebung manuell konfigurieren

Der Linux VDA verwendet dieselbe Smartcard-Umgebung wie der Windows VDA. In dieser Umgebung müssen mehrere Komponenten konfiguriert werden, darunter der Domänencontroller, die Microsoft-Zertifizierungsstelle (CA), die Internet Information Services, Citrix StoreFront und die Citrix Workspace-App. Informationen zur Konfiguration basierend auf der YubiKey 4-Smartcard finden Sie im Knowledge Center-Artikel CTX206156.

Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie sicher, dass alle Komponenten korrekt konfiguriert sind, der private Schlüssel und das Benutzerzertifikat auf die Smartcard heruntergeladen wurden und Sie sich erfolgreich mit der Smartcard am Windows VDA anmelden können.

PC/SC LITE-PAKETE INSTALLIEREN

PCSC Lite ist eine Implementierung der Personal Computer/Smart Card (PC/SC)-Spezifikation unter Linux. Es bietet eine Windows-Smartcard-Schnittstelle für die Kommunikation mit Smartcards und Lesegeräten. Die Smartcard-Umleitung im Linux VDA wird 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/CentOS 8:

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
```

Ubuntu 20.04, Ubuntu 18.04, Ubuntu 16.04, Debian 10.7:

```
apt-get install -y libpcsclite1 libccid
```

SMARTCARD-TREIBER INSTALLIEREN

OpenSC ist ein weit verbreiteter Smartcard-Treiber. Wenn OpenSC nicht installiert ist, führen Sie den folgenden Befehl aus, um es zu installieren:

RHEL 7/CentOS 7, RHEL 8/CentOS 8:

```
yum install opensc
```

Ubuntu 20.04, Ubuntu 18.04, Ubuntu 16.04, Debian 10.7:

```
apt-get install -y opensc
```

PAM-MODULE FÜR DIE SMARTCARD-AUTHENTIFIZIERUNG INSTALLIEREN

Führen Sie den folgenden Befehl aus, um die Module pam_krb5 und krb5-pkinit zu installieren.

RHEL 7/CentOS 7:

```
yum install pam_krb5 krb5-pkinit
```

RHEL 8/CentOS 8:

```
yum install krb5-pkinit
```

Ubuntu 20.04, Ubuntu 18.04, Ubuntu 16.04:

```
apt-get install libpam-krb5 krb5-pkinit
```

Debian 10.7:

```
apt-get install -y libpam-krb5 krb5-pkinit
```

Das pam_krb5-Modul ist ein steckbares Authentifizierungsmodul, das PAM-fähige Anwendungen verwenden können, um Passwörter zu überprüfen und Ticket-Granting-Tickets vom Key Distribution Center (KDC) zu erhalten. Das krb5-pkinit-Modul enthält das PKINIT-Plug-in, das Clients ermöglicht, anfängliche Anmeldeinformationen vom KDC mithilfe eines privaten Schlüssels und eines Zertifikats zu erhalten.

KONFIGURIEREN SIE DAS PAM_KRB5-MODUL

Das pam_krb5-Modul interagiert mit dem KDC, um Kerberos-Tickets mithilfe von Zertifikaten auf der Smartcard zu erhalten. Um die pam_krb5-Authentifizierung in PAM zu aktivieren, führen Sie den folgenden Befehl aus:

```
authconfig --enablekrb5 --update
```

Fügen Sie in der Konfigurationsdatei **/etc/krb5.conf** PKINIT-Informationen entsprechend dem tatsächlichen Realm hinzu.

Hinweis:

Die Option **pkinit_cert_match** gibt Abgleichsregeln an, die das Client-Zertifikat erfüllen muss, bevor es für einen PKINIT-Authentifizierungsversuch verwendet wird. Die Syntax der Abgleichsregeln lautet:

component-rule …

wobei `relation-operator` entweder `&&` sein kann, was bedeutet, dass alle Komponentenregeln übereinstimmen müssen, oder \|\|, was bedeutet, dass nur eine Komponentenregel übereinstimmen muss.

Hier ist ein Beispiel für eine generische krb5.conf-Datei:

```
EXAMPLE.COM = {


    kdc = KDC.EXAMPLE.COM


    auth_to_local = RULE:[1:$1@$0]


    pkinit_anchors = FILE:<path where you install the root certificate>/
certnew.pem

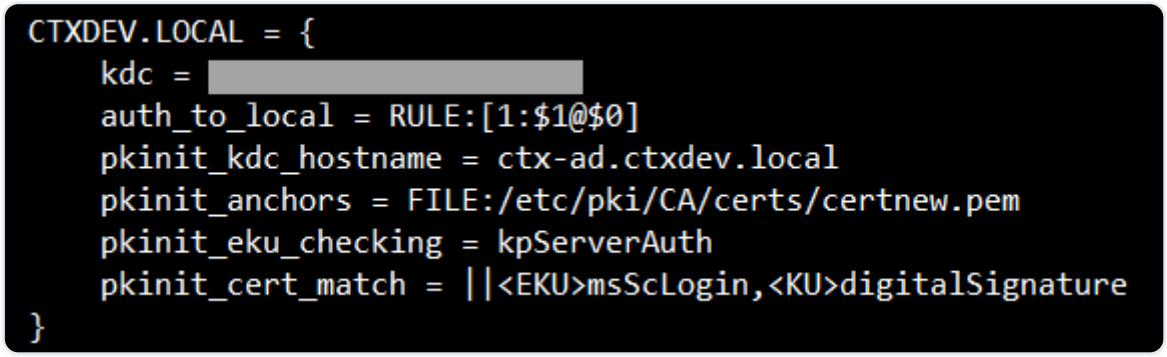

    pkinit_kdc_hostname = KDC.EXAMPLE.COM
```

```
    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature

    pkinit_eku_checking = kpServerAuth

 }
```

Die Konfigurationsdatei sieht wie folgt aus, nachdem Sie die PKINIT-Informationen hinzugefügt haben.



PAM-AUTHENTIFIZIERUNG KONFIGURIEREN

PAM-Konfigurationsdateien geben an, welche Module für die PAM-Authentifizierung verwendet werden. Um pam_krb5 als Authentifizierungsmodul hinzuzufügen, fügen Sie die folgende Zeile zur Datei **/etc/pam.d/smartcard-auth** 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 nach der Änderung wie folgt aus, 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

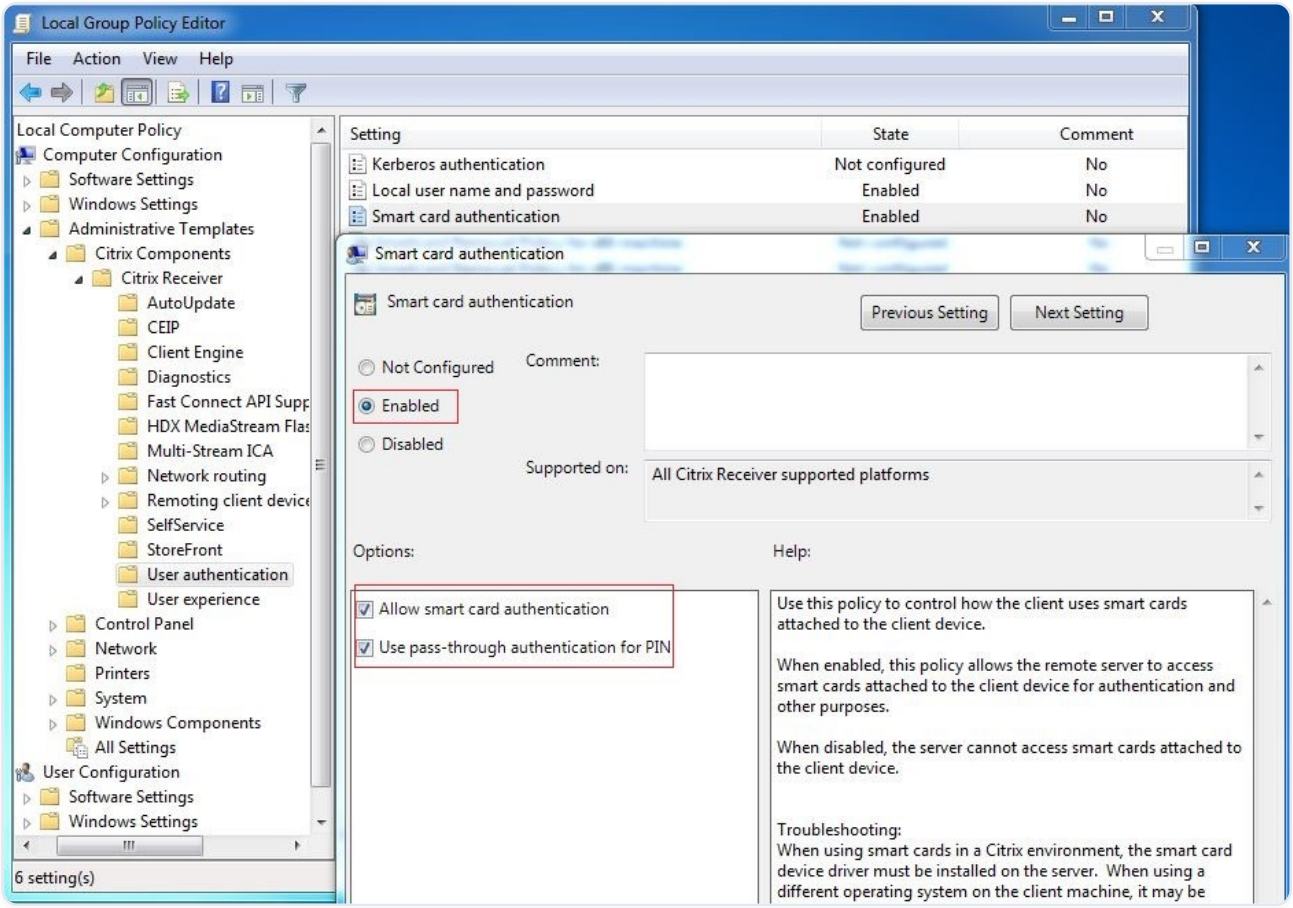
account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
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) Einmaliges Anmelden mithilfe von Smartcards

Single Sign-On (SSO) ist eine Citrix-Funktion, die die Pass-Through-Authentifizierung bei der Bereitstellung von virtuellen Desktops und Anwendungen implementiert. Diese Funktion reduziert die Häufigkeit, mit der Benutzer ihre PIN eingeben müssen. Um SSO mit dem Linux VDA zu verwenden, konfigurieren Sie die Citrix Workspace-App. Die Konfiguration ist dieselbe wie beim Windows VDA. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX133982.

Aktivieren Sie die Smartcard-Authentifizierung wie folgt, wenn Sie die Gruppenrichtlinie in der Citrix Workspace-App konfigurieren.



Schnelle Smartcard-Anmeldung

Die schnelle Smartcard ist eine Verbesserung gegenüber der bestehenden HDX PC/SC-basierten Smartcard-Umleitung. Sie verbessert die Leistung, wenn Smartcards in WAN-Umgebungen mit hoher Latenz verwendet werden. Weitere Informationen finden Sie unter Smartcards.

Der Linux VDA unterstützt schnelle Smartcards in den folgenden Versionen der Citrix Workspace-App:

- Citrix Receiver für Windows 4.12
- Citrix Workspace app 1808 für Windows und höher

Schnelle Smartcard-Anmeldung auf dem Client aktivieren

Die schnelle Smartcard-Anmeldung ist standardmäßig auf dem VDA aktiviert und auf dem Client standardmäßig deaktiviert. Um die schnelle Smartcard-Anmeldung auf dem Client zu aktivieren, fügen Sie den folgenden Parameter in die Datei default.ica der zugehörigen StoreFront-Site ein:

```
[WFClient]

SmartCardCryptographicRedirection=On
```

Schnelle Smartcard-Anmeldung auf dem Client deaktivieren

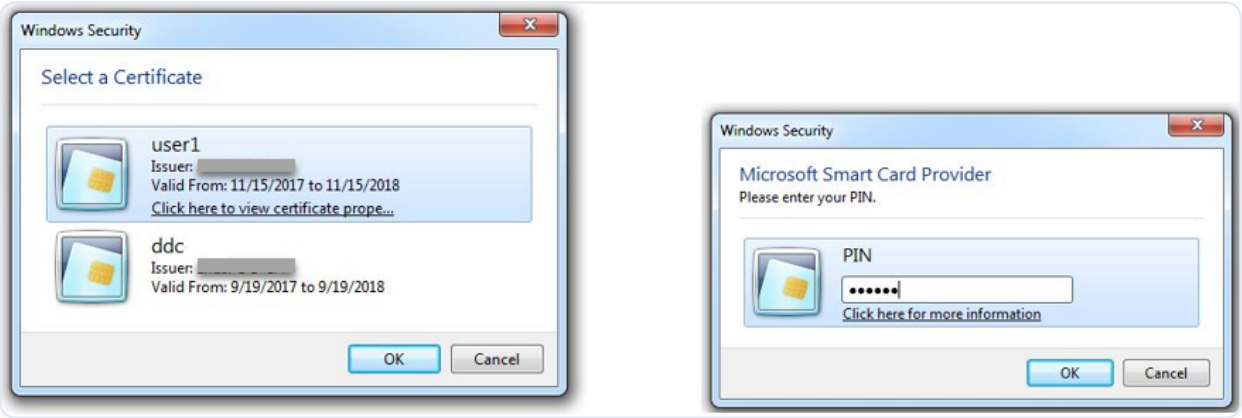
Um die schnelle Smartcard-Anmeldung auf dem Client zu deaktivieren, entfernen Sie den Parameter **SmartCardCryptographicRedirection** aus der Datei default.ica der zugehörigen StoreFront-Site.

Verwendung

Anmeldung am Linux VDA mit einer Smartcard

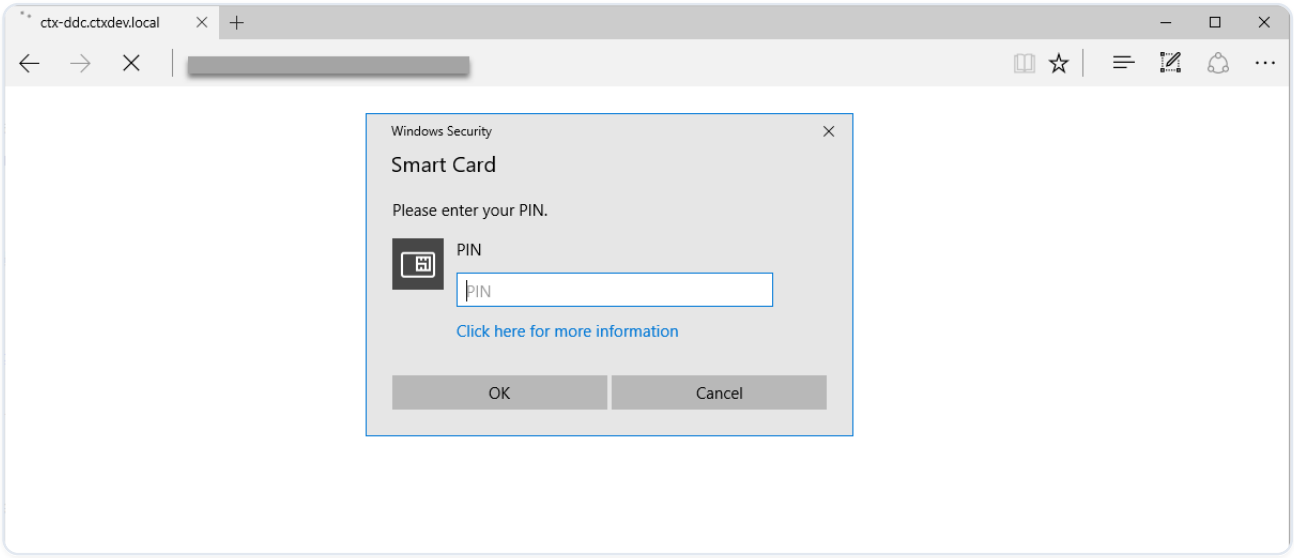
Sie können eine Smartcard verwenden, um sich sowohl in SSO- als auch in Nicht-SSO-Szenarien am Linux VDA anzumelden.

- Im SSO-Szenario melden Sie sich automatisch bei StoreFront™ an, indem Sie das zwischengespeicherte Smartcard-Zertifikat und die PIN verwenden. Wenn Sie eine virtuelle Linux-Desktopsitzung in StoreFront starten, wird die PIN zur Smartcard-Authentifizierung an den Linux VDA übergeben.
- Im Nicht-SSO-Szenario werden Sie aufgefordert, ein Zertifikat auszuwählen und eine PIN einzugeben, um sich bei StoreFront anzumelden.



Wenn Sie eine virtuelle Linux-Desktopsitzung in StoreFront starten, wird ein Dialogfeld für die Anmeldung beim Linux VDA wie folgt angezeigt. Der Benutzername wird aus dem Zertifikat der Smartcard extrahiert, und Sie müssen die PIN erneut für die Anmeldeauthentifizierung eingeben.

Dieses Verhalten ist dasselbe wie beim Windows VDA.



Wiederverbindung mit einer Sitzung mithilfe einer Smartcard

Um die Verbindung zu einer Sitzung wiederherzustellen, stellen Sie sicher, dass die Smartcard mit dem Clientgerät verbunden ist. Andernfalls wird auf der Linux VDA-Seite ein graues Caching-Fenster angezeigt, das schnell wieder verschwindet, da die erneute Authentifizierung ohne angeschlossene Smartcard fehlschlägt. In diesem Fall wird keine weitere Aufforderung angezeigt, die Sie daran erinnert, die Smartcard anzuschließen.

Auf der StoreFront-Seite kann es jedoch vorkommen, dass die StoreFront-Weboberfläche eine Warnung wie folgt anzeigt, wenn keine Smartcard angeschlossen ist, wenn Sie versuchen, die Verbindung zu einer Sitzung wiederherzustellen.



Einschränkung

Smartcard-Entfernungsrichtlinie

Der Linux VDA verwendet jetzt nur noch das Standardverhalten für die Smartcard-Entfernung. Wenn Sie die Smartcard nach erfolgreicher Anmeldung am 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 auf unserer Supportliste aufgeführt ist, können Sie versuchen, andere Smartcards und die PKCS#11-Bibliothek zu verwenden, da Citrix eine generische Smartcard-Umleitungslösung bereitstellt. Um zu Ihrer spezifischen Smartcard oder der PKCS#11-Bibliothek zu wechseln:

1. Ersetzen Sie alle `opensc-pkcs11.so` Instanzen durch Ihre PKCS#11-Bibliothek.
2. Um den Pfad Ihrer PKCS#11-Bibliothek in der Registrierung festzulegen, führen Sie den folgenden Befehl aus:

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v
   "PKCS11LibPath" -d "PATH"
   ```

   wobei **PATH** auf Ihre PKCS#11-Bibliothek verweist, z. B. /usr/lib64/pkcs11/opensc-pkcs11.so
3. Deaktivieren Sie die schnelle Smartcard-Anmeldung auf dem Client.

Double-Hop-Single-Sign-On-Authentifizierung

Die Funktion injiziert Benutzeranmeldeinformationen, die für den Zugriff auf einen StoreFront-Store eingegeben wurden, in das AuthManager-Modul der Citrix Workspace-App für Linux und Citrix Receiver für Linux 13.10. Nach der Injektion können Sie den Client verwenden, um aus einer

virtuellen Linux-Desktopsitzung heraus auf virtuelle Desktops und Anwendungen zuzugreifen, ohne die Benutzeranmeldeinformationen ein zweites Mal eingeben zu müssen.

Hinweis:

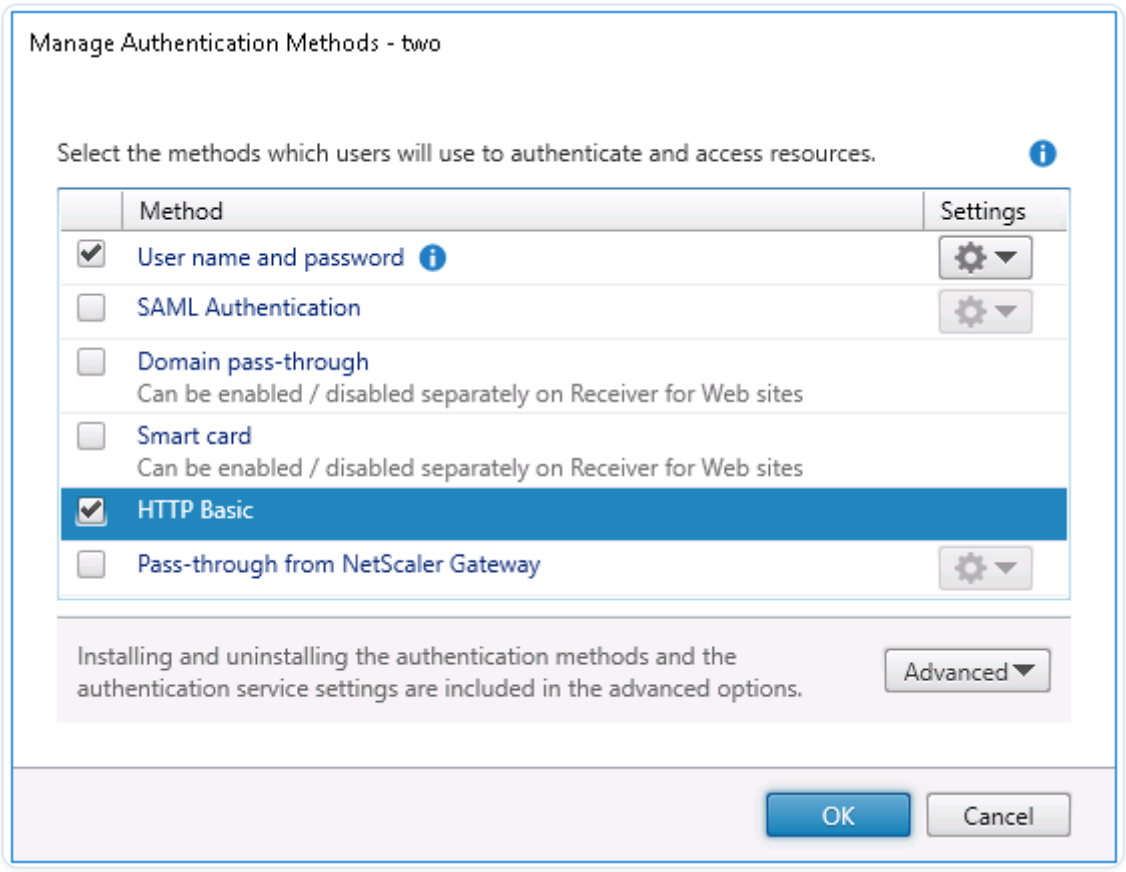
Diese Funktion wird in der Citrix Workspace-App für Linux und Citrix Receiver für Linux 13.10 unterstützt.

So aktivieren Sie die Funktion:

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 die Citrix Workspace-App oder für Citrix Receiver herunter.

   Der Standardinstallationspfad ist /opt/Citrix/ICAClient/. Wenn Sie die App in 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 Authentifizierungsmethode **HTTP Basic** für den Zielstore hinzu.



3. Fügen Sie den folgenden Schlüssel zur AuthManager-Konfigurationsdatei ($ICAROOT/config/AuthManConfig.xml) hinzu, um die HTTP-Basic-Authentifizierung zuzulassen:

```
<Protocols>

     <HTTPBasic>

         <Enabled>True</Enabled>

    </HTTPBasic>

</Protocols>
```

4. Führen Sie die folgenden Befehle aus, um das Stammzertifikat im angegebenen Verzeichnis zu installieren.

```
cp rootcert.pem $ICAROOT/keystore/cacerts/

$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
```

5. Führen Sie den folgenden Befehl aus, um die Funktion zu aktivieren:

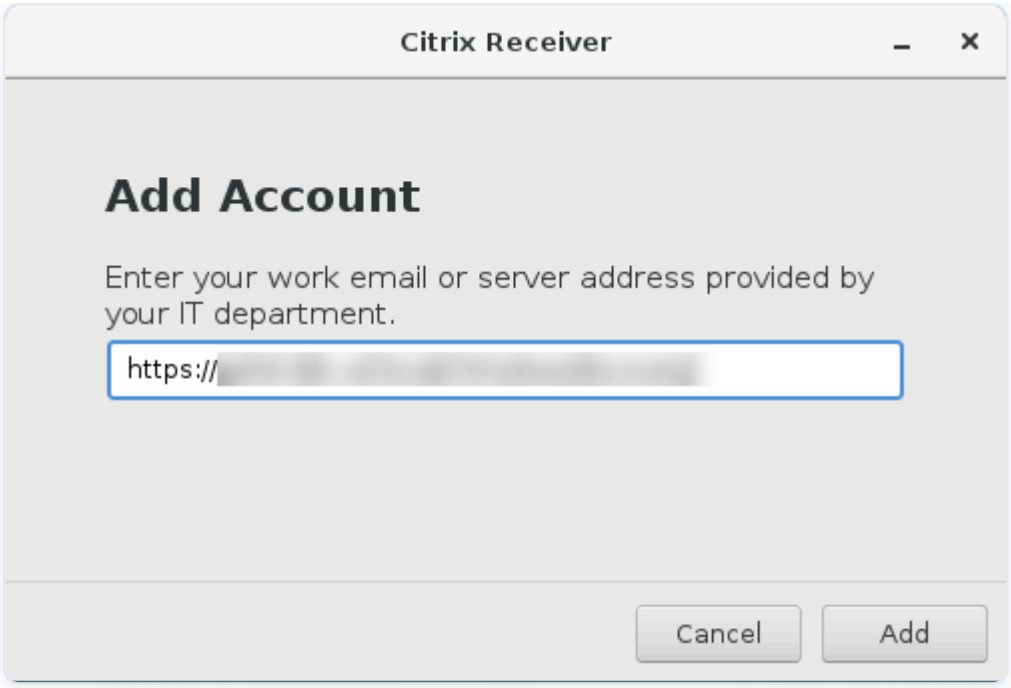
```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d
"0x00000001"
```

6. Starten Sie eine virtuelle Linux-Desktopsitzung und starten Sie die Citrix Workspace-App für Linux oder Citrix Receiver für Linux 13.10 in dieser Sitzung.

   Sie werden zur Eingabe eines Store-Kontos aufgefordert, wenn Sie die Citrix Workspace-App für Linux oder Citrix Receiver für Linux 13.10 zum ersten Mal innerhalb einer virtuellen Linux-Desktopsitzung starten. Später werden Sie automatisch bei dem zuvor angegebenen Store angemeldet.

   Hinweis:

   Geben Sie eine HTTPS-URL als Ihr Store-Konto ein.



Nicht authentifizierte Sitzungen konfigurieren

Verwenden Sie die Informationen in diesem Artikel, um nicht authentifizierte Sitzungen zu konfigurieren. Für die Installation des Linux VDA zur Nutzung dieser Funktion sind keine speziellen Einstellungen erforderlich.

> **Hinweis:**

> Beachten Sie bei der Konfiguration nicht authentifizierter Sitzungen, dass das Vorabstarten von Sitzungen nicht unterstützt wird. Das Vorabstarten von Sitzungen wird auch in der Citrix Workspace™-App für Android nicht unterstützt.

Nicht authentifizierten Store erstellen

Um eine nicht authentifizierte Sitzung auf dem Linux VDA zu unterstützen, (/de-de/storefront/current-release/configure-manage-stores/create-store-unauthenticated.html) erstellen Sie einen nicht authentifizierten Store mit StoreFront.

Nicht authentifizierte Benutzer in einer Bereitstellungsgruppe aktivieren

Nachdem Sie einen nicht authentifizierten Store erstellt haben, aktivieren Sie nicht authentifizierte Benutzer in einer Bereitstellungsgruppe, um eine nicht authentifizierte Sitzung zu unterstützen. Befolgen Sie zum Aktivieren nicht authentifizierter Benutzer in einer Bereitstellungsgruppe die Anweisungen in der (/de-de/citrix-virtual-apps-desktops/install-configure/delivery-groups-create.html).

Leerlaufzeit für nicht authentifizierte Sitzungen festlegen

Eine nicht authentifizierte Sitzung hat eine Standard-Leerlaufzeitüberschreitung von 10 Minuten. Dieser Wert wird über die Registrierungseinstellung **AnonymousUserIdleTime** konfiguriert. Verwenden Sie das Tool **ctxreg**, um diesen Wert zu ändern. Beispiel: Um diese Registrierungseinstellung auf fünf Minuten festzulegen:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime
 -d 0x00000005
```

Maximale Anzahl nicht authentifizierter Benutzer festlegen

Um die maximale Anzahl nicht authentifizierter Benutzer festzulegen, verwenden Sie den Registrierungsschlüssel **MaxAnonymousUserNumber**. Diese Einstellung begrenzt die Anzahl der nicht authentifizierten Sitzungen, die gleichzeitig auf einem einzelnen Linux VDA ausgeführt werden. Verwenden Sie das Tool **ctxreg**, um diese Registrierungseinstellung zu konfigurieren. Beispiel: Um den Wert auf 32 festzulegen:

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

Wichtig:

Begrenzen Sie die Anzahl der nicht authentifizierten Sitzungen. Zu viele gleichzeitig gestartete Sitzungen können Probleme auf dem VDA verursachen, einschließlich eines Mangels an verfügbarem Speicher.

Problembehandlung

Beachten Sie bei der Konfiguration nicht authentifizierter Sitzungen Folgendes:

- **Fehler beim Anmelden an einer nicht authentifizierten Sitzung**.

Stellen Sie sicher, dass die Registrierung aktualisiert wurde, um Folgendes (auf 0 gesetzt) aufzunehmen:

```
sudo /opt/Citrix/VDA/bin/ctxreg read –k
"HKLM\System\CurrentControlSet\Control\Citrix" –v MaxAnonymousUserNumber
```

Stellen Sie sicher, dass der **ncsd**-Dienst ausgeführt wird und so konfiguriert ist, dass er den **passwd**-Cache aktiviert:

```
ps  uax | grep nscd

cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```

Setzen Sie die **passwd**-Cache-Variable auf **no**, falls sie aktiviert ist, und starten Sie dann den **ncsd**-Dienst neu. Möglicherweise müssen Sie den Linux VDA nach dem Ändern dieser Konfiguration neu installieren.

- **Die Bildschirmsperrtaste wird in einer nicht authentifizierten Sitzung mit KDE angezeigt**.

Die Bildschirmsperrtaste und das Menü sind in einer nicht authentifizierten Sitzung standardmäßig deaktiviert. Sie können jedoch weiterhin in KDE angezeigt werden. Um in KDE die Bildschirmsperrtaste und das Menü für einen bestimmten Benutzer zu deaktivieren, fügen Sie die

folgenden Zeilen zur Konfigurationsdatei **$Home/.kde/share/config/kdeglobals** hinzu. Zum Beispiel:

```
[KDE Action Restrictions]

action/lock_screen=false
```

Wenn der `KDE Action Restrictions`-Parameter 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.

Um dieses Problem zu beheben, ändern Sie die systemweite `kdeglobals`-Datei, um das `[$i]`-Tag im Abschnitt `[KDE Action Restrictions]` zu entfernen, oder verwenden Sie direkt die systemweite Konfiguration, um die Bildschirmsperrtaste und das Menü zu deaktivieren. Weitere Informationen zur KDE-Konfiguration finden Sie auf der KDE System Administration/Kiosk/Keys-Seite.

LDAPS konfigurieren

Sicheres LDAP (LDAPS) ermöglicht es Ihnen, das Secure Lightweight Directory Access Protocol für Ihre von Active Directory verwalteten Domänen zu aktivieren, um die Kommunikation über SSL (Secure Socket Layer)/TLS (Transport Layer Security) bereitzustellen.

Standardmäßig sind LDAP-Kommunikationen zwischen Client- und Serveranwendungen nicht verschlüsselt. LDAP mit SSL/TLS (LDAPS) ermöglicht es Ihnen, den Inhalt der LDAP-Abfragen zwischen dem Linux VDA und den LDAP-Servern zu schützen.

Die folgenden Linux VDA-Komponenten haben Abhängigkeiten von LDAPS:

- Broker-Agent: Linux VDA-Registrierung bei einem Delivery Controller™
- Richtliniendienst: Richtlinienauswertung

Das Konfigurieren von LDAPS umfasst:

- LDAPS auf dem Active Directory (AD)/LDAP-Server aktivieren
- Die Stammzertifizierungsstelle (Root CA) für die Client-Nutzung exportieren
- LDAPS auf dem Linux VDA aktivieren/deaktivieren
- LDAPS für Drittanbieterplattformen konfigurieren
- SSSD konfigurieren

- Winbind konfigurieren
- Centrify konfigurieren
- Quest konfigurieren

Hinweis:

Sie können den folgenden Befehl ausführen, um einen Überwachungszyklus für Ihre LDAP-Server festzulegen. Der Standardwert ist 15 Minuten. Stellen Sie ihn auf mindestens 10 Minuten ein.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v
"ListOfLDAPServersMonitorPeroid" -t "REG_DWORD" -d "0x0000000f" --
force
```

LDAPS auf dem AD-/LDAP-Server aktivieren

Sie können LDAP über SSL (LDAPS) aktivieren, indem Sie ein ordnungsgemäß formatiertes Zertifikat von einer Microsoft-Zertifizierungsstelle (CA) oder einer Nicht-Microsoft-CA installieren.

Tipp:

LDAP über SSL/TLS (LDAPS) wird automatisch aktiviert, wenn Sie eine Enterprise-Stamm-CA auf einem Domänencontroller installieren.

Weitere Informationen zur Installation des Zertifikats und zur Überprüfung der LDAPS-Verbindung finden Sie unter How to enable LDAP over SSL with a third-party certification authority auf der Microsoft Support-Website.

Wenn Sie eine mehrstufige (z. B. zweistufige oder dreistufige) Zertifizierungsstellenhierarchie haben, verfügen Sie nicht automatisch über das entsprechende Zertifikat für die LDAPS-Authentifizierung auf dem Domänencontroller.

Informationen zum Aktivieren von LDAPS für Domänencontroller, die eine mehrstufige Zertifizierungsstellenhierarchie verwenden, finden Sie im Artikel LDAP over SSL (LDAPS) Certificate auf der Microsoft TechNet-Website.

Stammzertifizierungsstelle für die Clientnutzung aktivieren

Der Client muss ein Zertifikat von einer CA verwenden, der der LDAP-Server vertraut. Um die LDAPS-Authentifizierung für den Client zu aktivieren, importieren Sie das Stamm-CA-Zertifikat in einen vertrauenswürdigen Schlüsselspeicher.

Weitere Informationen zum Exportieren der Stamm-CA finden Sie unter How to export Root Certification Authority Certificate auf der Microsoft Support-Website.

LDAPS auf dem Linux VDA aktivieren oder deaktivieren

Um LDAPS auf dem Linux VDA zu aktivieren oder zu deaktivieren, führen Sie das folgende Skript aus (als Administrator angemeldet):

Die Syntax für diesen Befehl umfasst Folgendes:

- LDAP über SSL/TLS mit dem bereitgestellten Stamm-CA-Zertifikat aktivieren:

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

- LDAP über SSL/TLS mit Kanalbindung aktivieren:

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

> **Hinweis:**
>
> Das Stamm-CA-Zertifikat für die Kanalbindung muss im PEM-Format vorliegen. Wenn die Aktivierung von LDAPS keine Python3-virtuelle Umgebung erfolgreich erstellt, erstellen Sie diese manuell gemäß den Anweisungen unter Create a Python3 virtual environment.
>
> 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
```

- Rückgriff auf LDAP ohne SSL/TLS

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

Der für LDAPS dedizierte Java-Keystore befindet sich in **/etc/xdl/.keystore**. Betroffene Registrierungsschlüssel sind:

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore

HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
```

LDAPS für Drittanbieterplattform konfigurieren

Neben den Linux-VDA-Komponenten benötigen möglicherweise auch mehrere Drittanbieter-Softwarekomponenten, die dem VDA entsprechen, sicheres LDAP, wie SSSD, Winbind, Centrify und Quest. Die folgenden Abschnitte beschreiben, wie sicheres LDAP mit LDAPS, STARTTLS oder SASL Sign and Seal konfiguriert wird.

> **Tipp:**

> Nicht alle dieser Softwarekomponenten bevorzugen die Verwendung von SSL-Port 636, um sicheres LDAP zu gewährleisten. Und meistens kann LDAPS (LDAP über SSL auf Port 636) nicht mit STARTTLS auf Port 389 koexistieren.

SSSD

Konfigurieren Sie den sicheren LDAP-Verkehr von SSSD auf Port 636 oder Port 389 gemäß den Optionen. Weitere Informationen finden Sie auf der SSSD LDAP Linux-Manpage.

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). Ändern Sie die Dateien wie folgt:

- smb.conf

  `ldap ssl = start tls`

  `ldap ssl ads = yes` `client ldap sasl wrapping = plain`

- ldap.conf

  `TLS_REQCERT never`

Alternativ kann sicheres LDAP durch SASL GSSAPI Sign and Seal konfiguriert werden, es kann jedoch nicht mit TLS/SSL koexistieren. Um die SASL-Verschlüsselung zu verwenden, ändern Sie die **smb.conf**-Konfiguration:

`ldap ssl = off`

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

Centrify

Centrify unterstützt LDAPS auf Port 636 nicht. Es bietet jedoch eine sichere Verschlüsselung auf Port 389. Weitere Informationen finden Sie auf der Centrify-Website.

Quest

Quest Authentication Service unterstützt LDAPS auf Port 636 nicht, bietet aber eine sichere Verschlüsselung auf Port 389 mit einer anderen Methode.

Problembehandlung

Die folgenden Probleme können bei der Verwendung dieser Funktion auftreten:

- **LDAPS-Dienstverfügbarkeit**

  Stellen Sie sicher, dass die LDAPS-Verbindung auf dem AD/LDAP-Server verfügbar ist. Der Port ist standardmäßig auf 636 eingestellt.

- **Linux VDA-Registrierung fehlgeschlagen, wenn LDAPS aktiviert ist**

  Stellen Sie sicher, dass der LDAP-Server und die Ports korrekt konfiguriert sind. Überprüfen Sie zuerst das Root-CA-Zertifikat und stellen Sie sicher, dass es mit dem AD/LDAP-Server übereinstimmt.

- **Versehentliche Änderung der Registrierung**

  Wenn die LDAPS-bezogenen Schlüssel versehentlich ohne Verwendung von **enable_ldaps.sh** aktualisiert wurden, könnte dies die Abhängigkeit der LDAPS-Komponenten beeinträchtigen.

- **LDAP-Datenverkehr wird nicht über SSL/TLS von Wireshark oder anderen Netzwerküberwachungstools verschlüsselt**

  Standardmäßig ist LDAPS deaktiviert. Führen Sie **/opt/Citrix/VDA/sbin/enable_ldaps.sh** aus, um es zu erzwingen.

- **Kein LDAPS-Datenverkehr von Wireshark oder anderen Netzwerküberwachungstools**

  LDAP-/LDAPS-Datenverkehr tritt bei der Linux VDA-Registrierung und der Auswertung von Gruppenrichtlinien auf.

- **Fehler beim Überprüfen der LDAPS-Verfügbarkeit durch Ausführen von ldp connect auf dem AD-Server**

  Verwenden Sie den AD FQDN anstelle der IP-Adresse.

- **Fehler beim Importieren des Stammzertifikats der Zertifizierungsstelle durch Ausführen des Skripts /opt/Citrix/VDA/sbin/enable_ldaps.sh**

  Geben Sie den vollständigen Pfad des CA-Zertifikats an und überprüfen Sie, ob das Stammzertifikat der Zertifizierungsstelle der richtige Typ ist. Es sollte mit den meisten

unterstützten Java Keytool-Typen kompatibel sein. Wenn es nicht in der Supportliste aufgeführt ist, können Sie den Typ zuerst konvertieren. Wir empfehlen das base64-kodierte PEM-Format, wenn Sie ein Problem mit dem Zertifikatsformat haben.

- **Fehler beim Anzeigen des Stammzertifikats der Zertifizierungsstelle mit Keytool -list**

  Wenn Sie LDAPS durch Ausführen von `/opt/Citrix/VDA/sbin/enable_ldaps.sh` aktivieren, wird das Zertifikat nach /etc/xdl/.keystore importiert und das Kennwort zum Schutz des Keystores festgelegt. Wenn Sie das Kennwort vergessen, können Sie das Skript erneut ausführen, um einen Keystore zu erstellen.

Erstellen einer Python3-virtuellen Umgebung

Wenn Sie mit dem Netzwerk verbunden sind, kann die Ausführung des Befehls `sudo /opt/Citrix/VDA/bin/xdping` oder `/opt/Citrix/VDA/sbin/enable_ldaps.sh` eine Python3-virtuelle Umgebung erstellen. Wenn die Befehle jedoch keine Python3-virtuelle Umgebung erstellen können, können Sie diese manuell erstellen, auch ohne Netzwerkverbindung. Dieser Artikel beschreibt die Voraussetzungen und Schritte zum Erstellen einer Python3-virtuellen Umgebung ohne Netzwerkverbindung.

Voraussetzungen

- Sie müssen über Administratorrechte verfügen, um auf das Verzeichnis `/opt/Citrix/VDA/sbin/ctxpython3` zugreifen zu können.
- Die Wheel-Dateien der `Python3`-Pakete sind vorhanden. Sie können die Wheel-Dateien von `<https://pypi.org/>` herunterladen.

Erstellen einer Python3-virtuellen Umgebung

Führen Sie die folgenden Schritte aus, um eine Python3-virtuelle Umgebung zu erstellen:

1. Installieren Sie Python3-Abhängigkeiten.

   Für RHEL:

   ```
   yum -y install python36-devel krb5-devel gcc
   ```

   Hinweis:

> Möglicherweise müssen Sie ein bestimmtes Repository aktivieren, um einige Abhängigkeiten zu installieren. Führen Sie für RHEL 7 den Befehl `subscription-manager repos --enable rhel-7-server-optional-rpms` aus. Führen Sie für RHEL 8 den Befehl `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms` aus.

> **Für Ubuntu\Debian:**

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
```

Für SUSE:

```
zypper -i -n install python3-devel python3-setuptools krb5-devel gcc libffi48-devel
```

> **Hinweis:**

> Möglicherweise müssen Sie das Repository `SUSE_Linux_Enterprise_Software_Development_Kit_12_SP5_x86_64` aktivieren, um einige Abhängigkeiten zu installieren.

2. Erstellen Sie eine Python3-virtuelle 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 RHEL, Ubuntu, Debian:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

Für SUSE:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
setuptools==40.6.2
```

3. LDAPS-Abhängigkeiten installieren.

   Für RHEL, Ubuntu, Debian:

   ```
   sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install cffi ==
   1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi==1.6.2
   ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0 psutil == 5.8.0
   pyasn1 == 0.4.8 pycparser == 2.20 scramp == 1.2.0 six == 1.15.0
   termcolor == 1.1.0
   ```

   Für SUSE:

   ```
   sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install cffi
   == 1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi==1.6.2
   ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0 psutil == 5.8.0
   pyasn1 == 0.4.8 pycparser == 2.20 scramp == 1.2.0 six == 1.15.0
   termcolor == 1.1.0
   ```

4. `XDPing`-Abhängigkeiten installieren.

   Für RHEL, Ubuntu, Debian:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install cffi ==
1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi==1.6.2
ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0 psutil == 5.8.0
pyasn1 == 0.4.8 pycparser == 2.20 scramp == 1.2.0 six == 1.15.0
termcolor == 1.1.0



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /opt/
Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

Für SUSE:

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install cffi
== 1.14.2 cryptography == 3.1 decorator == 4.4.2 gssapi==1.6.2
ldap3==2.8.1 netifaces == 0.10.9 pg8000 == 1.17.0 psutil == 5.8.0
pyasn1 == 0.4.8 pycparser == 2.20 scramp == 1.2.0 six == 1.15.0
termcolor == 1.1.0



sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m easy_install /opt/
Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
```

XDPing

Beschreibung

Das Linux XDPing-Tool ist eine Befehlszeilenanwendung, die den Prozess der Überprüfung auf häufige Konfigurationsprobleme in einer Linux VDA-Umgebung automatisiert.

Das Linux XDPing-Tool führt über 150 einzelne Tests am System aus, die grob wie folgt kategorisiert werden:

- Überprüfen, ob die Systemanforderungen für Linux VDA erfüllt sind
- Maschineninformationen identifizieren und anzeigen, einschließlich der Linux-Distributionen
- Überprüfen der Linux-Kernel-Kompatibilität
- Auf bekannte Probleme mit Linux-Distributionen prüfen, die den Betrieb des Linux VDA beeinträchtigen können

- Überprüfen des Security-Enhanced Linux (SELinux)-Modus und der Kompatibilität
- Netzwerkschnittstellen identifizieren und Netzwerkeinstellungen überprüfen
- Speicherpartitionierung und verfügbaren Speicherplatz überprüfen
- Maschinen-Host- und Domänennamenkonfiguration überprüfen
- DNS-Konfiguration überprüfen und Lookup-Tests durchführen
- Zugrunde liegende Hypervisoren identifizieren und die Konfiguration der virtuellen Maschine überprüfen. Unterstützung für:
  - Citrix Hypervisor™
  - Microsoft HyperV
  - VMware vSphere
- Zeiteinstellungen überprüfen und überprüfen, ob die Netzwerkzeitsynchronisierung funktioniert
- Überprüfen, ob der PostgreSQL-Dienst ordnungsgemäß konfiguriert und betriebsbereit ist
- Überprüfen, ob die Firewall aktiviert und die erforderlichen Ports geöffnet sind
- Kerberos-Konfiguration überprüfen und Authentifizierungstests durchführen
- Die LDAP-Suchumgebung für die Gruppenrichtlinien-Dienst-Engine überprüfen
- Überprüfen, ob die Active Directory-Integration ordnungsgemäß eingerichtet ist und der aktuelle Computer der Domäne beigetreten ist. Unterstützung für:
  - Samba Winbind
  - Dell Quest Authentication Services
  - Centrify DirectControl
  - SSSD
- Die Integrität des Linux-Computerobjekts in Active Directory überprüfen
- Die Konfiguration des Pluggable Authentication Module (PAM) überprüfen
- Das Core-Dump-Muster überprüfen
- Überprüfen, ob die vom Linux VDA benötigten Pakete installiert sind
- Das Linux VDA-Paket identifizieren und die Integrität der Installation überprüfen
- Die Integrität der PostgreSQL-Registrierungsdatenbank überprüfen
- Überprüfen Sie, ob die Linux VDA-Dienste ordnungsgemäß konfiguriert und betriebsbereit sind.
- Überprüfen Sie die Integrität der VDA- und HDX™-Konfiguration.

- Jeden konfigurierten Delivery Controller™ abfragen, um zu testen, ob der Broker-Dienst erreichbar, betriebsbereit und reaktionsfähig ist.
- Überprüfen Sie, ob die Maschine bei der Delivery Controller-Farm registriert ist.
- Überprüfen Sie den Status jeder aktiven oder getrennten HDX-Sitzung.
- Protokolldateien nach Linux VDA-bezogenen Fehlern und Warnungen durchsuchen.
- Überprüfen Sie, ob die Xorg-Version geeignet ist.

Verwenden Sie das Linux XDPing-Tool

> **Hinweis:**

> Das Ausführen von ctxsetup.sh installiert XDPing nicht. Sie können `sudo /opt/Citrix/VDA/bin/xdping` ausführen, um XDPing zu installieren. Dieser Befehl erstellt auch eine virtuelle Python3-Umgebung, die für XDPing erforderlich ist. Wenn dieser Befehl keine virtuelle Python3-Umgebung erstellen kann, erstellen Sie sie manuell gemäß den Anweisungen unter Create a Python3 virtual environment.

> Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des pip-Tools auftreten können, ziehen Sie in Betracht, die folgenden vertrauenswürdigen Hosts zur Datei /etc/pip.conf hinzuzufügen:

> `[global]` `trusted-host =`

> `pypi.org` `files.pythonhosted.org`

> XDPing wird mit der einzelnen ausführbaren Datei namens `xdping` geliefert, die über die Befehlsshell ausgeführt wird.

Um die Befehlszeilenoptionen anzuzeigen, verwenden Sie die Option `--help`:

```
sudo /opt/Citrix/VDA/bin/xdping --help
```

Um die vollständige Testsuite auszuführen, führen Sie `xdping` ohne Befehlszeilenoptionen aus:

```
sudo /opt/Citrix/VDA/bin/xdping
```

Um die Umgebung vor der Installation des Linux VDA-Pakets zu überprüfen, führen Sie die `pre-flight`-Tests aus:

```
sudo /opt/Citrix/VDA/bin/xdping --preflight
```

Um nur bestimmte Testkategorien auszuführen, zum Beispiel die Zeit- und Kerberos-Tests, verwenden Sie die Option `-T`:

```
sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos
```

So testen Sie einen bestimmten XenDesktop® Controller:

```
sudo /opt/Citrix/VDA/bin/xdping -d myddc.domain.net
```

Beispielausgabe

Im Folgenden sehen Sie eine Beispielausgabe des 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$@X          ]: [MISSING]
  SPN system key [host/m                  l]: [Exists]
    Verify Kerberos system keys for UPN exist                            [ERROR]
    No system keys were found for the user principal name (UPN) of
    the machine account. For the Linux VDA to mutually authenticate
    with the Delivery Controller, the system keytab file must
    contain keys for both the UPN and host-based SPN of the machine
    account.
```

```
        Verify Kerberos system keys for SPN exist                    [Pass]
      Kerberos login: [FAILED AUTHENTICATION]
                      Keytab contains no suitable keys for MYVDA1$@[redacted]
                      while getting initial credentials
        Verify KDC authentication                                    [ERROR]
        Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
        from the KDC authentication service for the machine account UPN
        MYVDA1$@[redacted]. 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]
```

Xauthority konfigurieren

Der Linux VDA unterstützt Umgebungen, die X11-Anzeigefunktionen (einschließlich `xterm` und `gvim`) für die interaktive Fernsteuerung verwenden. Diese Funktion bietet einen Sicherheitsmechanismus, der für eine sichere Kommunikation zwischen XClient und XServer erforderlich ist.

Es gibt zwei Methoden, um die Berechtigung für diese sichere Kommunikation zu gewährleisten:

- **Xhost**. Standardmäßig erlaubt Xhost nur dem localhost XClient, mit dem XServer zu kommunizieren. Wenn Sie einem Remote-XClient den Zugriff auf den XServer erlauben möchten, muss der Befehl Xhost ausgeführt werden, um die Berechtigung auf der spezifischen Maschine zu erteilen. Alternativ können Sie auch **xhost +** verwenden, um jedem XClient die Verbindung zum XServer zu ermöglichen.
- **Xauthority**. Die `.Xauthority`-Datei befindet sich im Home-Verzeichnis jedes Benutzers. Sie wird verwendet, um Anmeldeinformationen in Cookies zu speichern, die von xauth zur Authentifizierung des XServers verwendet werden. Wenn eine XServer-Instanz (Xorg) gestartet wird, wird der Cookie verwendet, um Verbindungen zu dieser spezifischen Anzeige zu authentifizieren.

Funktionsweise

Wenn Xorg startet, wird eine `.Xauthority`-Datei an Xorg übergeben. Diese `.Xauthority`-Datei enthält die folgenden Elemente:

- Anzeigennummer
- Remote-Anforderungsprotokoll
- Cookie-Nummer

Sie können diese Datei mit dem Befehl `xauth` durchsuchen. Zum Beispiel:

```
# xauth -f ~/.Xauthority



# > list



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

Wenn sich ein XClient remote mit dem Xorg verbindet, müssen zwei Voraussetzungen erfüllt sein:

- Setzen Sie die Umgebungsvariable **DISPLAY** auf den Remote-XServer.
- Rufen Sie die `.Xauthority`-Datei ab, die eine der Cookie-Nummern in Xorg enthält.

Xauthority konfigurieren

Um Xauthority auf dem Linux VDA für die Remote-X11-Anzeige zu aktivieren, müssen Sie die folgenden zwei Registrierungsschlüssel erstellen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"XauthEnabled" -d "0x00000001" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"ListenTCP" -d "0x00000001" --force
```

Nach dem Aktivieren von Xauthority übergeben Sie die Datei `.Xauthority` manuell oder durch das Einbinden eines freigegebenen Home-Verzeichnisses an den XClient:

- Übergeben Sie die Datei `.Xauthority` manuell an den XClient.

  Nach dem Starten einer ICA®-Sitzung generiert der Linux VDA die Datei `.Xauthority` für den XClient und speichert die Datei im Home-Verzeichnis des angemeldeten Benutzers. Sie können diese Datei `.Xauthority` auf die Remote-XClient-Maschine kopieren und die Umgebungsvariablen `DISPLAY` und `XAUTHORITY` festlegen. `DISPLAY` ist die in der Datei `.Xauthority`

gespeicherte Anzeigenummer und `XAUTHORITY` ist der Dateipfad von Xauthority. Ein Beispiel finden Sie im folgenden Befehl:

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



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

> **Hinweis:**
>
> Wenn die Umgebungsvariable `XAUTHORITY` nicht festgelegt ist, wird standardmäßig die Datei `~/.Xauthority` verwendet.

- Übergeben Sie die Datei `.Xauthority` an den XClient, indem Sie ein freigegebenes Home-Verzeichnis einbinden.

  Der bequemste Weg ist, ein freigegebenes Home-Verzeichnis für den angemeldeten Benutzer einzubinden. Wenn der Linux VDA eine ICA-Sitzung startet, wird die Datei `.Xauthority` im Home-Verzeichnis des angemeldeten Benutzers erstellt. Wenn dieses Home-Verzeichnis mit dem XClient geteilt wird, muss der Benutzer diese Datei `.Xauthority` nicht manuell an den XClient übertragen. Nachdem die Umgebungsvariablen `DISPLAY` und `XAUTHORITY` korrekt festgelegt wurden, wird die GUI automatisch auf dem XServer-Desktop angezeigt.

Problembehandlung

Wenn Xauthority nicht funktioniert, führen Sie die folgenden Schritte zur Fehlerbehebung aus:

1. Rufen Sie als Administrator mit Root-Rechten alle Xorg-Cookies ab:

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

   Dieser Befehl zeigt den Xorg-Prozess und die beim Starten an Xorg übergebenen Parameter an. Ein weiterer Parameter zeigt an, welche Datei `.Xauthority` verwendet wird. Zum Beispiel:

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

Zeigen Sie die Cookies mit dem Befehl **Xauth** an:

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

2. Verwenden Sie den Befehl `Xauth`, um die in `~/.Xauthority` enthaltenen Cookies anzuzeigen. Für dieselbe Anzeigenummer müssen die angezeigten Cookies in den Dateien `.Xauthority` von Xorg und XClient identisch sein.
3. Wenn die Cookies identisch sind, überprüfen Sie die Erreichbarkeit des Remote-Anzeigeports, indem Sie die IP-Adresse des Linux VDA (z. B. 10.158.11.11) und die Anzeigenummer des veröffentlichten Desktops (z. B. 160) verwenden.

   Führen Sie den folgenden Befehl auf der XClient-Maschine aus:

   ```
   telnet 10.158.11.11 6160
   ```

   Die Portnummer ist die Summe von 6000 + \<Anzeigenummer\>.

   Wenn dieser Telnet-Vorgang fehlschlägt, blockiert möglicherweise die Firewall die Anforderung.

Federated Authentication Service konfigurieren

Der Linux VDA unterstützt die Verwendung von FAS für die Anmeldung bei Ihrer Citrix Virtual Apps and Desktops-Umgebung. Er verwendet dieselbe Windows-Umgebung wie der Windows VDA für die FAS-Anmeldefunktion. Informationen zum Konfigurieren der Windows-Umgebung für FAS finden Sie unter Federated Authentication Service. Dieser Artikel enthält zusätzliche Informationen speziell für den Linux VDA.

Hinweis

Der Linux VDA unterstützt die Richtlinie **In-session Behavior** nicht.

Der Linux VDA verwendet kurze Verbindungen zur Datenübertragung mit FAS-Servern.

FAS auf dem Linux VDA konfigurieren

FAS-Unterstützung unter RHEL 8/CentOS 8

FAS hängt vom pam_krb5-Modul ab, das unter RHEL 8/CentOS 8 veraltet ist. Um FAS unter RHEL 8/CentOS 8 zu verwenden, erstellen Sie das pam_krb5-Modul wie folgt:

1. Laden Sie den pam_krb5-2.4.8-6-Quellcode 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 pam_krb5-Modul unter RHEL 8/CentOS 8.

   ```
   yum install make gcc krb5-devel pam-devel autoconf libtool

   rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div

   tar xvzf pam_krb5-2.4.8.tar.gz

   cd pam_krb5-2.4.8

   ./configure --prefix=/usr

   make

   make install
   ```

3. Vergewissern Sie sich, dass pam_krb5.so unter /usr/lib64/security/ vorhanden ist.

   ```
   ls -l /usr/lib64/security | grep pam_krb5
   ```

FAS-Server festlegen

Geben Sie bei einer Neuinstallation des Linux VDA den FQDN jedes FAS-Servers ein, wenn Sie während der Ausführung von ctxinstall.sh oder ctxsetup.sh nach CTX_XDL_FAS_LIST gefragt werden. Da der Linux VDA keine AD-Gruppenrichtlinien unterstützt, können Sie stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen.

Um eine vorhandene Linux VDA-Installation zu aktualisieren, können Sie `ctxsetup.sh` erneut ausführen, um die FAS-Server festzulegen. Oder Sie können die folgenden Befehle ausführen, um die FAS-Server festzulegen und den Dienst `ctxvda` neu zu starten, damit Ihre Einstellung wirksam wird.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "<Your-FAS-Server-List>" --force



service ctxjproxy restart



service ctxvda restart
```

Um die FAS-Server über `ctxreg` zu aktualisieren, führen Sie die folgenden Befehle aus:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -v "Addresses" -d "<Your-FAS-Server-List>"



service ctxjproxy restart



service ctxvda restart
```

Zertifikate installieren

Zur Überprüfung der Benutzerzertifikate installieren Sie das Stamm-CA-Zertifikat und alle Zwischenzertifikate auf dem VDA. Um beispielsweise das Stamm-CA-Zertifikat zu installieren, rufen Sie das AD-Stammzertifikat aus dem vorhergehenden Schritt **Abrufen des CA-Zertifikats von der Microsoft CA (auf AD)** ab oder laden Sie dessen DER-Format vom Stamm-CA-Server `http://CA-SERVER/certsrv` herunter.

> **Hinweis:**

> Die folgenden Befehle gelten auch für die Konfiguration eines Zwischenzertifikats.

> Konvertieren Sie eine DER-Datei (.crt, .cer, .der) in PEM, indem Sie einen Befehl ähnlich dem folgenden ausführen:

```
sudo openssl x509 -inform der -in root.cer -out root.pem
```

Installieren Sie anschließend das Stamm-CA-Zertifikat im Verzeichnis `openssl`, indem Sie einen Befehl ähnlich dem folgenden ausführen:

```
sudo cp root.pem /etc/pki/CA/certs/
```

> **Hinweis:**

> Legen Sie das Stamm-CA-Zertifikat nicht unter dem Pfad **/root** ab. Andernfalls verfügt FAS nicht über die Leseberechtigung für das Stamm-CA-Zertifikat.

ctxfascfg.sh ausführen

Führen Sie das Skript ctxfascfg.sh aus, um die FAS-Parameter zu konfigurieren:

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

Zwei Umgebungsvariablen werden hinzugefügt, damit `ctxfascfg.sh` im unbeaufsichtigten Modus ausgeführt werden kann:

- **CTX_FAS_ADINTEGRATIONWAY=winbind \| sssd \| centrify** – Bezeichnet die Active Directory-Integrationsmethode, die `CTX_EASYINSTALL_ADINTEGRATIONWAY` entspricht, wenn `CTX_EASYINSTALL_ADINTEGRATIONWAY` angegeben ist. Wenn `CTX_EASYINSTALL_ADINTEGRATIONWAY` nicht angegeben ist, verwendet `CTX_FAS_ADINTEGRATIONWAY` seine eigene Werteinstellung.
- **CTX_FAS_CERT_PATH \=\<certificate path\>** – Gibt den vollständigen Pfad an, der das Stammzertifikat und alle Zwischenzertifikate speichert.

Wählen Sie die richtige Active Directory-Integrationsmethode und geben Sie dann den korrekten Pfad der Zertifikate ein (z. B. `/etc/pki/CA/certs/`).

Das Skript installiert dann die Pakete krb5-pkinit und pam_krb5 und legt die relevanten Konfigurationsdateien fest.

Einschränkung

- FAS unterstützt nur bestimmte Linux-Plattformen und AD-Integrationsmethoden. Siehe folgende Matrix:

	WINBIND	SSSD	CENTRIFY
RHEL 8.3 / CentOS 8.3	Ja	Ja	Ja
RHEL 8.2 / CentOS 8.2	Ja	Ja	Ja
RHEL 8.1 / CentOS 8.1	Ja	Ja	Ja
RHEL 7.9 / CentOS 7.9	Ja	Ja	Ja
RHEL 7.8 / CentOS 7.8	Ja	Ja	Ja
Ubuntu 20.04	Ja	Nein	Ja
Ubuntu 18.04	Ja	Nein	Ja
Ubuntu 16.04	Ja	Nein	Ja
SLES 12.5	Ja	Nein	Ja

- FAS unterstützt den Sperrbildschirm noch nicht. Wenn Sie in einer Sitzung auf die Sperrtaste klicken, können Sie sich nicht erneut mit FAS bei der Sitzung anmelden.
- Diese Version unterstützt nur die gängigen FAS-Bereitstellungen, die im Artikel Architekturübersicht des Federated Authentication Service zusammengefasst sind, und beinhaltet nicht **Windows 10 Azure AD Join**.

Problembehandlung

Bevor Sie Probleme mit FAS beheben, stellen Sie sicher, dass der Linux VDA korrekt installiert und konfiguriert ist, damit eine Nicht-FAS-Sitzung erfolgreich im gemeinsamen Store mit Kennwortauthentifizierung gestartet werden kann.

Wenn Nicht-FAS-Sitzungen ordnungsgemäß funktionieren, setzen Sie die HDX-Protokollstufe der Klasse **Login** auf VERBOSE und die VDA-Protokollstufe auf TRACE. Informationen zum Aktivieren der Ablaufverfolgung für den Linux VDA finden Sie im Knowledge Center-Artikel CTX220130.

FAS-Server-Konfigurationsfehler

Das Starten einer Sitzung aus dem FAS-Speicher schlägt fehl.

Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie nach dem Fehlerprotokoll, das dem folgenden ähnelt:

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon
Type] Federated Authentication Logon.



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start
connect to server 0



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed
to connect: Connection refused.



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed
to connect to server [0], please confirm if fas service list is well
configurated in condb



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit,
43
```

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed
to validate fas credential

2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate:
failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER
```

Lösung

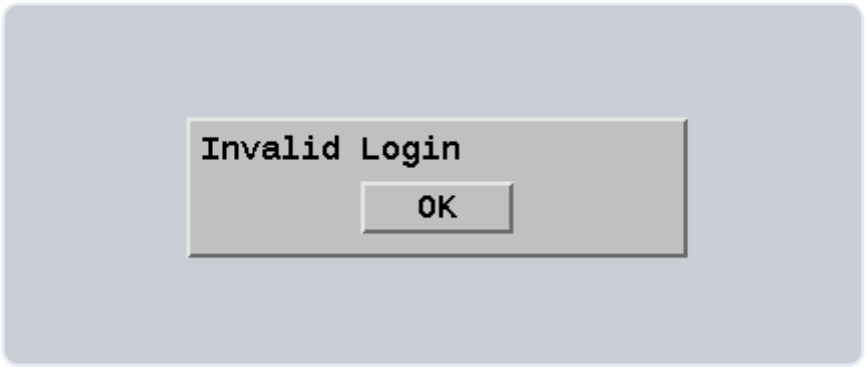
Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Citrix-Registrierungswert „HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\VirtualDesktopAgent\\Authentication\ \UserCredentialService“ auf \<Your-FAS-Server-List\> festgelegt ist.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
```

Wenn die vorhandene Einstellung falsch ist, befolgen Sie den vorhergehenden Schritt FAS-Server festlegen, um sie erneut festzulegen.

Falsche CA-Zertifikatkonfiguration

Das Starten einer Sitzung aus dem FAS-Speicher schlägt fehl. Ein graues Fenster erscheint und verschwindet einige Sekunden später.



Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie nach dem Fehlerprotokoll, das dem folgenden ähnelt:

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: entry
```

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller: current
process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]

2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_public_certificate: entry

2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
for response...

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query to
server success

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
get_public_certificate: exit

2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
input size 1888

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
output size 1415

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: get logon certificate success

2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
cache certificate success
```

```
2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: exit, 0


2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
```

Lösung

Überprüfen Sie, ob der vollständige Pfad, der das Stamm-CA-Zertifikat und alle Zwischenzertifikate speichert, in /etc/krb5.conf korrekt festgelegt ist. Der vollständige Pfad ähnelt dem folgenden:

```
 [realms]


EXAMPLE.COM = {


    ......


    pkinit_anchors = DIR:/etc/pki/CA/certs/


    ......

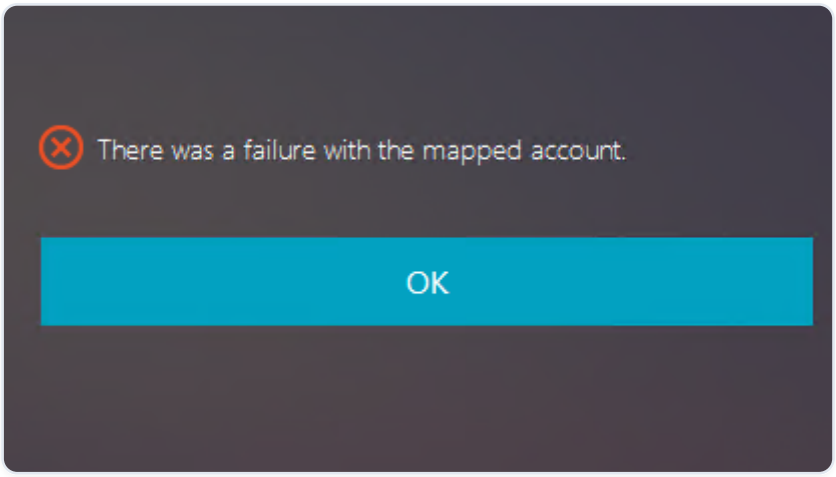

}
```

Wenn die vorhandene Einstellung falsch ist, befolgen Sie den vorhergehenden Schritt Zertifikate installieren, um sie erneut festzulegen.

Überprüfen Sie alternativ, ob das Stamm-CA-Zertifikat gültig ist.

Fehler bei der Zuordnung von Schattenkonten

FAS ist für die SAML-Authentifizierung konfiguriert. Der folgende Fehler kann auftreten, nachdem ein ADFS-Benutzer den Benutzernamen und das Kennwort auf der ADFS-Anmeldeseite eingegeben hat.



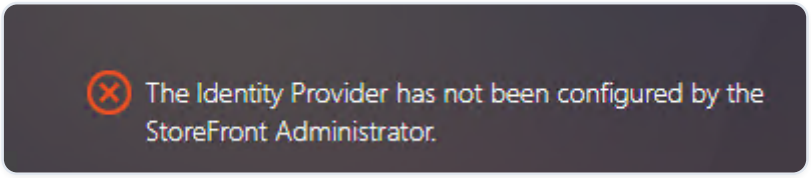
Dieser Fehler weist darauf hin, dass der ADFS-Benutzer erfolgreich überprüft wurde, aber kein Schattenbenutzer in AD konfiguriert ist.

Lösung

Richten Sie das Shadow-Konto in AD ein.

ADFS nicht konfiguriert

Der folgende Fehler tritt bei einem Anmeldeversuch im FAS-Store auf:



Das Problem tritt auf, wenn der FAS-Store für die Verwendung der SAML-Authentifizierung konfiguriert ist, die ADFS-Bereitstellung jedoch fehlt.

Lösung

Stellen Sie den ADFS IdP für den Federated Authentication Service bereit. Weitere Informationen finden Sie unter Bereitstellung von ADFS für den Federated Authentication Service.

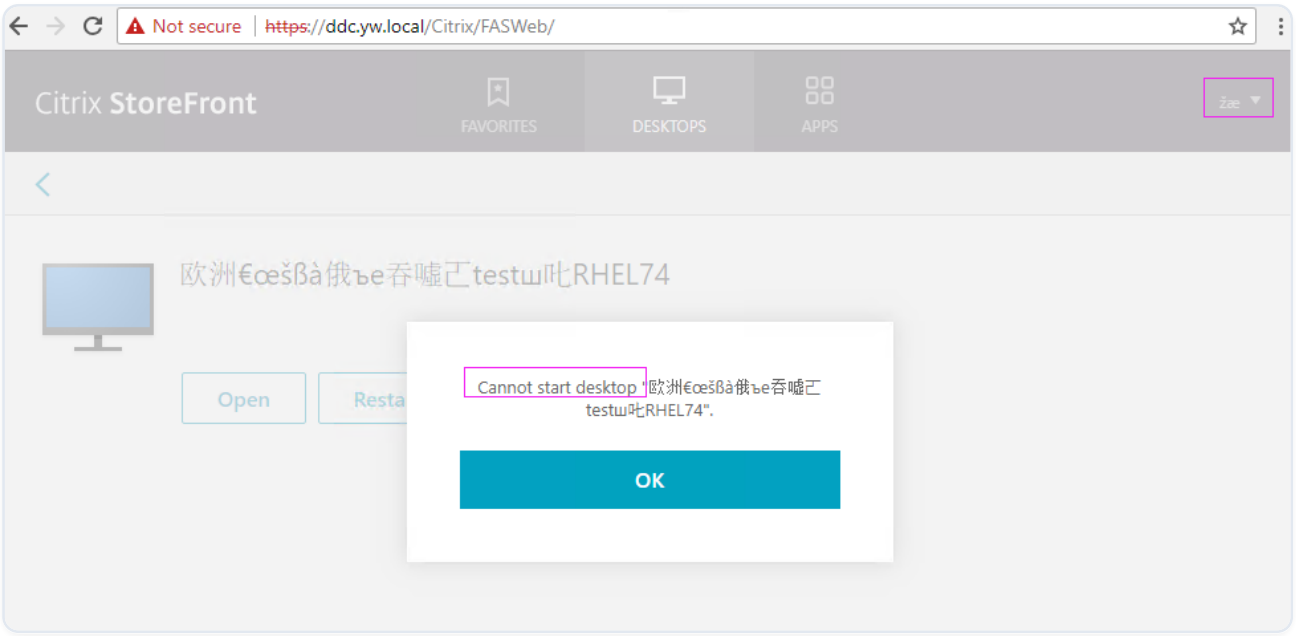
Verwandte Informationen

- Die gängigen FAS-Bereitstellungen sind im Artikel Architekturübersicht des Federated Authentication Service zusammengefasst.

- Anleitungen werden im Kapitel Erweiterte Konfiguration des Federated Authentication Service vorgestellt.

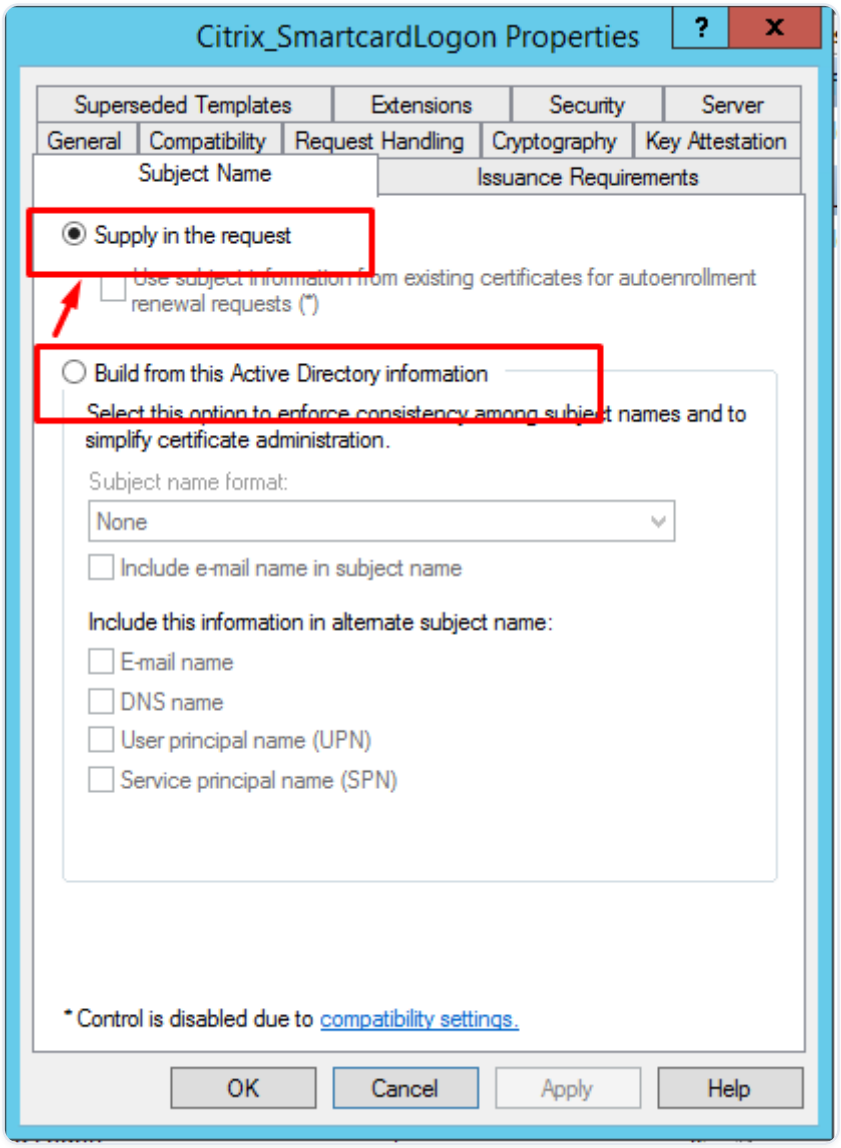
Bekanntes Problem

Wenn FAS verwendet wird, kann es zu Fehlern kommen, wenn Sie versuchen, eine veröffentlichte Desktop- oder App-Sitzung mit nicht-englischen Zeichen zu starten.



Problemumgehung

Klicken Sie im CA-Tool mit der rechten Maustaste auf **Vorlagen verwalten**, um die Vorlage **Citrix_SmartcardLogon** von **Aus diesen Active Directory-Informationen erstellen** in **In der Anforderung bereitstellen** zu ändern:


Citrix_SmartcardLogon Properties
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Subject Name
Issuance Requirements
Supply in the request
renewal requests (*)
Build from this Active Directory information
simplify certificate administration.
Subject name format:
None
Include e-mail name in subject name
Include this information in alternate subject name:
E-mail name
DNS name
User principal name (UPN)
Service principal name (SPN)
* Control is disabled due to compatibility settings.
OK
Cancel
Apply
Help

Linux Virtual Delivery Agent-Dokumentverlauf

Die folgende Tabelle enthält wichtige Änderungen an der Linux Virtual Delivery Agent 2107-Dokumentation. Um Benachrichtigungen über diese Updates zu erhalten, abonnieren Sie den RSS-Feed.

DATUM	ÄNDERUNG	BESCHREIBUNG
13 Jul 2021	Release von Linux Virtual Delivery Agent 2107	Neue Features in Linux Virtual Delivery Agent 2107