Linux Virtual Delivery Agent 2308

Contents

Linux Virtual Delivery Agent 2308

January 8, 2024

> **Wichtig:**
>
> Informationen zur Produktlebenszyklusstrategie für aktuelle Releases (CR) und Long Term Service Releases (LTSR) finden Sie unter Lifecycle Milestones.

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

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

Was ist neu

February 9, 2024

Was ist neu in 2308

Version 2308 des Linux VDA enthält die folgenden neuen und erweiterten Features:

Unterstützung für RHEL 8.8, Rocky Linux 8.8, RHEL 9.2 und Rocky Linux 9.2

Folgende Linux-Distributionen werden jetzt vom Linux VDA unterstützt:

- RHEL 8.8
- Rocky Linux 8.8
- RHEL 9.2
- Rocky Linux 9.2

Weitere Informationen finden Sie unter Systemanforderungen.

Beschleunigung durch GPU-Freigabe auf einem Linux VDA mit mehreren Sitzungen

Auf einem Linux VDA mit mehreren Sitzungen können Sie jetzt die Beschleunigung durch GPU-Freigabe aktivieren, um OpenGL 3D-Anwendungen zu beschleunigen. Weitere Informationen finden Sie unter Beschleunigung durch GPU-Freigabe auf einem Linux VDA mit mehreren Sitzungen.

Bestimmte Datenformate können zwischen Sitzung und Client kopiert und eingefügt werden

Sie können jetzt zulassen, dass bestimmte Datenformate zwischen der VDA-Sitzung und dem Clientgerät kopiert und eingefügt werden. Dieses Feature wird durch Citrix-Richtlinien aktiviert. Weitere Informationen finden Sie unter Zwischenablagenumleitung.

Erweiterte Unterstützung für Quest

Wir haben die Quest-Unterstützung auf RHEL 8.x, Rocky Linux 8.x, RHEL 9.x und Rocky Linux 9.x erweitert. Weitere Informationen finden Sie unter Systemanforderungen im Abschnitt **Active Directory-Integrationspakete**.

Serverseitiger Abruf und clientseitige Wiedergabe zur Browserinhaltsumleitung

Wir haben die Umleitung von Browserinhalten erweitert, um Szenarios mit serverseitigem Abruf und clientseitiger Wiedergabe zu unterstützen. In diesem Szenario ruft die Citrix Workspace-App (der Client) den Inhalt über den VDA und einen virtuellen Kanal (**CTXPFWD**) vom Webserver ab. Diese Option ist nützlich, wenn Clients (z. B. Thin Clients) keinen Zugriff auf einen Webserver haben. Sie senkt den CPU- und RAM-Verbrauch auf dem VDA, verbraucht jedoch Bandbreite im virtuellen ICA-Kanal. Weitere Informationen finden Sie unter Browserinhaltsumleitung.

Verbesserte EDT-Überlastungssteuerung (Preview)

Zur Optimierung des EDT-Protokolls (Enlightened Data Transport) wird ein neuer Algorithmus zur Überlastungssteuerung eingeführt. Damit kann EDT höhere Durchsätze erzielen und die Latenz reduzieren, wodurch das Benutzererlebnis verbessert wird. Das Feature ist in der Standardeinstellung deaktiviert. Weitere Informationen finden Sie unter Adaptiver Transport.

Weitere Menüelemente im Infobereich

Wir haben das Tool Bildschirmfreigabe im Infobereich um weitere Menüelemente erweitert. Derzeit können Sitzungsbenutzer auf das Symbol im Infobereich klicken, um auf folgende Menüelemente zuzugreifen und die entsprechenden Aktionen auszuführen:

- Bildschirmfreigabe
- Wechsel der Desktopumgebung
- Schieberegler für Grafikqualität
- CQI in Echtzeit

Weitere Informationen finden Sie unter Infobereich.

Verbesserte H.265-Hardwarecodierung

Wir haben die H.265-Hardwarecodierung erweitert, um eine verlustfreie Komprimierung für den gesamten Bildschirm und den verlustbehafteten H.265-Hardwarecodec für aktiv wechselnde Regionen zu ermöglichen. Weitere Informationen finden Sie unter Grafikkonfiguration und -feineinstellung.

XDPing-Erweiterung zur Unterstützung von SQLite-Tests und RC4-Problemprüfungen

Wir haben den Umfang einzelner Tests und Statusprüfungen der VDA-Registrierung, die mit dem **XDPing**-Tool von Linux möglich sind, um SQLite-Tests bzw. RC4-Problemprüfungen erweitert. Weitere Informationen finden Sie unter **XDPing**.

Realm wurde gründlich für Amazon Linux 2, RHEL 7.9 und CentOS 7.9 getestet

Das Hinzufügen einer Linux-VM zu einer Active Directory-Domäne mithilfe von **realm** wurde gründlich für Amazon Linux 2, RHEL 7.9 und CentOS 7.9 getestet. Sie können weiterhin den Befehl **net ads** verwenden, um die Linux-VMs, die auf Amazon Linux 2, RHEL 7.9 und CentOS 7.9 laufen, mit einer Active Directory-Domäne zu verbinden.

Weitere Informationen finden Sie unter Linux VDA manuell auf Amazon Linux 2, CentOS, RHEL und Rocky Linux installieren.

Was ist neu in früheren Releases

Informationen zu neuen Features in den Releases, die nach 1912 LTSR bis zu 2305 CR ausgeliefert wurden, finden Sie unter Neue Features –Archiv.

Behobene Probleme

January 8, 2024

Folgende Probleme wurden im Linux Virtual Delivery Agent 2308 behoben:

- Der Start von App-Sitzungen von einem unter RHEL 8.x oder Rocky Linux 8.x installierten Linux VDA aus schlagen fehl. Das Problem tritt auf, wenn der VDA über den System Security Services Daemon (SSSD) mit der Domäne verbunden ist und **default_shell** in der Datei **/etc/sssd/sssd.conf** auf **/bin/csh** festgelegt ist. [CVADHELP-22831]

- Wenn Sie die Sitzung in den Vollbildmodus versetzen und HDX 3D Pro auf einem Linux VDA aktiviert ist, wird die Sitzung möglicherweise unerwartet beendet. [CVADHELP-22352]

Bekannte Probleme

January 8, 2024

Die folgenden Probleme wurden in diesem Release identifiziert:

- Wenn Sie mit einem Clientgerät ohne Akku auf eine virtuelle Desktopsitzung zugreifen, wird der Akkustatus des Clients möglicherweise unerwartet in der Sitzung angezeigt. Das Problem tritt auf, wenn Sie mit der Citrix Workspace-App für Mac oder der Citrix Workspace-App für Linux auf eine Sitzung zugreifen, die Sie zuvor mit einem Clientgerät mit Akku geöffnet haben.

  [LNXVDA-15406]

- Wenn Sie den Linux VDA auf Version 2308 aktualisieren und ctxinstall.sh erneut ausführen, wird Ihr Basisordner geändert. Das Problem tritt auf, wenn der Kerberos-Bereichsname in Großbuchstaben angegeben ist und SSSD als Methode für den Domänenbeitritt verwendet wird. Um das Problem zu beheben, nehmen Sie die folgenden Änderungen in ctxinstall.sh vor:

  - Ändern Sie in der Skriptfunktion **get_realm** `realm=$(tr '[:upper:]''[:lower:]'<<<"${ CTX_EASYINSTALL_REALM } ")` in `realm="${ CTX_EASYINSTALL_REALM } "` und ändern Sie `realm=$(tr '[:upper:]''[:lower:]'<<<"$val")` in `realm="$val"`.
  - Ändern Sie in der Skriptfunktion **get_netbios_domain** `workgroup=$(tr '[:upper:]''[:lower:]'<<<"$CTX_EASYINSTALL_NETBIOS_DOMAIN")` in `workgroup="$CTX_EASYINSTALL_NETBIOS_DOMAIN"`.

  [CVADHELP-23303]

- Wenn HDX 3D Pro aktiviert ist, erscheinen Sitzungen auf den Erweiterungsbildschirmen schwarz und nur der Hauptbildschirm zeigt die Sitzungen ordnungsgemäß an. Um das Problem zu beheben, öffnen Sie ein Terminal-Fenster auf dem VDA und führen Sie nach Bedarf die folgenden Befehle aus:

  - Bei zwei Bildschirmen:

    ```
    1  #sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP"" /etc/X11/ctx-nvidia-2.conf
    2  <!--NeedCopy-->
    ```

  - Bei drei Bildschirmen:


```
#sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP, DFP"" /etc/X11/ctx-nvidia-3.conf
<!--NeedCopy-->
```

- Bei vier Bildschirmen:

```
#sed -i "/UseEDID/a \ \ Option "ConnectedMonitor" "DFP, DFP, DFP, DFP"" /etc/X11/ctx-nvidia-4.conf
<!--NeedCopy-->
```

[LNXVDA-15259]

- Sitzungsstartfehler treten auf, wenn die in PostgreSQL festgelegte maximale Anzahl von Verbindungen nicht für gleichzeitige Sitzungen ausreicht. Erhöhen Sie als Workaround die maximale Anzahl an Verbindungen, indem Sie die Einstellung **max_connections** in der Datei **postgresql.conf** ändern.
- Die VDA-Registrierung schlägt möglicherweise aufgrund der folgenden LDAP-Ausnahme in **/var/log/xdl/jproxy.log** fehl:

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

Sie umgehen das Problem wie folgt:

- Ändern Sie den LDAP-Timeoutwert. Ändern Sie beispielsweise den LDAP-Timeoutwert mit dem folgenden Befehl in 60 Sekunden:

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

- Beschleunigen Sie LDAP-Abfragen, indem Sie eine Suchbasis einrichten. Sie können eine Suchbasis mit der Variablen CTX_XDL_SEARCH_BASE in ctxsetup.sh oder mit dem folgenden Befehl einrichten:

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

[CVADHELP-20895]

- Microsoft veröffentlichte im November 2022 die kumulativen Updates KB5019966 und KB5019964 für Windows 10. Durch die Updates kommt es zu Fehlern beim Domänenbeitritt und bei der Registrierung. Informationen zur Umgehung des Problems finden Sie im Knowledge Center-Artikel CTX474888.

- Wenn der Verschlüsselungstyp **RC4_HMAC_MD5** für Kerberos zugelassen ist, kann sich der Linux VDA möglicherweise nicht beim Controller registrieren und die folgende Fehlermeldung wird angezeigt:

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

  Als Problemlösung deaktivieren Sie **RC4_HMAC_MD5** global in Ihrer Active Directory-Domäne (*oder in einer bestimmten Organisationseinheit*) oder lassen Sie schwache Verschlüsselungstypen auf dem Linux VDA zu. Löschen Sie anschließend die zwischengespeicherten Kerberos-Tickets auf dem Controller und dem Citrix Cloud Connector mit dem Befehl **klist -li 0x3e4 purge** und starten Sie den Linux VDA neu.

  Führen Sie die folgenden Schritte aus, um **RC4_HMAC_MD5** global in Ihrer Active Directory-Domäne zu deaktivieren:

  1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
  2. Suchen Sie die Zieldomäne und wählen Sie dann **Standarddomänenrichtlinie**.
  3. Klicken Sie mit der rechten Maustaste auf **Standarddomänenrichtlinie** und wählen Sie **Bearbeiten**. Der Gruppenrichtlinienverwaltungs-Editor wird geöffnet.
  4. Wählen Sie **Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen**.
  5. Doppelklicken Sie auf **Netzwerksicherheit: Für Kerberos zulässige Verschlüsselungstypen konfigurieren**.
  6. Deaktivieren Sie die Kontrollkästchen **DES_CBC_CRC**, **DES_CBC_MD5** und **RC4_HMAC_MD5** und aktivieren Sie **AES128_HMAC_SHA1**-, **AES256_HMAC_SHA1**- und **Künftige Verschlüsselungstypen**.

  Führen Sie die folgenden Schritte aus, um schwache Verschlüsselungstypen auf dem Linux VDA zuzulassen:

  > **Hinweis:**
  >
  > Schwache Verschlüsselungstypen machen Ihre Bereitstellung anfällig für Angriffe.

  1. Öffnen Sie die Datei /etc/krb5.conf auf dem Linux VDA.
  2. Fügen Sie im Abschnitt **[libdefaults]** den folgenden Eintrag hinzu:

     ```
     allow_weak_crypto= TRUE
     ```

- Der Linux VDA unterstützt keine SecureICA-Verschlüsselung. Wenn SecureICA auf dem Linux VDA aktiviert ist, führt dies zu einem Sitzungsstartfehler.
- In einer GNOME-Desktopsitzung schlagen Versuche, das Tastaturlayout zu ändern, möglicherweise fehl. [CVADHELP-15639]

- Beim Dateidownload wird unerwartet ein Fenster angezeigt. Das Fenster hat keine Auswirkungen auf die Dateidownloadfunktion und wird nach einiger Zeit automatisch ausgeblendet. [LNXVDA-5646]
- Wenn die SSL-Verschlüsselung aktiviert und die Sitzungszuverlässigkeit deaktiviert ist, können keine Sitzungen in der Citrix Workspace-App für Linux gestartet werden. [RFLNX-1557]
- Ubuntu-Grafiken: In HDX 3D Pro wird nach dem Ändern des Desktop Viewer u. U. ein schwarzer Rahmen angezeigt oder der Hintergrund ist schwarz.
- Drucker, die mit der Linux VDA-Druckumleitung erstellt wurden, können nach dem Abmelden von einer Sitzung u. U. nicht entfernt werden.
- CDM-Dateien fehlen, wenn das Verzeichnis viele Dateien und Unterverzeichnisse enthält Wenn clientseitig zu viele Dateien oder Verzeichnisse vorliegen, kann dieses Problem auftreten.
- In diesem Release wird nur UTF-8-Codierung für andere Sprachen als Englisch unterstützt.
- Der Status der Feststelltaste in der Citrix Workspace-App für Android kann beim Sitzungsroaming umgekehrt werden. Der Status der Feststelltaste kann aufgehoben werden, wenn über eine vorhandene Verbindung Roaming zu Citrix Workspace-App für Android erfolgt. Verwenden Sie als Workaround die Umschalttaste auf der erweiterten Tastatur, um zwischen Groß- und Kleinbuchstaben zu wechseln.
- Tastenkombinationen mit der Alt-Taste funktionieren nicht immer, wenn Sie mit der Citrix Workspace-App für Mac eine Verbindung zu einem Linux VDA herstellen. Citrix Workspace-App für Mac sendet standardmäßig für die linke und die rechte Alt-Taste den Befehl "Alt Gr". Sie können dieses Verhalten in den Einstellungen für die Citrix Workspace-App ändern, die Ergebnisse sind jedoch je nach Anwendung unterschiedlich.
- Die Registrierung schlägt fehl, wenn der Linux VDA der Domäne wieder hinzugefügt wird. Beim erneuten Verbindungsaufbau wird ein neuer Satz Kerberos-Schlüssel generiert. Der Broker verwendet jedoch unter Umständen ein veraltetes zwischengespeichertes VDA-Dienstticket, das auf dem vorherigen Kerberos-Schlüsselsatz basiert. Wenn der VDA sich dann mit dem Broker verbinden will, kann der Broker u. U. keinen Sicherheitskontext zum VDA herstellen. Normalerweise schlägt die VDA-Registrierung dann fehl.

  Dieses Problem löst sich irgendwann von selber, wenn das VDA-Dienstticket abläuft und erneuert wird. Diensttickets haben jedoch eine lange Lebensdauer, sodass dies einige Zeit dauern kann.

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

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


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

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

Hinweise zu Drittanbietern

January 8, 2024

Linux Virtual Delivery Agent Version 2308 (PDF-Download)

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

Einstellung von Features und Plattformen

January 8, 2024

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

Veraltete und entfernte Produkte und Features

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

Veraltete Elemente werden nicht sofort entfernt. Der Support von Citrix wird in dieser Version fortgesetzt. In einer zukünftigen Version werden sie entfernt werden.
Entfernte Elemente wurden entfernt oder werden in Linux VDA nicht mehr unterstützt.

Element	Einstellung der Unterstützung angekündigt	Entfernt in
Unterstützung für SUSE 15.4	2308	2311
Unterstützung für Rocky Linux 9.1, Rocky Linux 8.7	2305	2308
Unterstützung für RHEL 9.1, RHEL 8.7	2305	2308
Unterstützung für RHEL 8.4	2303	2308
Unterstützung für Ubuntu 18.04	2212	2305
Unterstützung für SUSE 15.3	2210	2301
Unterstützung für Debian 10.9	2206	2210
Unterstützung für SUSE 15.2	2206	2209
Unterstützung für RHEL 8.2	2206	2209
Unterstützung für RHEL 8.1, RHEL 8.3	2203	2206
Unterstützung für RHEL 7.8, CentOS 7.8	2203	2204
Unterstützung für CentOS 8.x	2110	2201
Unterstützung für SUSE 12.5	2109	2204
Unterstützung für Ubuntu 16.04	2109	2203
Unterstützung für RHEL 7.7, CentOS 7.7	2006	2009
Unterstützung für SUSE 12.3	2006	2006
Unterstützung für RHEL 6.10, CentOS 6.10	2003	2003
Unterstützung für RHEL 6.9, CentOS 6.9	1909	1909
Unterstützung für RHEL 7.5, CentOS 7.5	1903	1903
Unterstützung für RHEL 7.4, CentOS 7.4	1811	1811
Unterstützung für RHEL 6.8, CentOS 6.8	1811	1811

Element	Einstellung der Unterstützung angekündigt	Entfernt in
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

January 8, 2024

Das aktuelle Release von Linux VDA ist mit Citrix Virtual Apps and Desktops abgestimmt. Es ist auch abwärtskompatibel mit früheren Versionen von Citrix Virtual Apps and Desktops, die das Ende ihres Lebenszyklus noch nicht erreicht haben. Weitere Informationen zum Citrix Produktlebenszyklus und wann Citrix die Unterstützung bestimmter Produktversionen beendet, finden Sie unter Citrix Product Lifecycle Matrix.

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

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

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

Unterstützte Linux-Distributionen, Xorg-Versionen und Desktopumgebungen

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

Linux-Distribution	Xorg-Version	Unterstützter Desktop
Amazon Linux 2	1.20	GNOME, GNOME Classic, MATE
Debian 11.3	1.20	GNOME, GNOME Classic, KDE, MATE

Linux-Distribution	Xorg-Version	Unterstützter Desktop
RHEL 9.2/9.0	1.20	GNOME
RHEL 8.8/8.6	1.20	GNOME, GNOME Classic, MATE
RHEL 7.9, CentOS 7.9	1.20	GNOME, GNOME Classic, KDE, MATE
Rocky Linux 9.2/9.0	1.20	GNOME
Rocky Linux 8.8/8.6	1.20	GNOME, GNOME Classic, KDE, MATE
SUSE 15.4	1.20	GNOME, GNOME Classic, MATE
Ubuntu 22.04	1.21	GNOME, GNOME Classic, KDE, MATE
Ubuntu 20.04	1.20	GNOME, GNOME Classic, KDE, MATE

Hinweis:

- Wenn Ihr Betriebssystem vom Hersteller nicht mehr unterstützt wird, kann Citrix Probleme möglicherweise nur noch eingeschränkt beheben. Informationen zu veralteten oder entfernten Plattformen finden Sie unter Einstellung von Features und Plattformen.
- Mindestens ein Desktop muss installiert sein. Sie können mit dem Skript ctxinstall.sh oder ctxsetup.sh die GNOME-, GNOME Classic- oder MATE-Desktopumgebung angeben, die in Sitzungen verwendet werden soll.
- Gemäß der Dokumentation zu Red Hat Enterprise Linux ist GNOME die einzige Desktopumgebung, die in RHEL 9 verfügbar ist.
- Verwenden Sie nicht den `HWE kernel` oder `HWE Xorg` in Ubuntu.
- Ihr Benutzernamenformat muss den `systemd`-Syntaxregeln für Ihren aktuellen Displaymanager entsprechen. Weitere Hinweise zur `systemd`-Benutzernamenssyntax finden Sie unter User/Group Name Syntax.

Unterstützte Hostplattformen und Virtualisierungsumgebungen

- Bare-Metal-Server
- Amazon Web Services (AWS)
- Citrix Hypervisor
- Google Cloud Platform (GCP)
- Kernel-based Virtual Machine (KVM)

- Microsoft Azure
- Microsoft Hyper-V
- VMware vSphere Hypervisor
- Nutanix AHV

> **Hinweis:**
>
> In allen Fällen wird die Prozessorarchitektur x86-64 unterstützt.
>
> Ab Release 2203 können Sie den Linux VDA auf Microsoft Azure, AWS und GCP für Citrix Virtual Apps and Desktops sowie auf Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) hosten. Um diese Verbindungen mit Hosts öffentlicher Clouds zu Ihrer Citrix Virtual Apps and Desktops-Bereitstellung hinzuzufügen, benötigen Sie eine Citrix Universal Subscription- oder eine Hybrid Rights-Lizenz. Informationen zu Universal Subscription- und Hybrid Rights-Lizenzen finden Sie unter Transition and Trade Up (TTU) mit Citrix Universal Subscription.

Active Directory-Integrationspakete

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

	Winbind	SSSD	Centrify	PBIS	Quest
Amazon Linux 2	Ja	Ja	Ja	Ja	Nein
Debian 11.3	Ja	Ja	Ja	Ja	Nein
RHEL 9.2/9.0, Rocky Linux 9.2/9.0/8.8/8.6	Ja	Ja	Nein	Nein	Ja (Quest v4.1 und höher)
RHEL 8.8/8.6	Ja	Ja	Ja	Ja	Ja (Quest v4.1 und höher)
RHEL 7.9, CentOS 7.9	Ja	Ja	Ja	Ja	Ja (Quest v4.1 und höher)
SUSE 15.4	Ja	Ja	Ja	Ja	Nein
Ubuntu 22.04/20.04	Ja	Ja	Ja	Ja	Ja (Quest v4.1 und höher)

HDX 3D Pro

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

funktionieren.

Hypervisors

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

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

> **Hinweis:**
>
> Die Hypervisors sind mit bestimmten Linux-Distributionen kompatibel.
> Um HDX 3D Pro für Amazon Linux 2 zu verwenden, empfehlen wir die Installation des NVIDIA-Treibers 470.

GPUs

Für den Linux VDA unterstützt HDX 3D Pro die folgenden GPU-Typen:

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

Stellen Sie sicher, dass Sie den neuesten vGPU-Treiber für Ihre GPU-Karte installiert haben. Derzeit unterstützt der Linux VDA bis zu vGPU 15. Weitere Informationen finden Sie unter NVIDIA Virtual GPU Software Supported GPUs.

Nicht virtualisierte GPUs In der Linux VDA-Dokumentation beziehen sich nicht virtualisierte GPUs auf:

- GPUs, die in Remote-PC-Zugriff-Szenarios verwendet werden
- GPUs, die von einem Hypervisor übergeben werden

NVIDIA-GPUs, die das NVIDIA Capture SDK für Linux unterstützen Aktivieren Sie bei NVIDIA-GPUs, die das NVIDIA Capture SDK für Linuxunterstützen, HDX 3D Pro durch Festlegen von

CTX_XDL_HDX_3D_PRO auf **Y** bei der Installation des Linux VDA. Eine zusätzliche Konfiguration ist nicht erforderlich. Die Hardwarebeschleunigung wird standardmäßig aktiviert, wenn Sie HDX 3D Pro aktivieren.

Installationsübersicht

January 8, 2024

Dieser Abschnitt erläutert die folgenden Verfahren:

- Domänengebundene VDAs mit Easy Install erstellen
- Nicht domänengebundene Linux VDAs mit den Maschinenerstellungsdiensten erstellen
- Linux VDAs mit den Maschinenerstellungsdiensten erstellen
- Linux-VDAs mit Citrix Provisioning erstellen
- Linux VDAs in Citrix DaaS Standard für Azure erstellen
- Linux VDA manuell installieren
  - Linux VDA manuell auf Amazon Linux 2, CentOS, RHEL und Rocky Linux installieren
  - Linux VDA manuell auf SUSE installieren
  - Linux VDA manuell auf Ubuntu installieren
  - Linux VDA manuell auf Debian installieren

Domänengebundene VDAs mit Easy Install erstellen

May 30, 2024

> **Wichtig:**
>
> - Bei Neuinstallationen wird dieser Artikel für eine schnelle Installation empfohlen. Der Artikel beschreibt die einzelnen Schritte zum Installieren und Konfigurieren des Linux VDA mit Easy Install. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als eine manuelle Installation. Sie können hiermit eine Umgebung zum Ausführen des Linux VDA einrichten, wobei die erforderlichen Pakete automatisch installiert und die Konfigurationsdateien automatisch angepasst werden.
> - Easy Install unterstützt den Domainbeitritt mit Quest nicht.

> - Um nicht domänengebundene VDAs zu erstellen, müssen Sie Maschinenerstellungsdienste (MCS) verwenden. Weitere Informationen finden Sie unter Nicht domänengebundene Linux VDAs erstellen.
> - Weitere Informationen zu Features, die für nicht domänengebundene VDAs verfügbar sind, finden Sie unter Nicht domänengebundene VDAs.

Schritt 1: Vorbereiten der Konfigurationsinformationen und der Linux-Maschine

Halten Sie die folgenden Konfigurationsinformationen für Easy Install bereit:

- Hostname: Hostname der Maschine, auf der der Linux VDA installiert werden soll.
- IP-Adresse des Domänennamenservers.
- IP-Adresse oder Zeichenfolgenname des NTP-Servers.
- Domänenname: NetBIOS-Name der Domäne.
- Bereichsname: Kerberos-Bereichsname.
- Vollqualifizierter Domänenname (FQDN) der Domäne.
- Active Directory-Integrationsmethode: Easy Install unterstützt aktuell Winbind, SSSD, Centrify und PBIS.
- Benutzername: Name des Benutzers, der die Maschine mit der Domäne verbindet.
- Kennwort: Kennwort des Benutzers, der die Maschine mit der Domäne verbindet.
- OE: Organisationseinheit. Optional.

> **Wichtig:**
>
> - Für die Installation des Linux VDA muss sichergestellt sein, dass die Repositorys der Linux-Maschine richtig hinzugefügt wurden.
> - Zum Starten einer Sitzung muss sichergestellt sein, dass das X Window System und die Desktopumgebungen installiert sind.
> - Das Kennwort für den Domänenbeitritt wird aus Sicherheitsgründen nicht von Easy Install gespeichert. Sie müssen daher bei jedem Ausführen des Skripts für Easy Install (ctxinstall.sh) im interaktiven Modus das Kennwort für den Domänenbeitritt manuell eingeben. Im automatischen Modus müssen Sie das Kennwort für den Domänenbeitritt in **/Citrix/VDA/sbin/ctxinstall.conf** festlegen oder das Kennwort exportieren. Es wird empfohlen, nicht das Administratorkonto für den Domänenbeitritt zu verwenden. Delegieren Sie die Berechtigungen für den Domänenbeitritt stattdessen an einen anderen Active Directory-Benutzer. Nutzen Sie den **Assistenten zum Zuweisen der Objektverwaltung**, um die Steuerung auf dem Domänencontroller zu delegieren.

Schritt 2: Vorbereiten des Hypervisors

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

Festlegen der Zeitsynchronisierung auf Citrix Hypervisor

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

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

```
su -

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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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

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

```
xen.independent_wallclock = 1
```

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

```
su -

```



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

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

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

Auf dem verwaltenden Betriebssystem:

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

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

Festlegen der Zeitsynchronisierung auf ESX und ESXi

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

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

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

Schritt 3: .NET Runtime 6.0 installieren

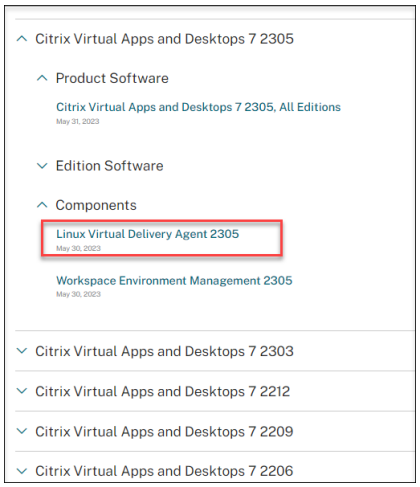
Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

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

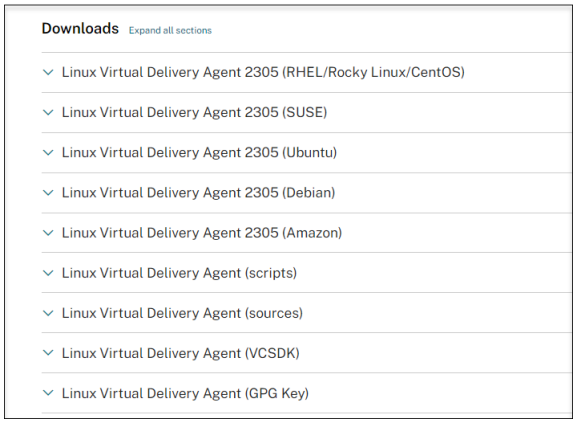
Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 4: Herunterladen des Linux VDA-Pakets

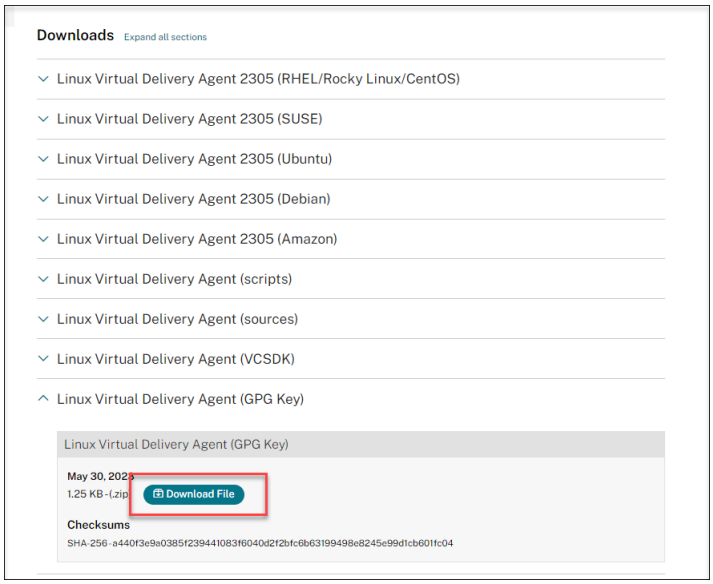
1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
2. Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. Erweitern Sie **Komponenten**, um den Linux VDA zu finden. Beispiel:



4. Klicken Sie auf den Linux VDA-Link, um auf die Linux VDA-Downloads zuzugreifen.



5. Laden Sie das Linux VDA-Paket herunter, das Ihrer Linux-Distribution entspricht.
6. Laden Sie den öffentlichen GPG-Schlüssel herunter, mit dem Sie die Integrität des Linux VDA-Pakets überprüfen können. Beispiel:



Überprüfen der Integrität des Linux VDA-Pakets mit dem öffentlichen Schlüssel:

- Führen Sie für ein RPM-Paket die folgenden Befehle aus, um den öffentlichen Schlüssel in die RPM-Datenbank zu importieren und die Paketintegrität zu überprüfen:

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

- Führen Sie für ein DEB-Paket die folgenden Befehle aus, um den öffentlichen Schlüssel in die DEB-Datenbank zu importieren und die Paketintegrität zu überprüfen:

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

Schritt 5: Installieren des Linux VDA-Pakets

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

Amazon Linux 2-, CentOS-, RHEL- und Rocky Linux-Distributionen:

> **Hinweis:**
>
> - Installieren Sie für RHEL und CentOS das EPEL-Repository, bevor Sie den Linux VDA erfol-

> greich installieren können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter https://docs.fedoraproject.org/en-US/epel/.
>
> - Aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher, bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 installieren.

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

> **Hinweis:**
>
> Nach der Installation des Linux VDA auf RHEL 8.x/9.x oder Rocky Linux 8.x/9.x, das auf GCP gehostet wird, wird die Ethernetverbindung möglicherweise unterbrochen und der Linux VDA ist nach einem VM-Neustart u. U. nicht erreichbar. Um das Problem zu umgehen, legen Sie ein Root-Kennwort fest, wenn Sie sich das erste Mal an der VM anmelden, und stellen sicher, dass Sie sich als Root-Benutzer an der VM anmelden können. Führen Sie dann nach dem Neustart der VM die folgenden Befehle in der Konsole aus:
>
> ```
> nmcli dev connect eth0
> service NetworkManager restart
> <!--NeedCopy-->
> ```

Für Ubuntu/Debian-Distributionen:

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

> **Hinweis:**
>
> - Um die notwendigen Abhängigkeiten für eine Distribution mit Debian 11.3 zu installieren, fügen Sie die Zeile `deb http://deb.debian.org/debian/ bullseye main` in der Datei /etc/apt/sources.list hinzu.
> - Deaktivieren Sie RDNS für Ubuntu 20.04 auf GCP. Fügen Sie dazu in /etc/krb5.conf die Zeile **rdns = false** unter **[libdefaults]** hinzu.

SUSE-Distributionen:

1. Für SUSE 15.4 in AWS, Azure und GCP ist Folgendes sicherzustellen:
   - Sie verwenden **libstdc++6** Version 12 oder höher.
   - Der Parameter **Default_WM** in **/etc/sysconfig/windowmanager** ist auf **"gnome"** gesetzt.
2. Führen Sie den folgenden Befehl aus, um den Linux VDA zu installieren:

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


Schritt 6: Installieren von NVIDIA GRID-Treibern

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

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

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

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

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

Schritt 7: Angeben einer zu verwendenden Datenbank

Sie können nach der Installation des Linux VDA-Pakets zwischen SQLite und PostgreSQL wechseln. Führen Sie hierzu die folgenden Schritte aus:

> **Hinweis:**
>
> - Wir empfehlen, SQLite nur für den VDI-Modus und PostgreSQL für ein Bereitstellungsmodell für gehostete freigegebene Desktops zu verwenden.
> - Bei Easy Install und den Maschinenerstellungsdiensten (MCS) können Sie SQLite oder PostgreSQL zur Verwendung angeben, ohne die Systeme manuell installieren zu müssen. Sofern nicht anders durch **/etc/xdl/db.conf** angegeben, verwendet der Linux VDA standardmäßig PostgreSQL.
> - Sie können auch **/etc/xdl/db.conf** verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

1. Bearbeiten Sie **/etc/xdl/db.conf**, um eine zu verwendende Datenbank anzugeben.
2. Führen Sie **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** oder **/opt/Citrix/VDA/bin/easyinstall** aus.

Schritt 8: Einrichten der Laufzeitumgebung für die Installation

Nach der Installation des Linux VDA-Pakets konfigurieren Sie die Laufzeitumgebung, indem Sie das Skript ctxinstall.sh ausführen oder die GUI verwenden.

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

ctxinstall.sh

ctxinstall.sh ist das Installationsskript für Easy Install, das die Laufzeitumgebung für den Linux VDA konfiguriert. Weitere Informationen erhalten Sie durch Eingabe des Hilfebefehls **ctxinstall.sh -h**.

Mit der Konfigurationsdatei **/opt/Citrix/VDA/sbin/ctxinstall.conf** werden die Werte aller Umgebungsvariablen festgelegt, gespeichert und synchronisiert, die für GUI und ctxinstall.sh erforderlich sind. Verwenden Sie eine der folgenden Methoden, wenn Sie die Konfigurationsdatei zum ersten Mal erstellen:

- Kopieren Sie die Vorlagendatei **/opt/Citrix/VDA/sbin/ctxinstall.conf.tmpl** und speichern Sie sie unter **/opt/Citrix/VDA/sbin/ctxinstall.conf**.
- Führen Sie ctxinstall.sh aus. Jedes Mal, wenn Sie ctxinstall.sh ausführen, wird Ihre Eingabe in **/opt/Citrix/VDA/sbin/ctxinstall.conf** gespeichert.

> **Hinweis:**
>
> - Gemäß dem Prinzip der geringsten Privilegien sollten Sie sicherstellen, dass nur der Root-Benutzer **/opt/Citrix/VDA/sbin/ctxinstall.conf** lesen kann, da das Kennwort für den Domänenbeitritt möglicherweise in der Datei festgelegt ist.
> - Durch die Deinstallation des Linux VDA werden Dateien unter **/opt/Citrix/VDA** entfernt. Wir empfehlen, ein Backup von **/opt/Citrix/VDA/sbin/ctxinstall.conf** zu erstellen, bevor Sie den VDA deinstallieren.

Sie können ctxinstall.sh im interaktiven Modus oder im automatischen Modus ausführen. Legen Sie die folgenden Umgebungsvariablen fest, bevor Sie das Skript ausführen:

- **CTX_EASYINSTALL_HOSTNAME=host-name**: Hostname des Linux VDA-Servers.
- **CTX_EASYINSTALL_DNS=ip-address-of-dns** –IP-Adresse des DNS.
- **CTX_EASYINSTALL_NTPS=address-of-ntps**: IP-Adresse oder Zeichenfolgenname des NTP-Servers.
- **CTX_EASYINSTALL_REALM=realm-name**: Der Kerberos-Bereichsname.
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**

- **CTX_EASYINSTALL_USERNAME=domain-user-name**: Name des Benutzers, der das Gerät mit der Domäne verbindet.
- **CTX_EASYINSTALL_PASSWORD=password**: Kennwort des Benutzers, der die Maschine mit der Domäne verbindet.

  > **Hinweis:**
  >
  > Es wird empfohlen, nicht das Administratorkonto für den Domänenbeitritt zu verwenden. Delegieren Sie die Berechtigungen für den Domänenbeitritt stattdessen an einen anderen Active Directory-Benutzer. Nutzen Sie den **Assistenten zum Zuweisen der Objektverwaltung**, um die Steuerung auf dem Domänencontroller zu delegieren.

Die folgenden vier Variablen sind optional. Auch wenn sie nicht festgelegt sind, wird ctxinstall.sh im automatischen Modus nicht abgebrochen, und Sie werden im interaktiven Modus nicht zur Benutzereingabe aufgefordert. Sie können sie nur festlegen, indem Sie ihre Werte exportieren oder **/Citrix/VDA/sbin/ctxinstall.conf** bearbeiten.

- **CTX_EASYINSTALL_NETBIOS_DOMAIN=netbios-domain-name** –Der NetBIOS-Domainname ist in der Regel die erste Komponente des DNS-Domänennamens, getrennt durch einen Punkt (.). Andernfalls passen Sie einen anderen NetBIOS-Domänennamen an. Diese Variable ist optional.
- **CTX_EASYINSTALL_OU=ou-value** –OU-Werte variieren je nach **AD**-Integrationsmethode. Eine Tabelle mit Beispielwerten für Organisationseinheiten finden Sie im Abschnitt Überlegungen dieses Artikels. Diese Variable ist optional.
- **CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=centrify-local-path** —Das Centrify-Paket wird mit Easy Install über das Internet heruntergeladen. Falls Centrify bereits installiert ist, können Sie das Centrify-Paket von einem lokalen Verzeichnis abrufen, das durch diese Variable definiert ist. Diese Variable ist optional.
- **CTX_EASYINSTALL_PBIS_LOCAL_PATH= pbis-local-path** —Das PBIS-Paket wird mit Easy Install über das Internet heruntergeladen. Falls PBIS bereits installiert ist, können Sie das PBIS-Paket von einem lokalen Verzeichnis abrufen, das durch diese Variable definiert ist. Diese Variable ist optional.

Beim Ausführen von ctxinstall.sh wird das Skript ctxsetup.sh aufgerufen. ctxsetup.sh verwendet die folgenden Variablen:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'**–Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME muss angegeben werden.

- **CTX_XDL_VDA_PORT=port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –Die Linux Virtual Desktop-Dienste werden nach dem Systemstart gestartet.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen.
- **CTX_XDL_AD_INTEGRATION=winbind | sssd | centrify | pbis** –Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt.
- **CTX_XDL_HDX_3D_PRO=Y | N** –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Bei aktiviertem HDX 3D Pro wird der VDA für VDI-Desktopmodus (Einzelsitzungen) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y | N** –Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Legen Sie den Wert bei Umgebungen mit HDX 3D Pro auf "Y"fest.
- **CTX_XDL_SITE_NAME=dns-name** –Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Wenn dies unnötig ist, legen Sie **<none>** fest.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268 oder ad1.mycompany.com:636 ad2.mycompany.com:3269 ad3.mycompany.com:3269, wenn Sie LDAPS verwenden. Für schnellere LDAP-Abfragen in einer Active Directory-Gesamtstruktur aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben als LDAP-Portnummer 3268 bzw., sofern Sie LDAPS verwenden, 3269 an. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE=search-base-set** –Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Wenn dies unnötig ist, legen Sie **<none>** fest.
- **CTX_XDL_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt

die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. ctx_xdl_fas_fas_list='FAS_Server_1_URL:Port_Number; fas_server_2_url: port_number; fas_server_3_url: port_number'.

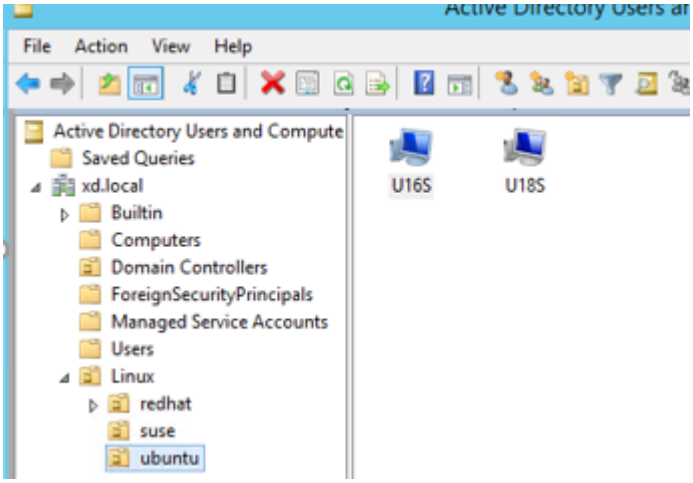
- **CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate**: Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.
- **CTX_XDL_START_SERVICE=Y | N**: Legt fest, ob die Linux VDA-Dienste nach Abschluss der Konfiguration gestartet werden.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

Überlegungen

- Der NetBIOS-Domainname ist in der Regel die erste Komponente des DNS-Domänennamens, getrennt durch einen Punkt (.). Um einen benutzerdefinierten NetBIOS-Domänennamen in Ihrer Umgebung zu verwenden, legen Sie die Umgebungsvariable **CTX_EASYINSTALL_NETBIOS_DOMAIN** in **/opt/Citrix/VDA/sbin/ctxinstall.conf** fest.
- Gehen Sie folgendermaßen vor, um den VDA einer Organisationseinheit anzufügen:

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

     Ein OU-Beispiel sehen Sie im folgenden Screenshot.



2. Legen Sie die Umgebungsvariable **CTX_EASYINSTALL_OU** in **/opt/Citrix/VDA/sbin/ctxinstall.conf** fest.

   OU-Werte variieren je nach AD-Methode. Die folgende Tabelle enthält die Beispielnamen von Organisationseinheiten in der vorherigen Bildschirmaufnahme. Sie können beliebige andere Namen für Organisationseinheiten in Ihrer Organisation verwenden.

Betriebssystem	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	`"Linux/amazon"`	`"Linux/amazon"`	`"XD.LOCAL/Linux/amazon"`	`"Linux/amazon"`
Debian	`"Linux/debian"`	`"Linux/debian"`	`"XD.LOCAL/Linux/debian"`	`"Linux/debian"`
RHEL 9.2/9.0, Rocky Linux 9.2/9.0	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	–	–
RHEL 8.x	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	`"XD.LOCAL/Linux/redhat"`	`"Linux/redhat"`
Rocky Linux 8.x	`"OU=redhat,OU=Linux"`	`"OU=redhat,OU=Linux"`	–	–
RHEL 7	`"Linux/redhat"`	`"Linux/redhat"`	`"XD.LOCAL/Linux/redhat"`	`"Linux/redhat"`

Betriebssystem	Winbind	SSSD	Centrify	PBIS
SUSE	"Linux/suse"	"Linux/suse"	"XD.LOCAL/Linux/suse"	"Linux/suse"
Ubuntu	"Linux/ubuntu"	"Linux/ubuntu"	"XD.LOCAL/Linux/ubuntu"	"Linux/ubuntu"

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

  Protokoll:

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

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

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

- Easy Install unterstützt reines **IPv6** ab Linux VDA 7.16. Es gelten folgende Voraussetzungen und Einschränkungen:

  - Ihr Linux-Repository muss so konfiguriert sein, dass die erforderlichen Pakete über reine **IPv6**-Netzwerke heruntergeladen werden können.
  - Centrify wird in reinen **IPv6**-Netzwerken nicht unterstützt.

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

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

  1. Erstellen Sie die Datei `.xsession` oder `.Xclients` auf dem VDA im Verzeichnis **$HOME/<username>**. Wenn Sie Amazon Linux 2 verwenden, erstellen Sie die Datei

`.Xclients`. Wenn Sie andere Distributionen verwenden, erstellen Sie die Datei `.xsession`.

2. Geben Sie in der Datei `.xsession` oder `.Xclients` eine auf Distributionen basierende Desktopumgebung an.

   - **Für MATE-Desktop**

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

   - **Für GNOME Classic-Desktop**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     <!--NeedCopy-->
     ```

   - **Für GNOME-Desktop**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     exec gnome-session
     fi
     <!--NeedCopy-->
     ```

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

Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebung anpassen. Um dieses Feature zu aktivieren, müssen Sie umschaltbare Desktopumgebungen vorher auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen nach Sitzungsbenutzern.

- Wenn Sie Centrify als Methode zum Domänenbeitritt wählen, benötigt das Skript ctxinstall.sh das Centrify-Paket. Möglichkeiten zum Abrufen des Centrify-Pakets durch ctxinstall.sh:

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

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

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

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

Ubuntu/Debian: wget https://downloads.centrify.com/products/server-suite/2022/component-update-1/delinea-server-suite-2022-deb9-x86_64.tgz

- Rufen Sie das Centrify-Paket von einem lokalen Verzeichnis ab, falls Centrify bereits installiert ist. Um das Verzeichnis des Centrify-Pakets zu definieren, legen Sie **CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=/home/mydir** in **/opt/citrix/vda/sbin/ctxinstall.conf** fest. Beispiel:

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

- Wenn Sie PBIS als Methode zum Domänenbeitritt wählen, benötigt das Skript ctxinstall.sh das PBIS-Paket. Möglichkeiten zum Abrufen des PBIS-Pakets durch ctxinstall.sh:

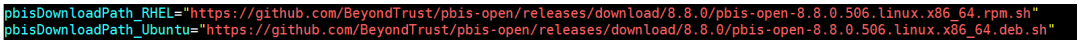
  - Mit Easy Install wird das PBIS-Paket automatisch über das Internet heruntergeladen. URLs für die Distributionen:

    Amazon Linux 2, CentOS 7, RHEL 8, RHEL 7, SUSE 15.4: wget https://github.com/BeyondTrust/pbis-open/releases/download/9.1.0/pbis-open-9.1.0.551.linux.x86_64.rpm.sh

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

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

  Ein Beispiel sehen Sie im folgenden Screenshot:

- Rufen Sie das PBIS-Paket von einem lokalen Verzeichnis ab, falls PBIS bereits installiert ist. Um das Verzeichnis des PBIS-Pakets zu definieren, legen Sie **CTX_EASYINSTALL_PBIS_LOCAL_PATH** in **/opt/citrix/vda/sbin/ctxinstall.conf** fest.

Interaktiver Modus Um das Skript **ctxinstall.sh** im interaktiven Modus auszuführen, verwenden Sie den Befehl **sudo /opt/Citrix/VDA/sbin/ctxinstall.sh** ohne die Option **-S**. Geben Sie an jeder Eingabeaufforderung der Befehlszeilenschnittstelle den entsprechenden Variablenwert ein. Falls eine Variable bereits festgelegt ist, werden Sie in ctxinstall.sh aufgefordert, Änderungen zu bestätigen.

Automatischer Modus Im automatischen Modus müssen Sie die vorherigen Variablen mithilfe von **/opt/Citrix/VDA/sbin/ctxinstall.conf** oder dem Befehl zum Exportieren festlegen. Führen Sie danach **ctxinstall.sh -S** aus (**S** muss hier **groß** geschrieben werden). Wenn nicht alle erforderlichen Variablen festgelegt sind oder ein Wert ungültig ist, bricht **ctxinstall.sh** die Ausführung ab, sofern keine Standardwerte vorhanden sind.

Der exportierte Wert für jede Variable überschreibt den Wert in **/Citrix/VDA/sbin/ctxinstall.conf**, sofern ein Wert festgelegt ist. Alle aktualisierten Werte werden in **/Citrix/VDA/sbin/ctxinstall.conf** gespeichert, mit Ausnahme des Kennworts für den Domänenbeitritt. Sie müssen daher im automatischen Modus das Kennwort für den Domänenbeitritt in **/Citrix/VDA/sbin/ctxinstall.conf** festlegen oder das Kennwort exportieren.

```
export CTX_EASYINSTALL_HOSTNAME=host-name

export CTX_EASYINSTALL_DNS=ip-address-of-dns

export CTX_EASYINSTALL_NTPS=address-of-ntps

export CTX_EASYINSTALL_REALM=realm-name

export CTX_EASYINSTALL_FQDN=ad-fqdn-name

export CTX_EASYINSTALL_USERNAME=domain-user-name

export CTX_EASYINSTALL_PASSWORD=password
```



```
14
15 export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N
16
17 export CTX_XDL_DDC_LIST='list-ddc-fqdns'
18
19 export CTX_XDL_VDA_PORT=port-number
20
21 export CTX_XDL_REGISTER_SERVICE=Y | N
22
23 export CTX_XDL_ADD_FIREWALL_RULES=Y | N
24
25 export CTX_XDL_AD_INTEGRATION=winbind | centrify | sssd | pbis
26
27 export CTX_XDL_HDX_3D_PRO=Y | N
28
29 export CTX_XDL_VDI_MODE=Y | N
30
31 export CTX_XDL_SITE_NAME=dns-site-name | '<none>'
32
33 export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'
34
35 export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'
36
37 export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'
38
39 export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime
40
41 export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
      none>'
42
43 export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number
44
45 export CTX_XDL_TELEMETRY_PORT=port-number
46
47 export CTX_XDL_START_SERVICE=Y | N
48
49 sudo -E /opt/Citrix/VDA/sbin/ctxinstall.sh -S
50 <!--NeedCopy-->
```

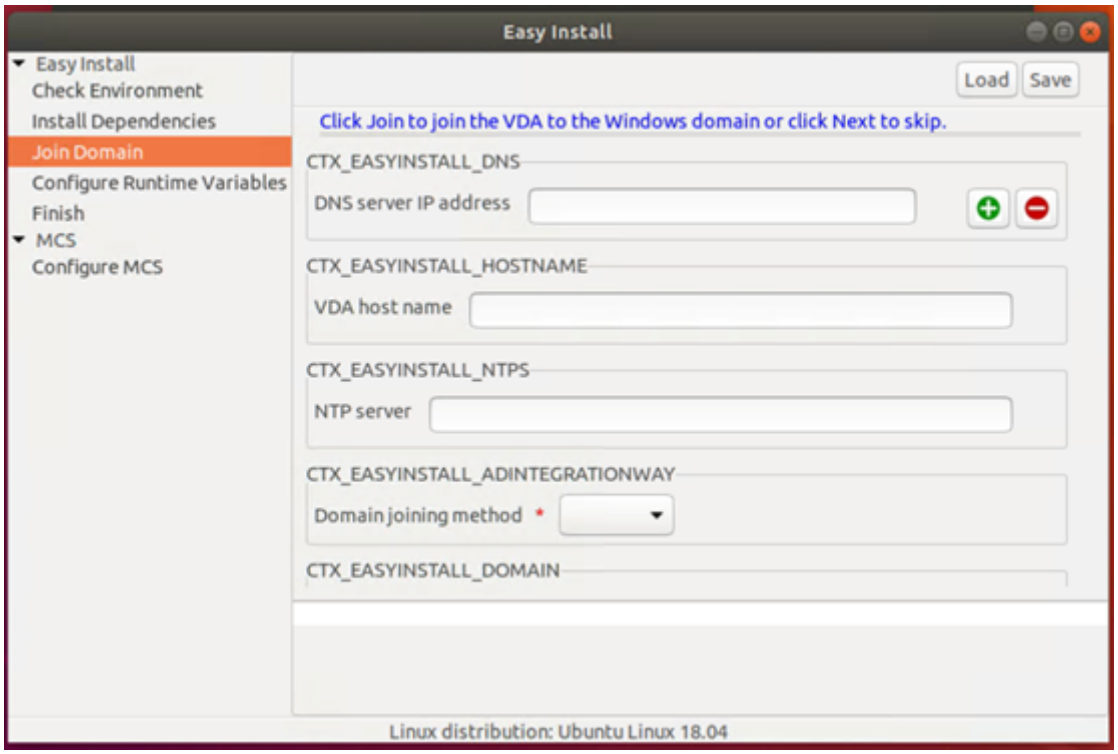
Sie müssen die Option **-E** mit dem Befehl “sudo”angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.

Alternativ können Sie alle Variablen mit einem einzigen Befehl festlegen.

Um die VDA-Laufumgebungsvariablen einzurichten (sie beginnen mit **CTX_XDL_**), können Sie **ctxinstall.sh -s** ausführen (der Buchstabe **s** wird hier **klein** geschrieben).

Grafische Benutzeroberfläche (GUI)

Wenn Sie SSSD oder Winbind für den Domänenbeitritt verwenden, können Sie Easy Install über eine GUI verwenden. Führen Sie den Befehl **/opt/Citrix/VDA/bin/easyinstall** in der Desktopumgebung Ihres VDA aus und folgen Sie dann den Anweisungen in der GUI für Easy Install.



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

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

> **Tipp:**
>
> - Klicken Sie auf **Speichern**, um Variableneinstellungen in einer lokalen Datei unter dem von Ihnen angegebenen Pfad zu speichern. Klicken Sie auf **Laden**, um Variableneinstellungen aus einer von Ihnen angegebenen Datei zu laden. Informationen zur Konfiguration von MCS-Variablen finden Sie unter Schritt 3: Vorbereiten eines Masterimages.
> - Das Skript ctxinstall.sh speichert alle Variableneinstellungen bis auf das Kennwort für den Domänenbeitritt in **/Citrix/VDA/sbin/ctxinstall.conf**.

Schritt 9: Ausführen von XDPing

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

Schritt 10: Ausführen des Linux VDA

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo systemctl start ctxhdx.service

sudo systemctl start ctxvda.service
<!--NeedCopy-->
```

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
sudo systemctl stop ctxvda.service

sudo systemctl stop ctxhdx.service
<!--NeedCopy-->
```

> **Hinweis:**
>
> Führen Sie erst den Befehl **systemctl stop ctxmonitord** aus, um den Monitor Service Daemon zu stoppen, bevor Sie die Dienste **ctxvda** und **ctxhdx** stoppen. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo systemctl stop ctxvda.service

sudo systemctl restart ctxhdx.service

sudo systemctl start ctxvda.service
<!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda.service

sudo systemctl status ctxhdx.service
<!--NeedCopy-->
```


Schritt 11: Maschinenkataloge erstellen

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

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

- Auswahl des Betriebssystems:
  - Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

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

Schritt 12: Bereitstellungsgruppen erstellen

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

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

- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.

- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

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

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2308.

Schritt 13: Upgrade des Linux VDA (optional)

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

RHEL 7 und CentOS 7:

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

RHEL 8 und Rocky Linux 8:

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

RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

> **Hinweis:**
>
> Aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher, bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 aktualisieren.

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

SUSE:

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

Ubuntu 20.04:

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

Ubuntu 22.04:


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

Problembehandlung

Verwenden Sie die Informationen in diesem Abschnitt, um Probleme zu beheben, die sich aus der Verwendung des Features Easy Install ergeben können.

Fehler beim Beitreten zu einer Domäne mit SSSD

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

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

/var/log/xdl/vda.log:

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



```
2016-11-04 02:11:52.364 [ERROR] - Could not register with any
    controllers. Waiting to try again in 120000 ms. Multi-forest - false
2016-11-04 02:11:52.365 [INFO ] - The Citrix Desktop Service failed to
    register with any controllers in the last 470 minutes.
<!--NeedCopy-->
```

/var/log/messages:

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

Lösen des Problems:

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

Grauer Bildschirm bei Ubuntu Desktopsitzungen

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

Lösen des Problems:

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

Ubuntu-Desktopsitzungen können aufgrund des fehlenden Basisverzeichnisses nicht gestartet werden

/var/log/xdl/hdx.log:

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

```

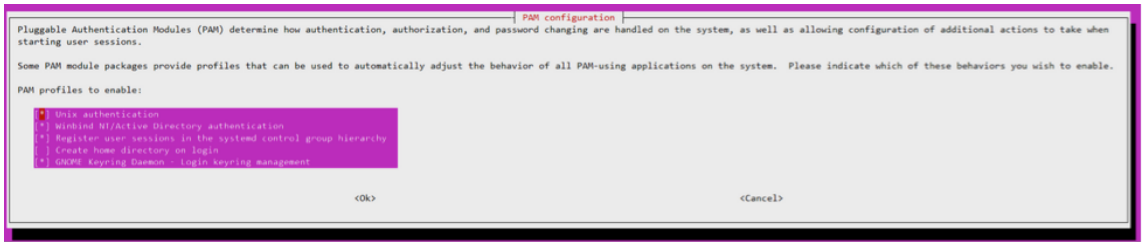


```
2016-11-02 13:21:19.017 <P22227> citrix-ctxhdx: logSessionEvent:
    Session started for user ctxadmin.

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

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

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

Lösen des Problems:

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



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

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

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

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

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

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

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

```



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

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

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

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

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

SELinux verhindert den Zugriff auf das Homeverzeichnis durch SSHD

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

/var/log/xdl/ctxinstall.log:

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



```
    complete SELinux messages. run sealert -l 32f52c1f-8ff9-4566-a698
    -963a79f16b81

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

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

If you want to allow polyinstantiation to enabled

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

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

    Do

       setsebool -P polyinstantiation_enabled 1

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

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

Then you should report this as a bug.

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

      Do

       allow this access for now by executing:

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

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

Lösen des Problems:

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

   SELINUX=disabled

2. Starten Sie den VDA neu.

Nicht domänengebundene Linux VDAs erstellen

January 8, 2024

In diesem Artikel erfahren Sie, wie Sie die Maschinenerstellungsdienste (MCS) verwenden, um nicht domänengebundene Linux-VDAs in Citrix DaaS zu erstellen.

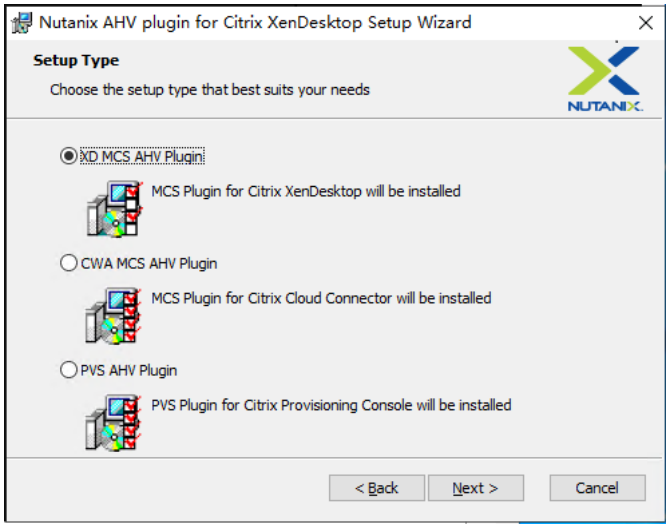
> **Wichtig:**
>
> - Nicht domänengebundene VDAs werden nur in Citrix DaaS unterstützt.
>   - Ihre Steuerungsebene muss über Citrix DaaS bereitgestellt werden.
>   - Sie können nicht domänengebundene VDAs in einer öffentlichen Cloud oder einem On-Premises-Datencenter bereitstellen. Nicht domänengebundene VDAs werden von der Steuerungsebene in Citrix DaaS verwaltet.
>   - Sie können Rendezvous V2 so konfigurieren, dass Citrix Cloud Connectors umgangen werden. Andernfalls müssen Sie Cloud Connectors installieren, um VDAs mit Ihrer Steuerungsebene zu verbinden.
> - Um VDAs zu erstellen, die nicht domänengebunden sind, müssen Sie die Maschinenerstellungsdienste (MCS) verwenden.
>   - Bare-Metal-Server werden von den Maschinenerstellungsdiensten nicht unterstützt.
> - Für nicht domänengebundene Linux VDAs sind folgende Features verfügbar:
>   - Lokaler Benutzer mit angegebenen Attributen auf nicht domänengebundenen VDAs erstellen
>   - Authentifizierung ohne Single Sign-On
>   - Authentifizierung mit Azure Active Directory
>   - Rendezvous V2

Schritt 1 (nur für Nutanix): Installieren und Registrieren des Nutanix-AHV-Plug-Ins

Beschaffen Sie das Nutanix AHV Plug-In-Paket von Nutanix. Installieren und registrieren Sie das Plug-In in der Citrix Virtual Apps and Desktops-Umgebung. Weitere Informationen finden Sie in der Installationsdokumentation zum Nutanix Acropolis MCS-Plug-In, verfügbar im Nutanix Support Portal.

Schritt 1a: Installieren und Registrieren des Nutanix AHV-Plug-Ins für On-Premises-Delivery Controller

Nach Installation von Citrix Virtual Apps and Desktops wählen und installieren Sie **XD MCS AHV Plugin** auf den Delivery Controllern.



Schritt 1b: Installieren und Registrieren des Nutanix AHV-Plug-Ins für Cloud-Delivery Controller

Wählen und installieren Sie **CWA MCS AHV Plugin** für Citrix Cloud Connectors. Installieren Sie das Plug-In auf allen Citrix Cloud Connectors, die beim Citrix Cloud-Mandanten registriert sind. Sie müssen Citrix Cloud Connectors auch dann registrieren, wenn sie einen Ressourcenstandort ohne AHV bereitstellen.

Schritt 1c: Ausführen der nachfolgend aufgeführten Schritte nach der Plug-In-Installation

- Vergewissern Sie sich, dass in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0` ein Nutanix Acropolis-Ordner erstellt wurde.
- Führen Sie den Befehl `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe"-PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"` aus.
- Starten Sie den Citrix Host, Citrix Broker und Citrix Maschinenerstellungsdienste auf den On-Premises-Delivery Controllern neu bzw. starten Sie auf Citrix Cloud Connectors Citrix Remote-HCLServer neu.

  > **Tipp:**
  >
  > Wir empfehlen, den Citrix Host, den Citrix Broker und Maschinenerstellungsdienste zu beenden und neu zu starten, wenn Sie das Nutanix-AHV-Plug-In installieren oder aktualisieren.

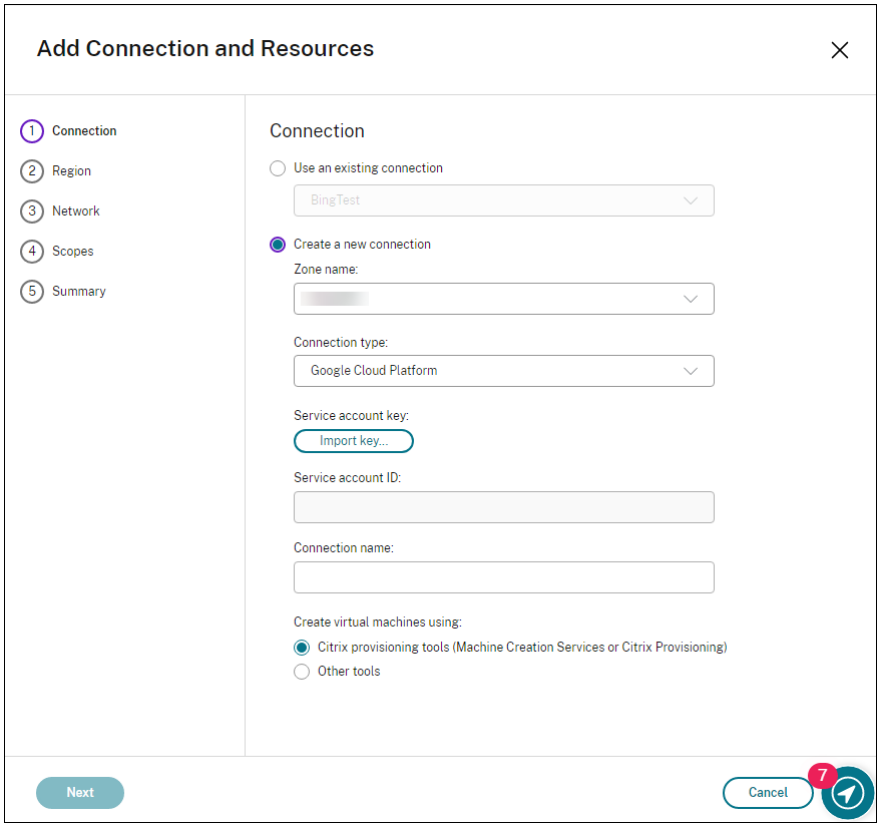
Schritt 2: Erstellen einer Hostverbindung

Hosts sind Hypervisors oder Cloudservices, die an Ihren Ressourcenstandorten verwendet werden. In diesem Schritt können Sie Informationen angeben, die DaaS für die Kommunikation mit VMs auf einem Host verwendet. Zu den detaillierten Informationen gehören der Ressourcenstandort, der Hosttyp, die Anmeldeinformationen für den Zugriff, die zu verwendende Speichermethode und die Netzwerke, die die VMs auf dem Host verwenden können.

> **Wichtig:**
>
> Die Hostressourcen (Speicher und Netzwerk) am Ressourcenstandort müssen verfügbar sein, bevor Sie eine Verbindung erstellen.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste die Option **Verbindung und Ressourcen hinzufügen**.
5. Der Assistent führt Sie durch die folgenden Seiten. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Wenn Sie mit einer Seite fertig sind, wählen Sie jeweils **Weiter**, bis Sie zur letzten Seite **Zusammenfassung** gelangen.

Schritt 2a: Verbindung



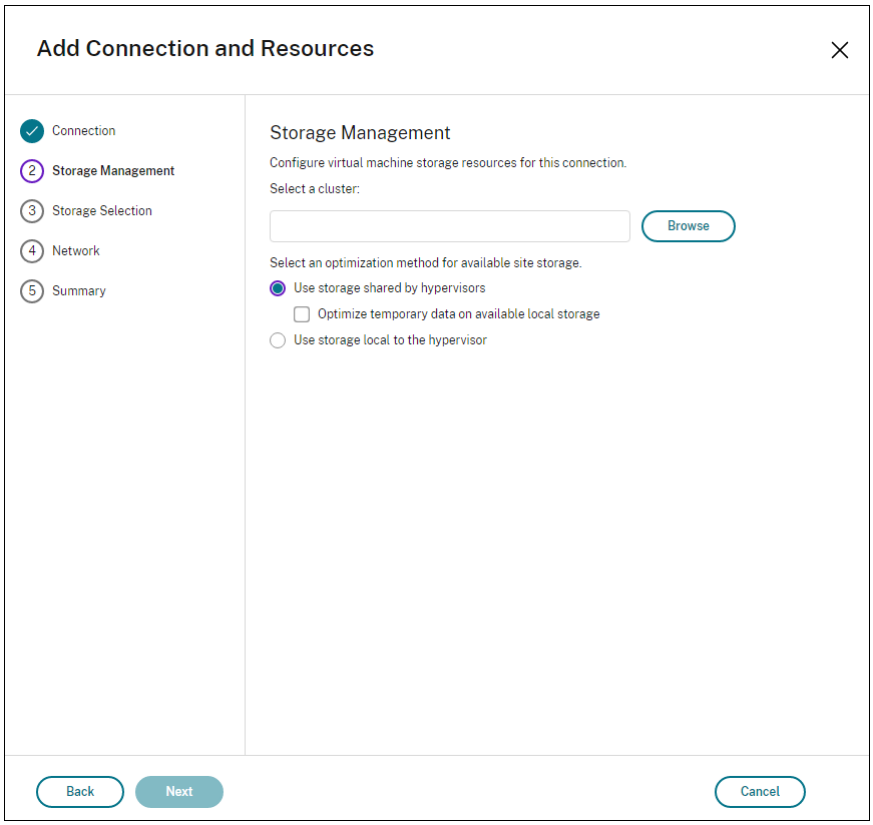
Auf der Seite **Verbindung**:

- Um eine Verbindung zu erstellen, wählen Sie **Neue Verbindung erstellen**. Um eine Verbindung zu erstellen, die auf derselben Hostkonfiguration wie eine bestehende Verbindung basiert, klicken Sie **Vorhandene Verbindung verwenden** und wählen dann die entsprechende Verbindung.
- Wählen Sie im Feld **Zonenname** eine Zone. Die Optionen sind alle von Ihnen konfigurierten Ressourcenstandorte.
- Wählen Sie im Feld **Verbindungstyp** den Hypervisor oder Clouddienst. Die Optionen sind Hypervisors und Cloudservices, deren Plug-ins ordnungsgemäß in der Zone installiert sind. Alternativ können Sie mit dem PowerShell-Befehl `Get-HypHypervisorPlugin -ZoneUid` die Liste der Hypervisor-Plug-ins abrufen, die in der ausgewählten Zone verfügbar sind.
- Geben Sie einen Verbindungsnamen ein. Dieser Name wird in der **Verwaltungsanzeige** angezeigt.
- Wählen Sie das Tool zur Erstellung virtueller Maschinen: Maschinenerstellungsdienste oder Citrix Provisioning.

Die Informationen auf der Seite **Verbindung** variieren je nach verwendetem Host (Verbindungstyp).

Wenn Sie beispielsweise Azure Resource Manager verwenden, können Sie einen vorhandenen Dienstprinzipal verwenden oder einen erstellen.

Schritt 2b: Speicherverwaltung



Informationen zur Speicherverwaltungstypen und -methoden finden Sie unter Hostspeicher.

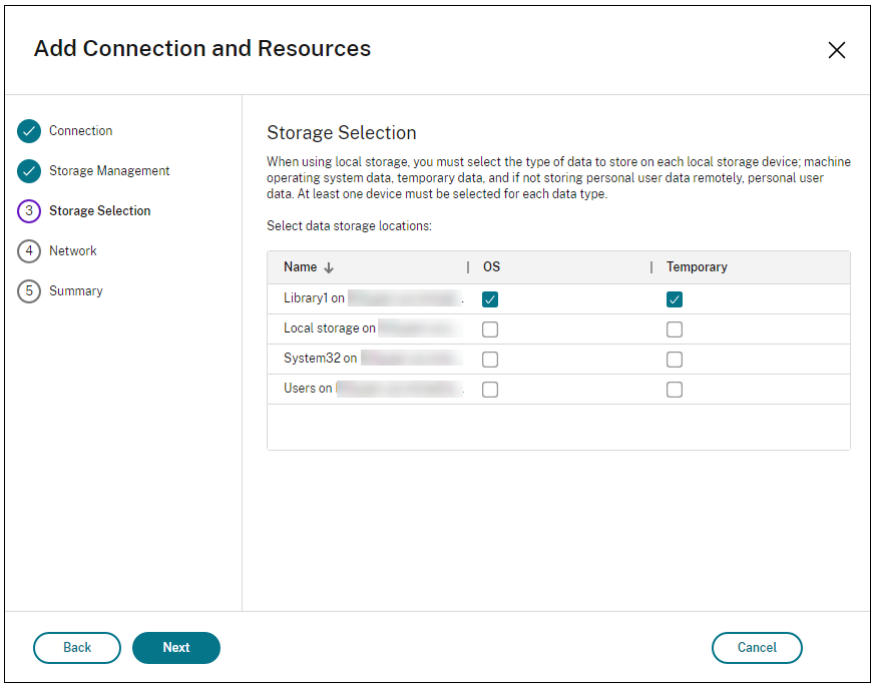
Wenn Sie eine Verbindung zu einem Hyper-V- oder VMware-Host konfigurieren, navigieren Sie zu einem Clusternamen und wählen Sie ihn aus. Andere Verbindungstypen erfordern keine Clusternamen.

Wählen Sie eine Speicherverwaltungsmethode: für Hypervisors freigegebener Speicher oder lokaler Speicher auf dem Hypervisor.

- Wenn Sie für Hypervisors freigegebenen Speicher wählen, geben Sie an, ob temporäre Daten im verfügbaren lokalen Speicher gespeichert werden sollen. (Sie können benutzerdefinierte temporäre Speichergrößen in den Maschinenkatalogen angeben, die diese Verbindung verwenden.) **Ausnahme:** Wenn Sie geclusterte Speichervolumes (CSV) verwenden, gestattet Microsoft System Center Virtual Machine Manager kein Erstellen von temporären Datenträgercaches im lokalen Speicher. Versuche, dieses Speicherverwaltungssetup in der **Verwaltungskonsole** zu konfigurieren, schlagen fehl.

Wenn Sie freigegebenen Speicher in einem Citrix Hypervisor-Pool verwenden, geben Sie an, ob Sie IntelliCache zum Reduzieren der Last auf dem freigegebenen Speichergerät verwenden. Siehe Citrix Hypervisor-Virtualisierungsumgebungen.

Schritt 2c: Speicherauswahl



Weitere Informationen zur Speicherauswahl finden Sie unter Hostspeicher.

Wählen Sie mindestens ein Hostspeichergerät für jeden verfügbaren Datentyp. Die auf der vorherigen Seite ausgewählte Speicherverwaltungsmethode bestimmt, welche Datentypen Sie auf dieser Seite auswählen können. Wählen Sie mindestens ein Speichergerät für jeden unterstützten Datentyp, bevor Sie mit der nächsten Seite im Assistenten fortfahren.

Der untere Teil der Seite **Speicherauswahl** enthält weitere Konfigurationsoptionen, wenn Sie von Hypervisors freigegebenen Speicher gewählt und **Temporäre Daten in verfügbarem lokalem Speicher optimieren** aktivieren. Sie können die lokalen Speichergeräte (im gleichen Hypervisorpool) für temporäre Daten auswählen.

Die Anzahl der zurzeit ausgewählten Speichergeräte wird angezeigt (siehe Abbildung: "1 Speichergerät ausgewählt"). Wenn Sie mit dem Mauszeiger darauf zeigen, werden die Namen der ausgewählten Geräte angezeigt, es sei denn, es sind keine Geräte konfiguriert.

1. Wählen Sie **Auswählen**, um die verwendeten Speichergeräte zu ändern.
2. Aktivieren oder deaktivieren Sie im Dialogfeld **Speicher auswählen** die Kontrollkästchen für Speichergeräte, und wählen Sie **OK**.

Schritt 2d: Region

(Nur für einige Hosttypen angezeigt.) Die Auswahl der Region gibt an, wo VMs bereitgestellt werden. Wählen Sie im Idealfall eine Region in der Nähe des Standorts, an dem die Benutzer auf ihre Anwendungen zugreifen.

Schritt 2e: Netzwerk

Geben Sie einen Namen für die Ressourcen ein. Dieser Name wird in der **Verwaltungskonsole** angezeigt, um die Speicher- und Netzwerkkombination zu identifizieren, die der Verbindung zugeordnet sind.
Wählen Sie mindestens ein Netzwerk für die VMs aus.

Für manche Verbindungstypen (z. B. Azure Resource Manager) werden außerdem von den VMs verwendete Subnetze aufgeführt. Wählen Sie mindestens ein Subnetz aus.

Schritt 2f: Zusammenfassung

Überprüfen Sie Ihre Auswahl. Wenn Sie Änderungen vornehmen möchten, kehren Sie zu den vorherigen Seiten des Assistenten zurück. Wählen Sie zum Abschluss **Fertig stellen**.

Nicht vergessen: Wenn Sie temporäre Daten lokal speichern, können Sie benutzerdefinierte Werte für den temporären Datenspeicher konfigurieren, wenn Sie den Katalog mit den Maschinen für diese Verbindung erstellen.

> **Hinweis:**
>
> Für Administratoren mit Vollzugriff wird kein Geltungsbereich angezeigt. Weitere Informationen finden Sie unter Administratoren, Rollen und Geltungsbereiche.

Weitere Informationen finden Sie unter Verbindungen erstellen und verwalten.

Schritt 3: Masterimage vorbereiten

> **Tipp:**
>
> Sie können ein einzelnes Image zum Erstellen von VDAs sowohl mit als auch ohne Domäneneinbindung verwenden.

(Nur für Citrix Hypervisor) Schritt 3a: Citrix VM Tools installieren

Installieren Sie Citrix VM Tools auf der Vorlagen-VM für jede VM, die die xe-Befehlszeilenschnittstelle oder XenCenter verwenden soll. Die VM kann langsam sein, wenn Sie die Tools nicht installieren. Folgende Schritte sind ohne diese Tools nicht möglich:

- Herunterfahren, Neustarten oder Anhalten einer VM.
- Anzeige der VM-Leistungsdaten in XenCenter.
- Migrieren einer ausgeführten VM (über XenMotion).
- Erstellen von Prüfpunkten (Snapshots mit oder ohne Arbeitsspeicher) und Wiederherstellen der Snapshots
- Anpassen der Anzahl der vCPUs auf einer laufenden Linux-VM.

1. Führen Sie folgenden Befehl aus, um Citrix VM Tools bereitzustellen (Dateiname: guest-tools.iso).

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

2. Führen Sie je nach Linux-Distribution folgenden Befehl aus, um das Paket xe-guest-utilities zu installieren.

   RHEL/CentOS/Rocky Linux:

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

   Ubuntu/Debian:

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

   SUSE:

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

3. Überprüfen Sie den Virtualisierungsstatus der Vorlagen-VM auf der Registerkarte **Allgemein** in XenCenter. Wenn Citrix VM Tools ordnungsgemäß installiert sind, wird der Virtualisierungsstatus als **Optimiert** angezeigt.

Schritt 3b: Installieren des Linux VDA-Pakets auf der Vorlagen-VM

> **Hinweis:**
>
> Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden möchten, lassen Sie diesen Schritt aus.
>
> Installieren Sie .NET Runtime 6.0, bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren.

Führen Sie gemäß Ihrer Linux-Distribution folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

RHEL/CentOS/Rocky Linux:

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

> **Hinweis:**
>
> Installieren Sie für RHEL und CentOS das EPEL-Repository, bevor Sie den Linux VDA installieren und `deploymcs.sh` erfolgreich ausführen können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter https://docs.fedoraproject.org/en-US/epel/.
>
> - Nach der Installation des Linux VDA auf RHEL 8.x/9.x oder Rocky Linux 8.x/9.x, das auf GCP gehostet wird, wird die Ethernetverbindung möglicherweise unterbrochen und der Linux VDA ist nach einem VM-Neustart u. U. nicht erreichbar. Führen Sie als Workaround die folgenden Befehle aus, bevor Sie die VM neu starten:
>
>   ```
>   nmcli dev connect eth0
>   service NetworkManager restart
>   <!--NeedCopy-->
>   ```

Ubuntu/Debian:

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

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

SUSE:

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

Schritt 3c: Repositorys zur Installation des tdb-tools-Pakets aktivieren (nur für RHEL 7)

RHEL 7-Server:


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

RHEL 7-Arbeitsstation:

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

Schritt 3d (SUSE): Manuelle Installation von ntfs-3g

Unter SUSE gibt es kein Repository, das ntfs-3g bereitstellt. Laden Sie den Quellcode herunter, führen Sie die Kompilation aus und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC) Compiler-System und das make-Paket:

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

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

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

Schritt 3e: Zu verwendende Datenbank angeben

Als experimentelles Feature können Sie SQLite zusätzlich zu PostgreSQL verwenden. Sie können nach der Installation des Linux VDA-Pakets auch zwischen SQLite und PostgreSQL wechseln. Führen Sie hierzu die folgenden Schritte aus:

1. Führen Sie `/opt/Citrix/VDA/sbin/ctxcleanup.sh` aus. Lassen Sie diesen Schritt aus, wenn es sich um eine Neuinstallation handelt.

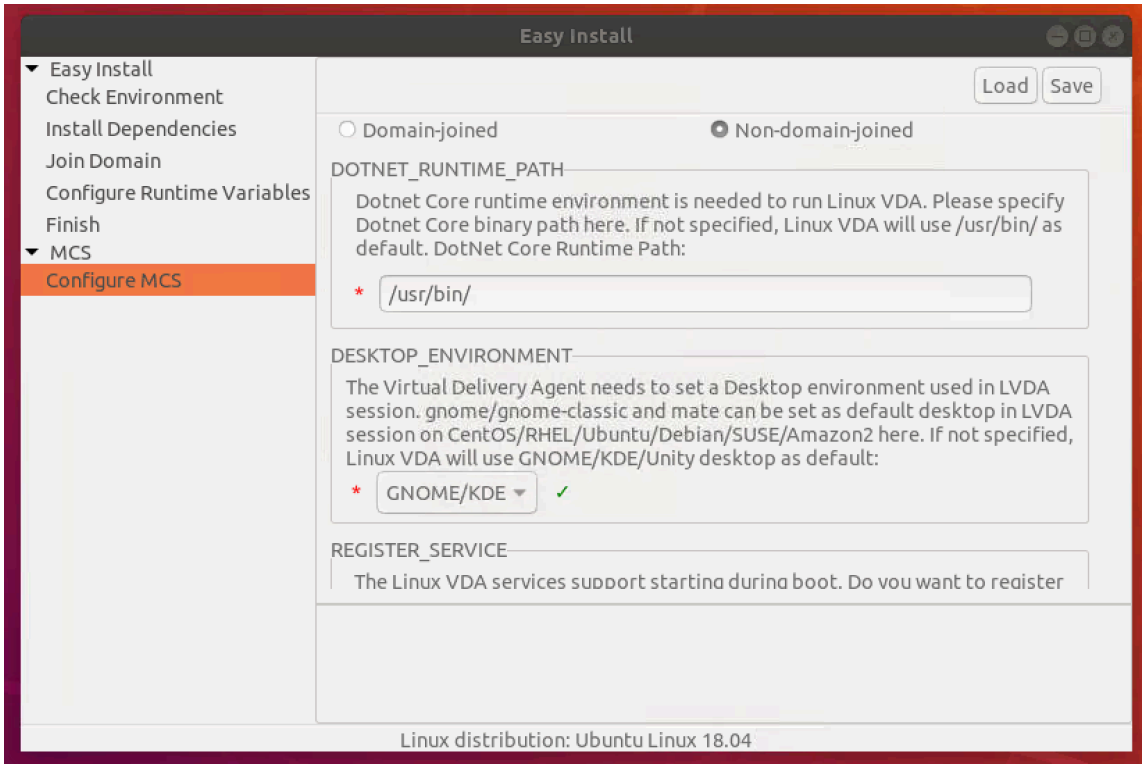
2. Bearbeiten Sie `/etc/xdl/db.conf`, bevor Sie `deploymcs.sh` ausführen.

> **Hinweis:**
>
> - Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.
> - Bei Easy Install und den Maschinenerstellungsdiensten (MCS) können Sie zwischen SQLite und PostgreSQL wechseln, ohne die Systeme manuell installieren zu müssen. Sofern nicht anders durch `/etc/xdl/db.conf` angegeben, verwendet der Linux VDA standardmäßig PostgreSQL.
> - Sie können auch `/etc/xdl/db.conf` verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

Schritt 3f: MCS-Variablen konfigurieren

Es gibt zwei Möglichkeiten zum Konfigurieren von MCS-Variablen:

- Bearbeiten Sie die `/etc/xdl/mcs/mcs.conf`-Datei.
- Verwenden Sie die GUI für Easy Install. Führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktopumgebung Ihres Linux VDA aus, um die GUI für Easy Install zu öffnen.



> **Tipp:**
>
> Klicken Sie auf **Speichern**, um Variableneinstellungen in einer lokalen Datei unter dem von Ihnen angegebenen Pfad zu speichern. Klicken Sie auf **Laden**, um Variableneinstellungen aus einer von Ihnen angegebenen Datei zu laden.

Die folgenden MCS-Variablen können Sie für Szenarios ohne Domäneneinbindung konfigurieren: Sie können die Standardwerte der Variablen verwenden oder die Variablen nach Bedarf anpassen (optional):

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

Schritt 3g: Registrierungswerte für die Maschinenerstellungsdienste (MCS) schreiben oder aktualisieren (optional)

Fügen Sie auf der Vorlagenmaschine der Datei `/etc/xdl/mcs/mcs_local_setting.reg` Befehlszeilen hinzu, um Registrierungswerte nach Bedarf zu schreiben oder zu aktualisieren. Diese Aktion verhindert den Verlust von Daten und Einstellungen bei jedem Neustart einer von MCS-Provisioningmaschine.

Jede Zeile in der Datei `/etc/xdl/mcs/mcs_local_setting.reg` ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

Beispielsweise können Sie der Datei `/etc/xdl/mcs/mcs_local_setting.reg` die folgenden Befehlszeilen hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

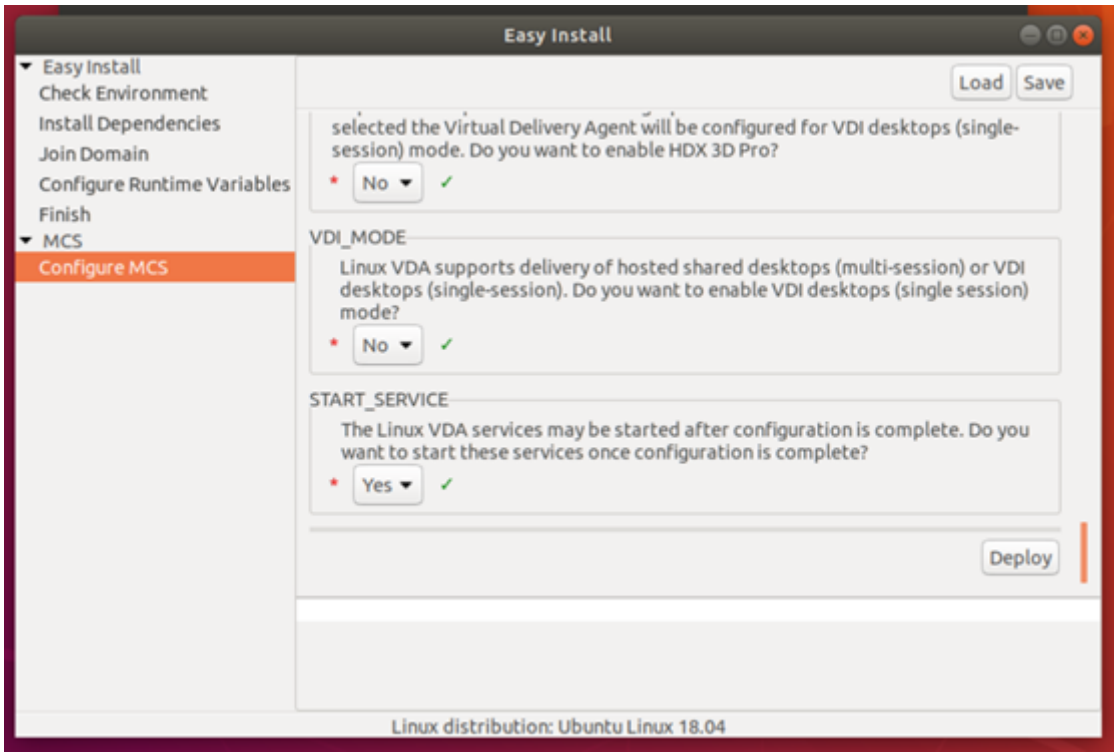
```
1 create -k "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels
     \Clipboard\ClipboardSelection" -t "REG_DWORD" -v "Flags" -d "0
     x00000003" --force
2 <!--NeedCopy-->
```

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

Schritt 3h: Erstellen eines Masterimages

1. Wenn Sie MCS-Variablen durch Bearbeiten von `/etc/xdl/mcs/mcs.conf` konfigurieren, führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus. Wenn Sie MCS-Variablen über

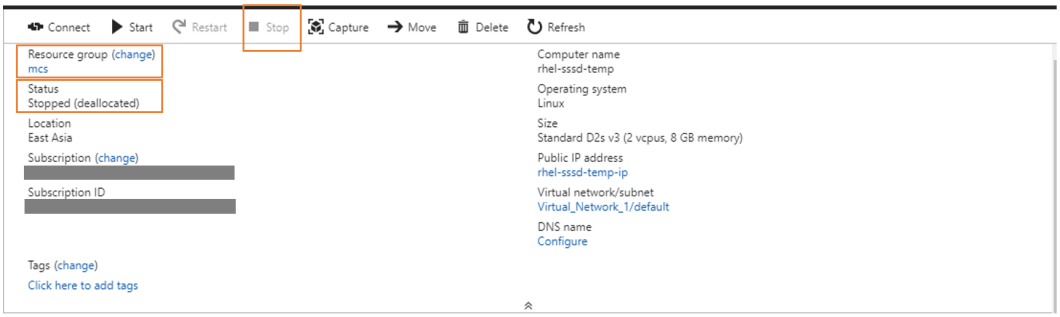
die GUI konfigurieren, klicken Sie auf **Bereitstellen**.



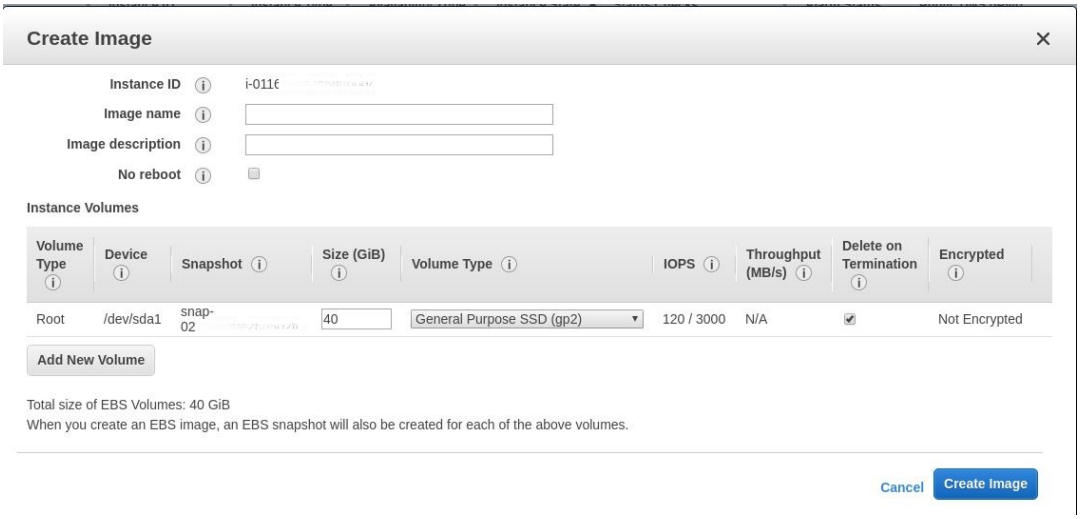
Nachdem Sie in der GUI auf **Bereitstellen** geklickt haben, werden die Variablen, die Sie in der Datei `/etc/xdl/mcs/mcs.conf` festgelegt haben, von den in der GUI festgelegten Variablen überschrieben.

2. Erstellen und benennen Sie einen Snapshot Ihres Masterimages basierend auf der von Ihnen verwendeten öffentlichen Cloud.

   - **(Citrix Hypervisor, GCP und VMware vSphere)** Installieren Sie Anwendungen auf der Vorlagen-VM, und fahren Sie die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages.
   - **(Azure)**: Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM vom Azure-Portal aus herunter. Stellen Sie sicher, dass der Energiestatus der Vorlagen-VM als **gestoppt (Zuordnung aufgehoben)** angezeigt wird. Merken Sie sich den Namen der Ressourcengruppe. Sie benötigen diesen Namen später, um Ihr Masterimage in Azure zu finden.



- **(AWS)** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM vom AWS EC2-Portal aus herunter. Stellen Sie sicher, dass der Instanzstatus der Vorlagen-VM als **gestoppt** angezeigt wird. Klicken Sie mit der rechten Maustaste auf die Vorlagen-VM und wählen Sie **Image > Image erstellen** aus. Geben Sie nach Bedarf Informationen ein und nehmen Sie die Einstellungen vor. Klicken Sie auf **Image erstellen**.



- **(Nutanix)** Fahren Sie unter Nutanix AHV die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages.

> **Hinweis:**
>
> Sie müssen den Namen von Acropolis-Snapshots zur Verwendung in Citrix Virtual Apps and Desktops `XD_` voranstellen. Verwenden Sie bei Bedarf die Acropolis-Konsole, um die Snapshots umzubenennen. Nach Umbenennen von Snapshots starten Sie den **Assistenten zum Erstellen von Katalogen** neu, damit eine aktualisierte Liste angezeigt wird.

Schritt 4: Maschinenkatalog erstellen

1. Melden Sie sich bei Citrix Cloud an.

2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** die Option **Maschinenkataloge** aus.
4. Der Assistent führt Sie durch das Erstellen eines Maschinenkatalogs.

   Wählen Sie auf der für Nutanix eindeutigen Seite **Container** den Container aus, den Sie zuvor für die Vorlagen-VM angegeben haben.

   Wählen Sie auf der Seite **Masterimage** den Snapshot des Images aus.

   Prüfen Sie auf der Seite **Virtuelle Maschinen** die Anzahl der virtuellen CPUs und die Anzahl der Kerne pro vCPU. Wählen Sie MCS als Methode zur Bereitstellung der Maschinen und wählen Sie **Gehört keiner Domäne an** als Identität für die im Katalog zu erstellenden Maschinen aus.

   Führen Sie nach Bedarf weitere Konfigurationsaufgaben aus. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

> **Hinweis:**
>
> Wenn die Erstellung des Maschinenkatalogs auf dem Delivery Controller lange dauert, fahren Sie in Nutanix Prism die Maschine mit dem Präfix **Preparation** manuell hoch. Dadurch wird der Erstellungsprozess fortgesetzt.

Schritt 5: Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Sie gibt die Benutzer an, die diese Maschinen verwenden können, und die für die Benutzer verfügbaren Anwendungen und Desktops. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

Linux VDAs über die Maschinenerstellungsdienste (MCS) erstellen

March 13, 2024

Mit MCS können Sie domänengebundene und nicht domänengebundene VDAs erstellen.

> **Wichtig:**
>
> Die folgenden wichtigen Änderungen gibt es ab Release 2212:
>
> - Diese **AD_INTEGRATION**-Variable in der Datei /etc/xdl/mcs/mcs.conf oder auf der GUI für Easy Install hat keinen Standardwert mehr. Sie müssen nach Bedarf einen Wert festlegen.

> Weitere Informationen finden Sie im Abschnitt Schritt 3h: MCS-Variablen konfigurieren in diesem Artikel.
> - Der gültige Wert des Eintrags **UPDATE_MACHINE_PW** in /etc/xdl/mcs/mcs.conf ist nicht mehr **aktiviert** oder **deaktiviert**, sondern **Y** oder **N**. Weitere Informationen finden Sie unter Kennwortaktualisierung für Maschinenkonten automatisieren in diesem Artikel.

Unterstützte Distributionen

	Winbind	SSSD	Centrify	PBIS
Debian 11.3	Ja	Ja	Nein	Ja
RHEL 9.2/9.0	Ja	Ja	Nein	Nein
RHEL 8.8/8.6	Ja	Ja	Ja	Ja
Rocky Linux 9.2/9.0	Ja	Ja	Nein	Nein
Rocky Linux 8.8/8.6	Ja	Ja	Nein	Nein
RHEL 7.9, CentOS 7.9	Ja	Ja	Ja	Ja
SUSE 15.4	Ja	Ja	Nein	Ja
Ubuntu 22.04, Ubuntu 20.04	Ja	Ja	Nein	Ja

> **Hinweis:**
>
> Um einen aktuell ausgeführten VDA mit RHEL 8.x/9.x oder Rocky Linux 8.x/9.x zu verwenden, der mit der Domäne verbunden ist und SSSD als Vorlagen-VM für MCS verwendet, stellen Sie Folgendes sicher:
>
> - Der VDA wurde manuell und nicht mithilfe von Easy Install installiert. Easy Install verwendet **Adcli** für RHEL 8.x/9.x und Rocky Linux 8.x/9.x und die Kombination von SSSD und **Adcli** wird von MCS nicht unterstützt.
> - Ein Samba-Server ist für die Verwendung von SSSD für die AD-Authentifizierung konfiguriert. Weitere Informationen finden Sie im Red Hat-Artikel unter https://access.redhat.com/solutions/3802321.

Unterstützte Hypervisors

- AWS

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

Das Vorbereiten des Masterimages auf einem anderen Hypervisor als den unterstützten kann zu unerwarteten Ergebnissen führen.

MCS zum Erstellen von Linux-VMs verwenden

Überlegungen

- Ab Release 2203 können Sie den Linux VDA auf Microsoft Azure, AWS und GCP für Citrix Virtual Apps and Desktops sowie auf Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) hosten. Um diese Verbindungen mit Hosts öffentlicher Clouds zu Ihrer Citrix Virtual Apps and Desktops-Bereitstellung hinzuzufügen, benötigen Sie eine Citrix Universal Subscription- oder eine Hybrid Rights-Lizenz. Informationen zu Universal Subscription- und Hybrid Rights-Lizenzen finden Sie unter Transition and Trade Up (TTU) mit Citrix Universal Subscription.
- Bare-Metal-Server werden nicht unterstützt, wenn MCS zum Erstellen virtueller Maschinen verwendet wird.
- Citrix verwendet die folgenden Centrify-Versionen für die Erstvalidierung der Features auf den relevanten Linux-Distributionen:

Linux-Distribution	Centrify-Version
RHEL 7/8	5.8.0
SUSE	5.7.1
Debian, Ubuntu	5.6.1

  Andere Versionen von Centrify können zu Fehlern führen. Verwenden Sie Centrify nicht, um eine Vorlagenmaschine einer Domäne hinzuzufügen.

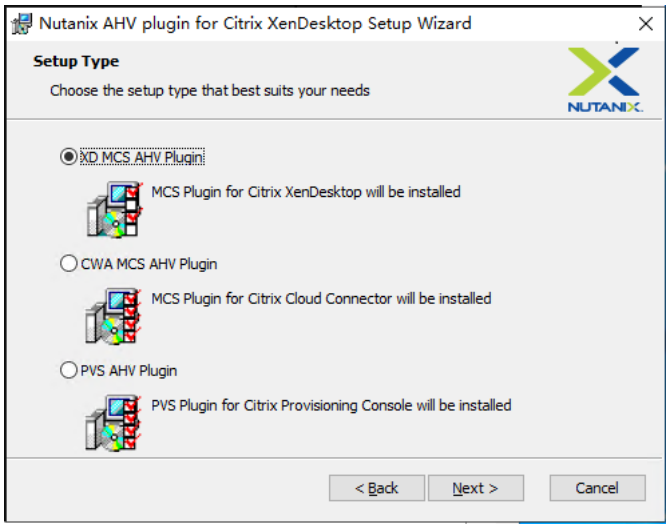
- Wenn Sie PBIS oder Centrify zum Hinzufügen von mit MCS erstellten Maschinen zu Windows-Domänen verwenden, führen Sie die folgenden Aufgaben aus:
  - Konfigurieren Sie auf der Vorlagenmaschine den Downloadpfad des PBIS- bzw. Centrify-Pakets in der Datei `/etc/xdl/mcs/mcs.conf` oder installieren Sie das Paket direkt.

- Erstellen Sie vor dem Ausführen von `/opt/Citrix/VDA/sbin/deploymcs.sh` eine Organisationseinheit mit Schreib- und Kennwortrücksetzberechtigung für alle untergeordneten, mit MCS erstellten Maschinen.
- Bevor Sie mit MCS erstellte Maschinen nach Abschluss der Ausführung von `/opt/Citrix/VDA/sbin/deploymcs.sh` neu starten, führen Sie je nach Bereitstellung `klist -li 0x3e4 purge` auf Ihrem Delivery Controller oder Citrix Cloud Connector aus.

Schritt 1 (nur für Nutanix): Installieren und Registrieren des Nutanix-AHV-Plug-Ins

Beschaffen Sie das Nutanix AHV Plug-In-Paket von Nutanix. Installieren und registrieren Sie das Plug-In in der Citrix Virtual Apps and Desktops-Umgebung. Weitere Informationen finden Sie in der Installationsdokumentation zum Nutanix Acropolis MCS-Plug-In, verfügbar im Nutanix Support Portal.

Schritt 1a: Installieren und Registrieren des Nutanix AHV-Plug-Ins für On-Premises-Delivery Controller Nach Installation von Citrix Virtual Apps and Desktops wählen und installieren Sie **XD MCS AHV Plugin** auf den Delivery Controllern.



Schritt 1b: Installieren und Registrieren des Nutanix AHV-Plug-Ins für Cloud-Delivery Controller Wählen und installieren Sie **CWA MCS AHV Plugin** für Citrix Cloud Connectors. Installieren Sie das Plug-In auf allen Citrix Cloud Connectors, die beim Citrix Cloud-Mandanten registriert sind. Sie müssen Citrix Cloud Connectors auch dann registrieren, wenn sie einen Ressourcenstandort ohne AHV bereitstellen.

Schritt 1c: Ausführen der nachfolgend aufgeführten Schritte nach der Plug-In-Installation

- Vergewissern Sie sich, dass in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0` ein Nutanix Acropolis-Ordner erstellt wurde.
- Führen Sie den Befehl `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe"-PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"` aus.
- Starten Sie den Citrix Host, Citrix Broker und Citrix Maschinenerstellungsdienste auf den On-Premises-Delivery Controllern neu bzw. starten Sie auf Citrix Cloud Connectors Citrix Remote-HCLServer neu.

  > **Tipp:**
  >
  > Wir empfehlen, den Citrix Host, den Citrix Broker und Maschinenerstellungsdienste zu beenden und neu zu starten, wenn Sie das Nutanix-AHV-Plug-In installieren oder aktualisieren.

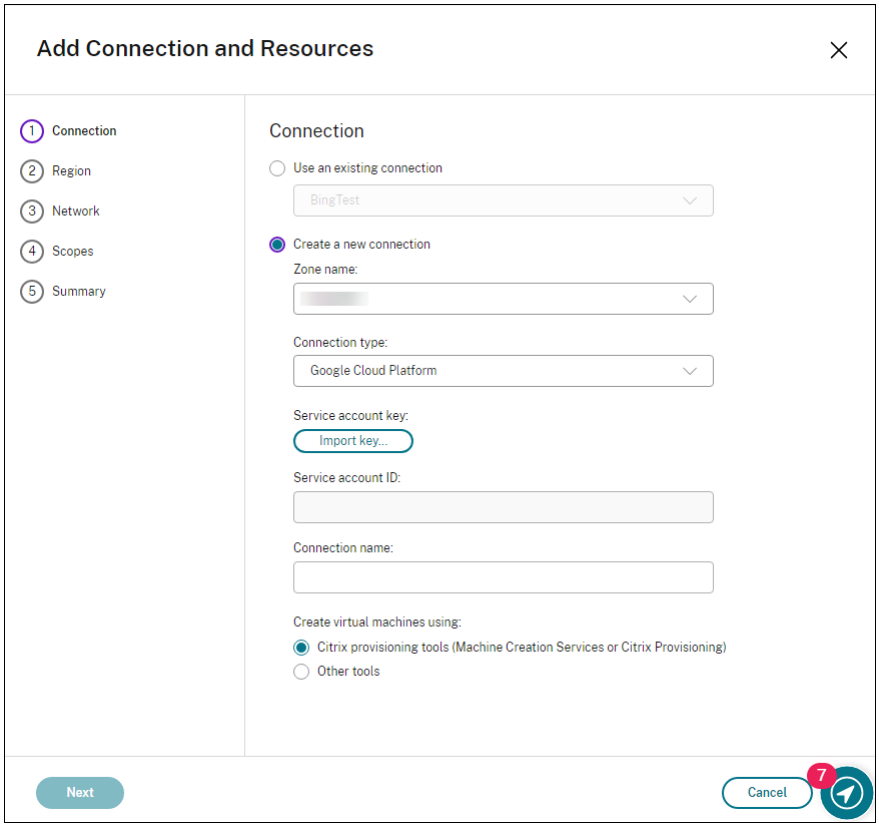
Schritt 2: Erstellen einer Hostverbindung

Dieser Abschnitt enthält Beispiele zum Erstellen einer Hostverbindung zu Azure, AWS, Citrix Hypervisor, GCP, Nutanix AHV und VMware vSphere. Weitere Informationen finden Sie unter Verbindungen und Ressourcen erstellen in der Dokumentation zu Citrix Virtual Apps and Desktops und Verbindungen erstellen und verwalten in der Citrix DaaS-Dokumentation.

- Hostverbindung zu Azure in Citrix Studio erstellen
- Hostverbindung zu AWS in Citrix Studio erstellen
- Hostverbindung zu Citrix Hypervisor in Citrix Studio erstellen
- Hostverbindung zu GCP in Citrix Studio erstellen
- Hostverbindung zu Nutanix in Citrix Studio erstellen
- Hostverbindung zu VMware in Citrix Studio erstellen

Hostverbindung zu Azure in Citrix Studio erstellen

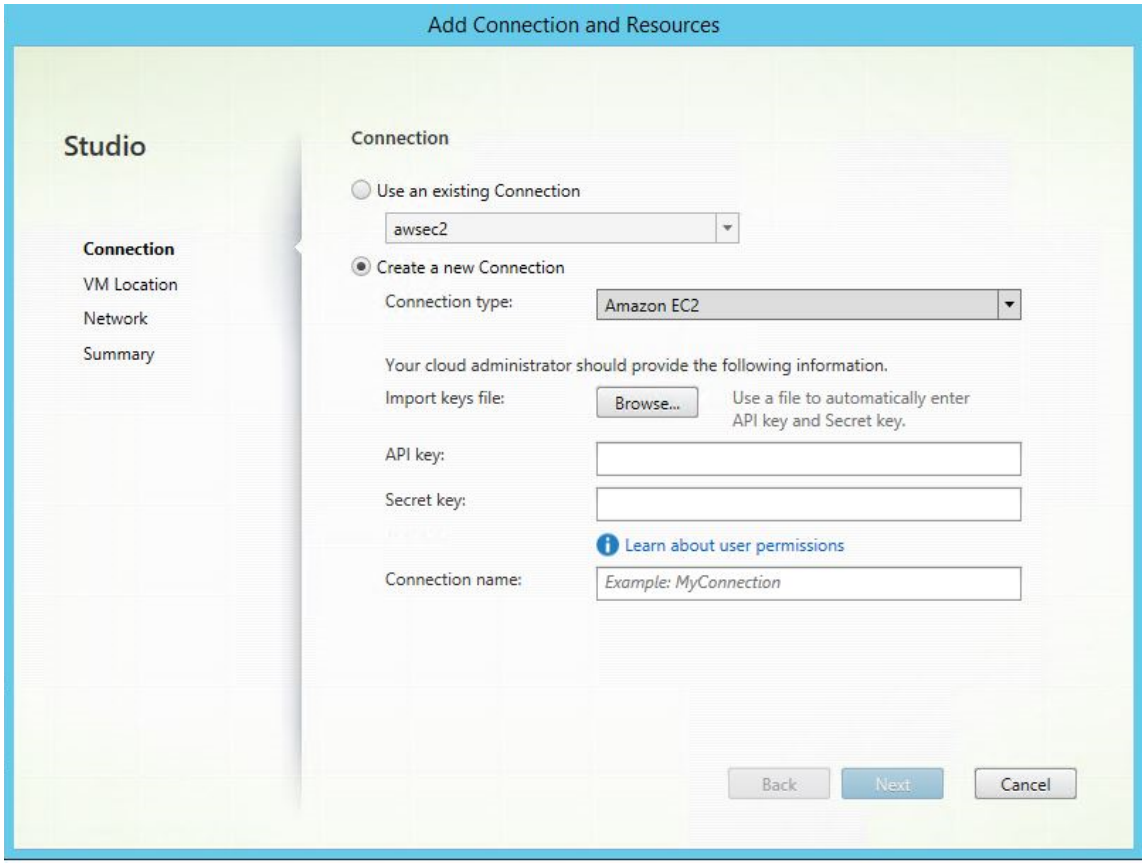
1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste **Verbindung und Ressourcen hinzufügen**.



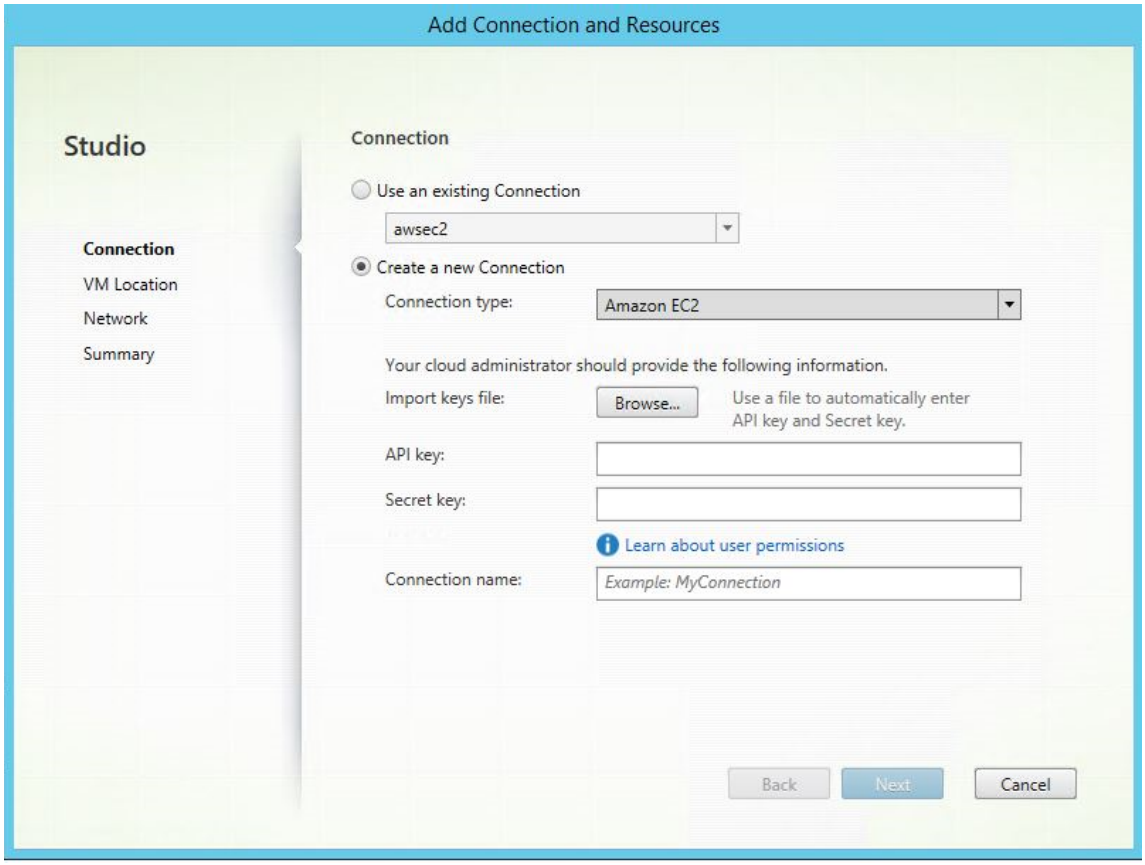
5. Wählen Sie als Verbindungstyp “Microsoft Azure”.
6. Der Assistent führt Sie durch die Seiten. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Wenn Sie mit einer Seite fertig sind, wählen Sie jeweils **Weiter**, bis Sie zur letzten Seite **Zusammenfassung** gelangen. Weitere Informationen finden Sie unter **Schritt 2: Hostverbindung erstellen** im Artikel Nicht domänengebundene Linux VDAs erstellen.

Hostverbindung zu AWS in Citrix Studio erstellen

1. Wählen Sie in Citrix Studio **Konfiguration** > **Hosting** > **Verbindung und Ressourcen hinzufügen**.
2. Wählen Sie als Verbindungstyp **Amazon EC2** aus.



3. Geben Sie den API-Schlüssel und den geheimen Schlüssel Ihres AWS-Kontos und Ihren Verbindungsnamen ein.



Der **API-Schlüssel** ist Ihre Zugriffsschlüssel-ID und der **geheime Schlüssel** ist Ihr geheimer Zugriffsschlüssel. Beide zusammen sind das Zugriffsschlüsselpaar. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, können Sie den Zugriffsschlüssel löschen und einen anderen erstellen. Gehen Sie folgendermaßen vor, um einen Zugriffsschlüssel zu erstellen:

a) Melden Sie sich bei AWS an.
b) Navigieren Sie zur IAM-Konsole (Identity and Access Management).
c) Wählen Sie im linken Navigationsbereich **Users** aus.
d) Wählen Sie den Zielbenutzer aus und scrollen Sie nach unten, um die Registerkarte **Security credentials** auszuwählen.
e) Scrollen Sie nach unten und klicken Sie auf **Create access key**. Ein neues Fenster wird angezeigt.
f) Klicken Sie auf **Download .csv file** und speichern Sie den Zugriffsschlüssel an einem sicheren Speicherort.

4. Der Assistent führt Sie durch die Seiten. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Wenn Sie mit einer Seite fertig sind, wählen Sie jeweils **Weiter**, bis Sie zur letzten Seite **Zusammenfassung** gelangen.

Hostverbindung zu Citrix Hypervisor in Citrix Studio erstellen

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste **Verbindung und Ressourcen hinzufügen**.
5. Wählen Sie **Citrix Hypervisor** als Verbindungstyp aus.
6. Geben Sie die Verbindungsadresse (die Citrix Hypervisor-URL) Ihres Citrix Hypervisor-Kontos, Ihren Benutzernamen und Ihr Kennwort sowie Ihren Verbindungsnamen ein.

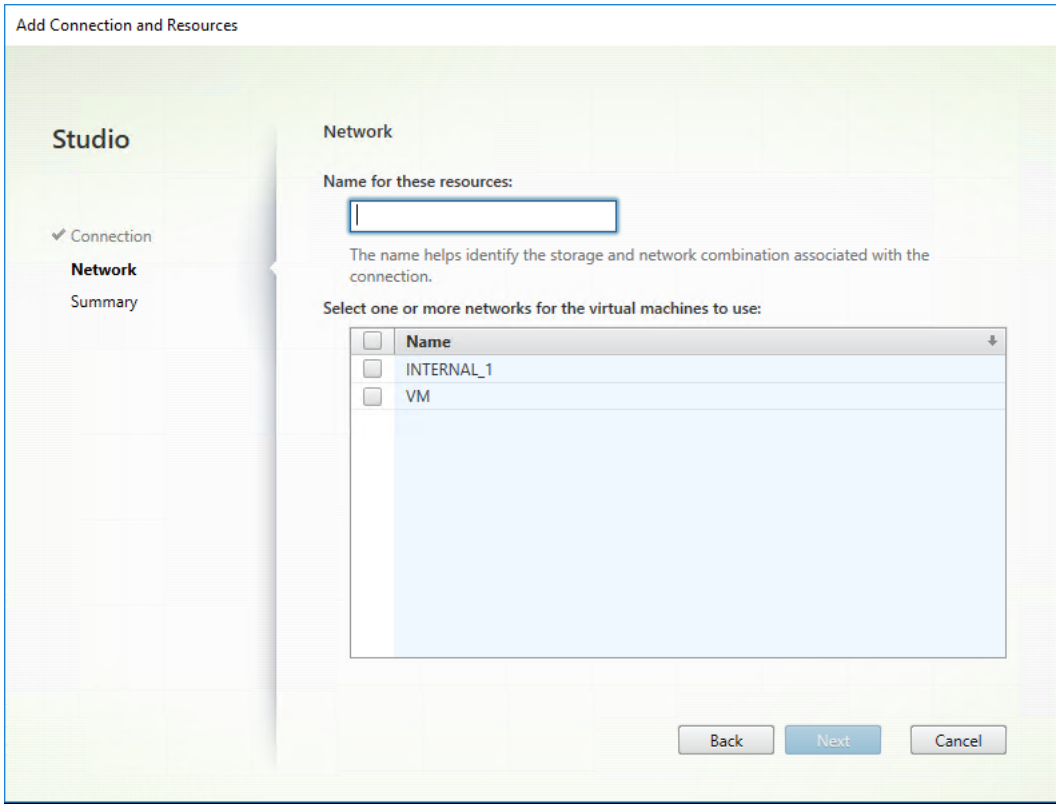
Hostverbindung zu GCP in Citrix Studio erstellen Richten Sie Ihre GCP-Umgebung gemäß Google Cloud Platform-Virtualisierungsumgebungen ein und führen Sie dann die folgenden Schritte aus, um eine Hostverbindung zu GCP herzustellen.

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste **Verbindung und Ressourcen hinzufügen**.
5. Wählen Sie als Verbindungstyp die Option **Google Cloud Platform**.
6. Importieren Sie den Dienstkontoschlüssel Ihres GCP-Kontos und geben Sie Ihren Verbindungsnamen ein.
7. Der Assistent führt Sie durch die Seiten. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Wenn Sie mit einer Seite fertig sind, wählen Sie jeweils **Weiter**, bis Sie zur letzten Seite **Zusammenfassung** gelangen. Weitere Informationen finden Sie unter **Schritt 2: Hostverbindung erstellen** im Artikel Nicht domänengebundene Linux VDAs erstellen.

Hostverbindung zu Nutanix in Citrix Studio erstellen

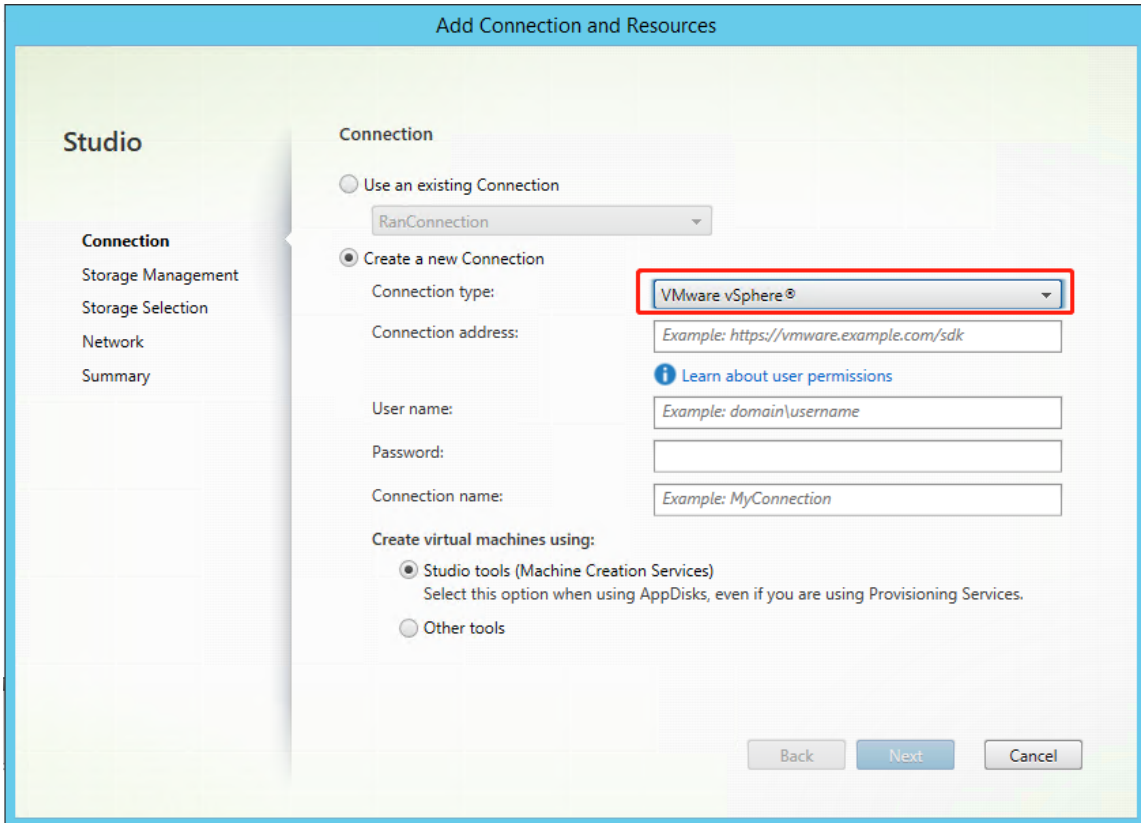
1. Wählen Sie für On-Premises-Delivery Controller im On-Premises-Citrix Studio **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**. Wählen Sie für Cloud-Delivery Controller **Verwalten > Hosting > Verbindung und Ressourcen hinzufügen** in der webbasierten Studio-Konsole in Citrix Cloud, um eine Verbindung zum Nutanix-Hypervisor herzustellen.
2. Wählen Sie im Assistenten zum Hinzufügen einer Verbindung und Ressourcen auf der Seite **Verbindung** den Verbindungstyp **Nutanix AHV**. Geben Sie dann die Hypervisoradresse und Anmeldeinformationen sowie Ihren Verbindungsnamen ein. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Einheit aus.

   Beispiel für On-Premises-Citrix Studio:

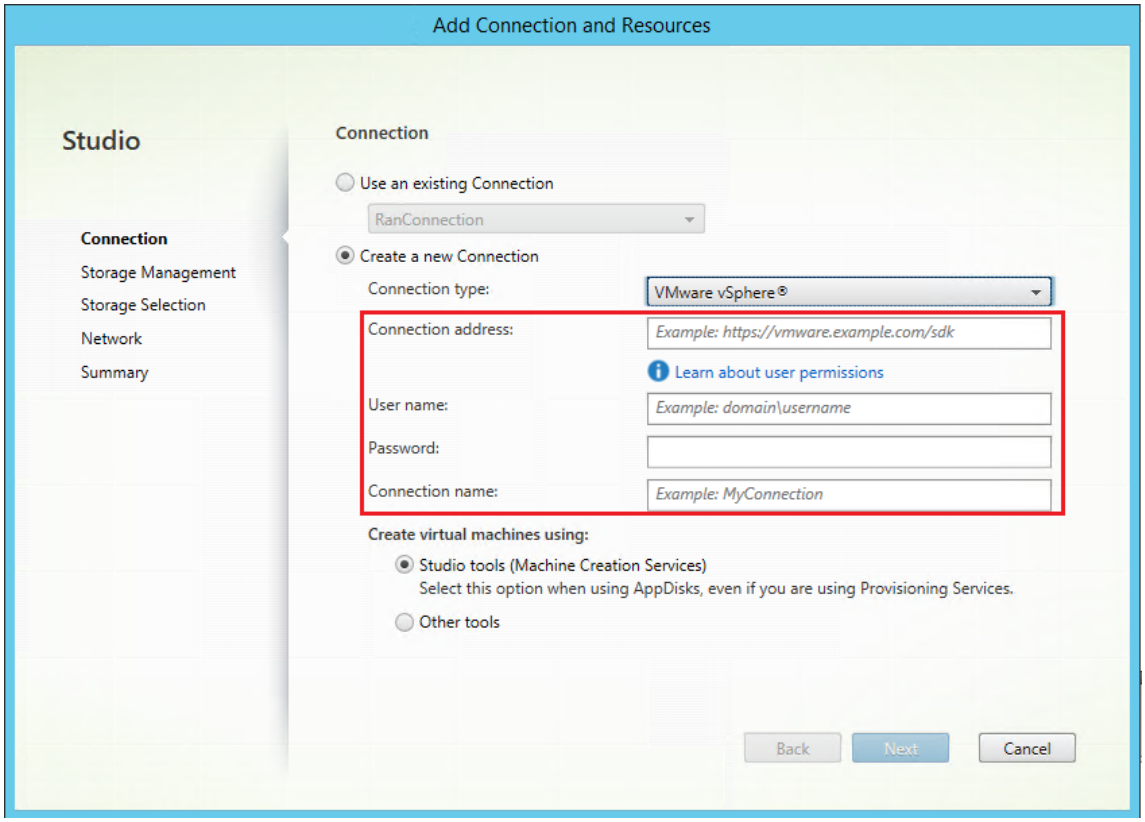


Hostverbindung zu VMware in Citrix Studio erstellen

1. Installieren Sie vCenter Server in der vSphere-Umgebung. Weitere Informationen finden Sie unter VMware vSphere.
2. Wählen Sie in Citrix Studio **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**.
3. Wählen Sie als Verbindungstyp “VMware vSphere”aus.



4. Geben Sie die Verbindungsadresse (die vCenter Server-URL) Ihres VMware-Kontos, Ihren Benutzernamen und Ihr Kennwort sowie Ihren Verbindungsnamen ein.



Schritt 3: Masterimage vorbereiten

(Nur für Citrix Hypervisor) Schritt 3a: Citrix VM Tools installieren Installieren Sie Citrix VM Tools auf der Vorlagen-VM für jede VM, die die xe-Befehlszeilenschnittstelle oder XenCenter verwenden soll. Die VM kann langsam sein, wenn Sie die Tools nicht installieren. Folgende Schritte sind ohne diese Tools nicht möglich:

- Herunterfahren, Neustarten oder Anhalten einer VM.
- Anzeige der VM-Leistungsdaten in XenCenter.
- Migrieren einer ausgeführten VM (über `XenMotion`).
- Erstellen von Prüfpunkten (Snapshots mit oder ohne Arbeitsspeicher) und Wiederherstellen der Snapshots
- Anpassen der Anzahl der vCPUs auf einer laufenden Linux-VM.

1. Führen Sie folgenden Befehl aus, um Citrix VM Tools bereitzustellen (Dateiname: guest-tools.iso).

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

2. Führen Sie je nach Linux-Distribution folgenden Befehl aus, um das Paket `xe-guest-utilities` zu installieren.

RHEL/CentOS/Rocky Linux:

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

Ubuntu/Debian:

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

SUSE:

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

3. Überprüfen Sie den Virtualisierungsstatus der Vorlagen-VM auf der Registerkarte **Allgemein** in XenCenter. Wenn Citrix VM Tools ordnungsgemäß installiert sind, wird der Virtualisierungsstatus als **Optimiert** angezeigt.

Schritt 3b: Konfigurationen für SUSE 15.4 in AWS, Azure und GCP überprüfen Für SUSE 15.4 in AWS, Azure und GCP ist Folgendes sicherzustellen:

- Sie verwenden **libstdc++6** Version 12 oder höher.
- Der Parameter **Default_WM** in **/etc/sysconfig/windowmanager** ist auf **"gnome"** gesetzt.

Schritt 3c: RDNS für Ubuntu 20.04 auf GCP deaktivieren Fügen Sie auf der Vorlagen-VM in /etc/krb5.conf die Zeile **rdns = false** unter **[libdefaults]** hinzu.

Schritt 3d: Linux VDA-Paket auf der Vorlagen-VM installieren

> **Hinweis:**
>
> - Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden möchten, lassen Sie diesen Schritt aus. Um einen aktuell ausgeführten VDA mit RHEL 8.x/9.x oder Rocky Linux 8.x/9.x zu verwenden, der mit der Domäne verbunden ist und SSSD als Vorlagen-VM verwendet, stellen Sie Folgendes sicher:
>
>   – The VDA is installed manually and not by using easy install. Easy install uses **Adcli** for RHEL 8.x/9.x and Rocky Linux 8.x/9.x and the combination of SSSD and **Adcli** is not supported by MCS.

> – A Samba server is configured to use SSSD for AD authentication. For more information, see the Red Hat article at https://access.redhat.com/solutions/3802321.
>
> • Installieren Sie .NET Runtime 6.0, bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren.

Führen Sie gemäß Ihrer Linux-Distribution folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

RHEL/CentOS/Rocky Linux:

> **Hinweis:**
>
> • Installieren Sie für RHEL und CentOS das EPEL-Repository, bevor Sie den Linux VDA installieren und `deploymcs.sh` erfolgreich ausführen können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter https://docs.fedoraproject.org/en-US/epel/.
>
> • Aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher, bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 installieren.

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

Ubuntu/Debian:

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

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

SUSE:

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

Schritt 3e: Repositorys zum Installieren des tdb-tools-Pakets aktivieren (nur für RHEL 7) RHEL 7-Server:

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

RHEL 7-Arbeitsstation:

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


Schritt 3f (SUSE): NTFS-3g manuell installieren Unter SUSE gibt es kein Repository, das ntfs-3g bereitstellt. Laden Sie den Quellcode herunter, führen Sie die Kompilation aus und installieren Sie ntfs-3g manuell:

1. Installieren Sie das GNU Compiler Collection (GCC) Compiler-System und das make-Paket:

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

2. Laden Sie das ntfs-3g-Paket herunter.
3. Dekomprimieren Sie das ntfs-3g-Paket:

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

4. Geben Sie den Pfad zum ntfs-3g-Paket ein:

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

5. Installieren Sie ntfs-3g:

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

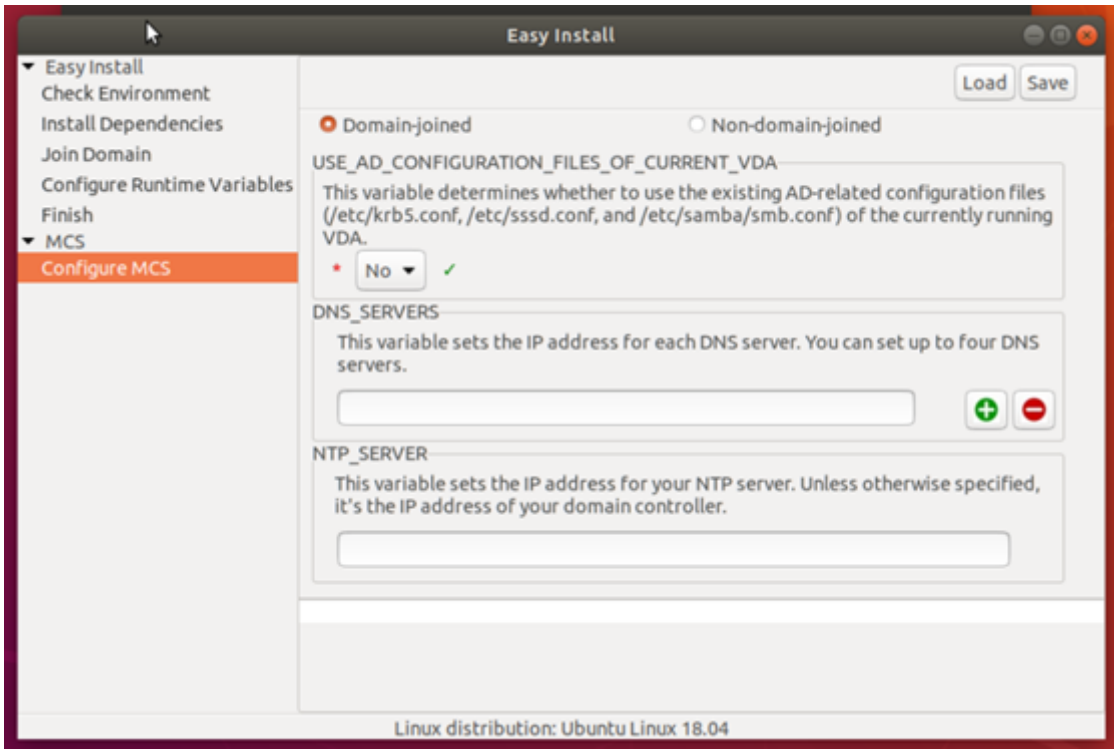
Schritt 3g: Zu verwendende Datenbank angeben Sie können nach der Installation des Linux VDA-Pakets zwischen SQLite und PostgreSQL wechseln. Führen Sie hierzu die folgenden Schritte aus:

> **Hinweis:**
>
> - Wir empfehlen, SQLite nur für den VDI-Modus und PostgreSQL für ein Bereitstellungsmodell für gehostete freigegebene Desktops zu verwenden.
> - Bei Easy Install und den Maschinenerstellungsdiensten (MCS) können Sie SQLite oder PostgreSQL zur Verwendung angeben, ohne die Systeme manuell installieren zu müssen. Sofern nicht anders durch **/etc/xdl/db.conf** angegeben, verwendet der Linux VDA standardmäßig PostgreSQL.
> - Sie können auch **/etc/xdl/db.conf** verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

1. Führen Sie `/opt/Citrix/VDA/sbin/ctxcleanup.sh` aus. Lassen Sie diesen Schritt aus, wenn es sich um eine Neuinstallation handelt.
2. Bearbeiten Sie `/etc/xdl/db.conf`, bevor Sie `deploymcs.sh` ausführen.

Schritt 3h: MCS-Variablen konfigurieren Es gibt zwei Möglichkeiten zum Konfigurieren von MCS-Variablen:

- Bearbeiten Sie die Datei `/etc/xdl/mcs/mcs.conf`.
- Verwenden Sie die GUI für Easy Install. Führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktopumgebung Ihres Linux VDA aus, um die GUI für Easy Install zu öffnen.



> **Tipp:**
>
> Klicken Sie auf **Speichern**, um Variableneinstellungen in einer lokalen Datei unter dem von Ihnen angegebenen Pfad zu speichern. Klicken Sie auf **Laden**, um Variableneinstellungen aus einer von Ihnen angegebenen Datei zu laden.

Die folgenden MCS-Variablen können Sie für Szenarios mit und ohne Domäneneinbindung konfigurieren:

- **Szenarien ohne Domäneneinbindung**

  Sie können die Standardwerte der Variablen verwenden oder die Variablen nach Bedarf anpassen (optional):

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


```
ADD_FIREWALL_RULES=Y | N
VDI_MODE=Y | N
START_SERVICE=Y | N
```

- **Szenarien mit Domäneneinbindung**
  - Use_AD_Configuration_Files_Of_Current_VDA: Legt fest, ob die AD-bezogenen Konfigurationsdateien (/etc/krb5.conf, /etc/sssd.conf und /etc/samba/smb.conf) des aktuell ausgeführten VDAs verwendet werden sollen. Bei Einstellung auf Y entsprechen die Konfigurationsdateien von durch MCS erstellten Maschinen den äquivalenten Dateien auf dem aktuell ausgeführten VDA. Die Variablen dns und AD_INTEGRATION müssen Sie dennoch konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsdateien von durch MCS erstellten Maschinen durch die Konfigurationsvorlagen auf dem Masterimage festgelegt werden. Um einen aktuell ausgeführten VDA als Vorlagen-VM zu verwenden, legen Sie den Wert auf Y fest. Andernfalls legen Sie ihn auf N fest.
  - dns: Festlegen der IP-Adresse für jeden DNS-Server. Sie können bis zu vier DNS-Server einrichten.
  - NTP_SERVER: Festlegen der IP-Adresse für Ihren NTP-Server. Sofern nicht anders angegeben, ist dies die IP-Adresse Ihres Domänencontrollers.
  - WORKGROUP: Legt den Arbeitsgruppennamen mit dem NetBIOS-Namen (Groß-/Kleinschreibung wird beachtet) fest, den Sie in AD konfiguriert haben. Andernfalls verwendet MCS den Teil des Domänennamens, der unmittelbar auf den Maschinenhostnamen folgt, als Arbeitsgruppennamen. Lautet das Maschinenkonto beispielsweise **user1.lvda.citrix.com**, verwendet MCS **lvda** als Arbeitsgruppennamen, wohingegen **Citrix** die richtige Wahl ist. Achten Sie darauf, den Arbeitsgruppennamen richtig festzulegen.
  - AD_INTEGRATION: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der Linux-Distributionen und Methoden zum Domänenbeitritt, die MSC unterstützt, finden Sie unter Unterstützte Distributionen in diesem Artikel.
  - CENTRIFY_DOWNLOAD_PATH: Legt den Pfad zum Herunterladen von Server Suite Free (zuvor "Centrify Express") fest. Der Wert wird nur wirksam, wenn Sie die Variable AD_INTEGRATION auf "Centrify"festlegen.
  - CENTRIFY_SAMBA_DOWNLOAD_PATH: Legt den Pfad zum Herunterladen des Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable AD_INTEGRATION auf "Centrify"festlegen.
  - PBIS_DOWNLOAD_PATH: Legt den Pfad zum Herunterladen des PBIS-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable AD_INTEGRATION auf "PBIS"festlegen.

- UPDATE_MACHINE_PW: Aktiviert oder deaktiviert die Automatisierung der Kennwortaktualisierung von Maschinenkonten. Weitere Informationen finden Sie unter Kennwortaktualisierung für Maschinenkonten automatisieren.
- Linux VDA-Konfigurationsvariablen:

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

Schritt 3i: Registrierungswerte für MCS schreiben oder aktualisieren Fügen Sie auf der Vorlagenmaschine der Datei /etc/xdl/mcs/mcs_local_setting.reg Befehlszeilen hinzu, um Registrierungswerte nach Bedarf zu schreiben oder zu aktualisieren. Diese Aktion verhindert den Verlust von Daten und Einstellungen bei jedem Neustart einer von MCS-Provisioningmaschine.

Jede Zeile in der Datei /etc/xdl/mcs/mcs_local_setting.reg ist ein Befehl zum Festlegen oder Aktualisieren eines Registrierungswerts.

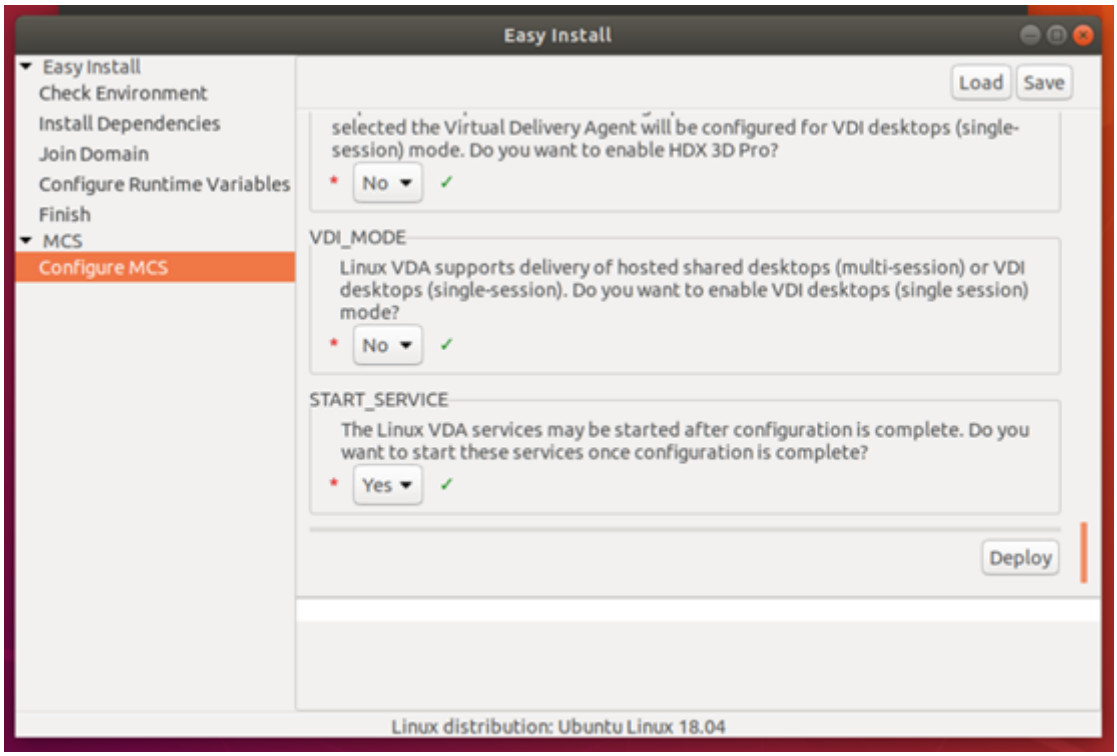
Beispielsweise können Sie der Datei /etc/xdl/mcs/mcs_local_setting.reg die folgenden Befehlszeilen hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

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

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

Schritt 3j: Masterimage erstellen

1. Nur SSSD + RHEL 8.x/9.x oder Rocky Linux 8.x/9.x: Führen Sie den Befehl `update-crypto-policies --set DEFAULT:AD-SUPPORT` aus und starten Sie dann die Vorlagen-VM neu.
2. Wenn Sie MCS-Variablen durch Bearbeiten von `/etc/xdl/mcs/mcs.conf` konfigurieren, führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus. Wenn Sie MCS-Variablen über die GUI konfigurieren, klicken Sie auf **Bereitstellen**.



   Nachdem Sie in der GUI auf **Bereitstellen** geklickt haben, werden die Variablen, die Sie in der Datei `/etc/xdl/mcs/mcs.conf` festgelegt haben, von den in der GUI festgelegten Variablen überschrieben.
3. (Wenn Sie einen aktuell ausgeführten VDA als Vorlagen-VM verwenden oder wenn es sich um ein Szenario ohne Domäneneinbindung handelt, lassen Sie diesen Schritt aus.) Aktualisieren Sie auf der Vorlagen-VM die Konfigurationsvorlagen, um die relevanten Dateien `/etc/krb5.conf`, `/etc/samba/smb.conf` und `/etc/sssd/sssd.conf` auf allen erstellten VMs anzupassen.

   Aktualisieren Sie für Winbind-Benutzer die Vorlagen `/etc/xdl/ad_join/winbind_krb5.conf.tmpl` und `/etc/xdl/ad_join/winbind_smb.conf.tmpl`.

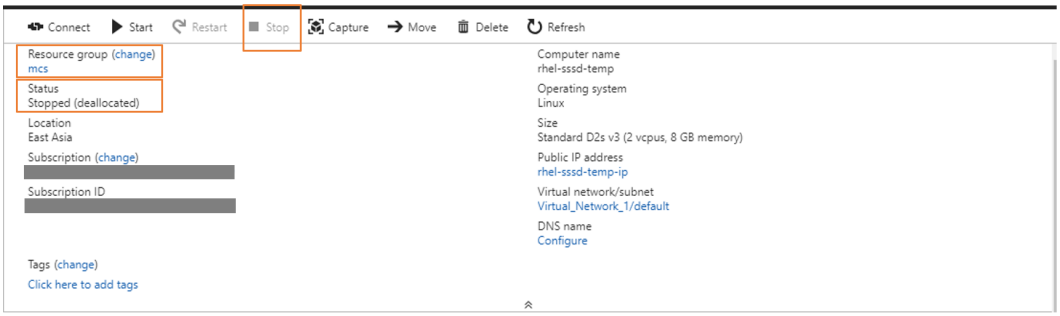
   Aktualisieren Sie für SSSD-Benutzer die Vorlagen `/etc/xdl/ad_join/sssd.conf.tmpl`, `/etc/xdl/ad_join/sssd_krb5.conf.tmpl` und `/etc/xdl/ad_join/sssd_smb.conf.tmpl`.

   Aktualisieren Sie für Centrify-Benutzer die Vorlagen `/etc/xdl/ad_join/centrify_krb5.conf.tmpl` und `/etc/xdl/ad_join/centrify_smb.conf.tmpl`.

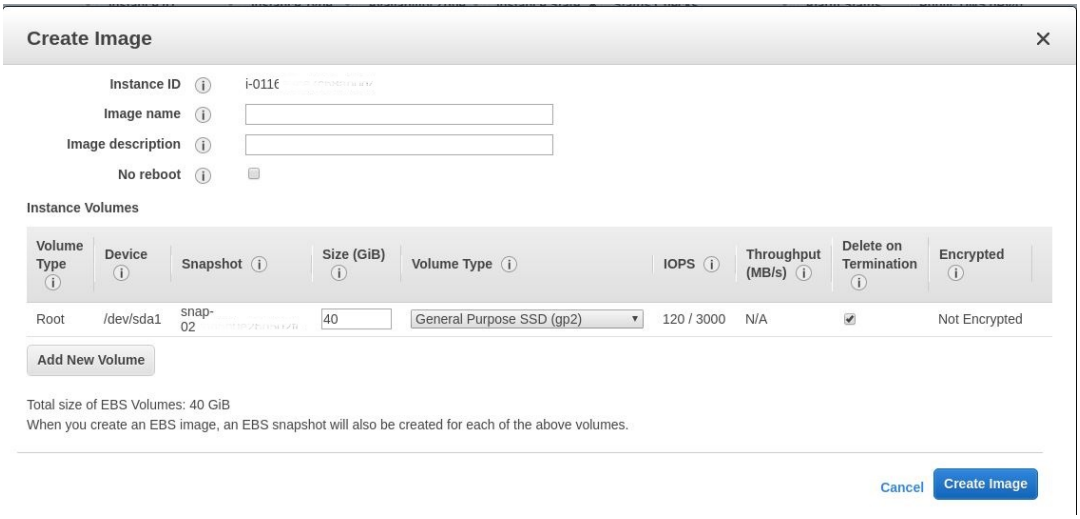
> **Hinweis:**
>
> Behalten Sie das vorhandene Format bei, das in den Vorlagendateien verwendet wird, und verwenden Sie Variablen wie $WORKGROUP, $REALM, $realm, ${new_hostname} und $AD_FQDN.

4. Erstellen und benennen Sie einen Snapshot Ihres Masterimages basierend auf der von Ihnen verwendeten öffentlichen Cloud.

   - **(Citrix Hypervisor, GCP und VMware vSphere)** Installieren Sie Anwendungen auf der Vorlagen-VM, und fahren Sie die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages.
   - **(Azure)**: Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM vom Azure-Portal aus herunter. Stellen Sie sicher, dass der Energiestatus der Vorlagen-VM als **gestoppt (Zuordnung aufgehoben)** angezeigt wird. Merken Sie sich den Namen der Ressourcengruppe. Sie benötigen diesen Namen später, um Ihr Masterimage in Azure zu finden.

   - **(AWS)** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM vom AWS EC2-Portal aus herunter. Stellen Sie sicher, dass der Instanzstatus der Vorlagen-VM als **gestoppt** angezeigt wird. Klicken Sie mit der rechten Maustaste auf die Vorlagen-VM und wählen Sie **Image > Image erstellen** aus. Geben Sie nach Bedarf Informationen ein und nehmen Sie die Einstellungen vor. Klicken Sie auf **Image erstellen**.



- **(Nutanix)** Fahren Sie unter Nutanix AHV die Vorlagen-VM herunter. Erstellen und benennen Sie einen Snapshot Ihres Masterimages.

  > **Hinweis:**
  >
  > Sie müssen den Namen von Acropolis-Snapshots zur Verwendung in Citrix Virtual Apps and Desktops `XD_` voranstellen. Verwenden Sie bei Bedarf die Acropolis-Konsole, um die Snapshots umzubenennen. Nach Umbenennen von Snapshots starten Sie den **Assistenten zum Erstellen von Katalogen** neu, damit eine aktualisierte Liste angezeigt wird.

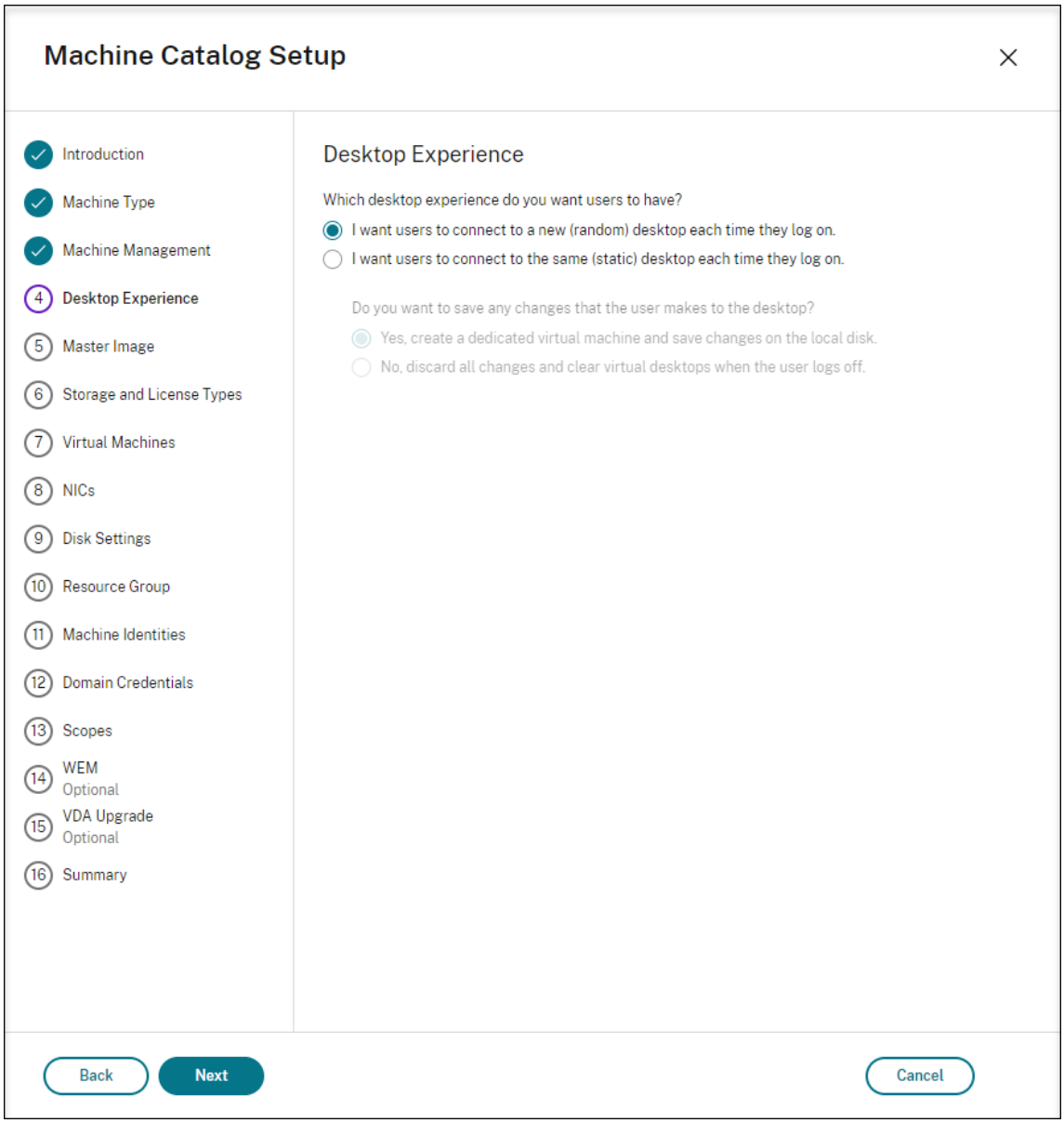
(Für GCP) Schritt 3k: Ethernetverbindung auf RHEL 8.x/9.x und Rocky Linux 8.x/9.x konfigurieren Nach der Installation des Linux VDA auf RHEL 8.x/9.x oder Rocky Linux 8.x/9.x, das auf GCP gehostet wird, wird die Ethernetverbindung möglicherweise unterbrochen und der Linux VDA ist nach einem VM-Neustart u. U. nicht erreichbar. Um das Problem zu umgehen, legen Sie ein Root-Kennwort fest, wenn Sie sich das erste Mal an der VM anmelden, und stellen sicher, dass Sie sich als Root-Benutzer an der VM anmelden können. Führen Sie dann nach dem Neustart der VM die folgenden Befehle in der Konsole aus:

```
nmcli dev connect eth0
service NetworkManager restart
<!--NeedCopy-->
```

Schritt 4: Maschinenkatalog erstellen

Erstellen Sie einen Maschinenkatalog in Citrix Studio oder Web Studio und geben Sie die Anzahl der VMs im Katalog an. Wählen Sie beim Erstellen des Maschinenkatalogs Ihr Masterimage und ziehen Sie Folgendes in Erwägung:

- Wählen Sie auf der für Nutanix eindeutigen Seite **Container** den Container aus, den Sie zuvor für die Vorlagen-VM angegeben haben.
- Wenn Sie einen Katalog mit Maschinen mit **Einzelsitzungs-OS** erstellen, wird die Seite **Desktoperfahrung** angezeigt, auf der Sie festlegen können, was bei jeder Benutzeranmeldung passiert.



Wählen Sie auf der Seite **Desktop Experience** eine der folgenden Optionen aus:

- Benutzer stellen bei jeder Anmeldung eine Verbindung mit einem neuen Desktop her
- Benutzer stellen bei jeder Anmeldung eine Verbindung mit dem gleichen Desktop her

Wenn Sie die erste Option wählen, werden Änderungen, die Benutzer am Desktop vornehmen, verworfen (nicht persistent).

Wenn Sie die zweite Option wählen und MCS für das Provisioning von Maschinen verwenden, können Sie festlegen, wie Änderungen der Benutzer am Desktop verarbeitet werden:

- Benutzeränderungen am Desktop auf dem lokalen Datenträger speichern (persistent)
- Änderungen verwerfen und virtuelle Desktops bei Abmeldung entfernen (nicht-persistent) Wählen Sie diese Option, wenn Sie den Benutzerpersonalisierungslayer verwenden.

- Wird ein Masterimage für einen MCS-Katalog mit persistenten Maschinen aktualisiert, verwenden alle dem Katalog neu hinzugefügten Maschinen das aktualisierte Image. Bereits vorhandene Maschinen verwenden weiterhin das ursprüngliche Masterimage.

Weitere Informationen finden Sie im Abschnitt zur Erstellung von Maschinenkatalogen in der Dokumentation zu Citrix Virtual Apps and Desktops und in der Dokumentation zu Citrix DaaS.

> **Hinweis:**
>
> Wenn die Erstellung des Maschinenkatalogs auf dem Delivery Controller in einer Nutanix-Umgebung lange dauert, fahren Sie in Nutanix Prism die Maschine mit dem Präfix **Preparation** manuell hoch. Dadurch wird der Erstellungsprozess fortgesetzt.

Schritt 5: Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Sie gibt die Benutzer an, die diese Maschinen verwenden können, und die für die Benutzer verfügbaren Anwendungen und Desktops.

Weitere Informationen finden Sie im Abschnitt zur Erstellung von Bereitstellungsgruppen in der Dokumentation zu Citrix Virtual Apps and Desktops und in der Dokumentation zu Citrix DaaS.

> **Hinweis:**
>
> Die virtuellen Maschinen, die Sie mit MCS erstellen, können möglicherweise nicht bei Citrix Cloud Connectors registriert werden und werden als **Nicht registriert** angezeigt. Das Problem tritt auf, wenn Sie die VMs in Azure hosten und mit Samba Winbind in die AD-Domäne aufnehmen. Sie umgehen das Problem wie folgt:
>
> 1. Öffnen Sie die ADSI Edit-Konsole, wählen Sie eine nicht registrierte VM aus und bearbeiten Sie das Attribut **msDS-SupportedEncryptionTypes** im zugehörigen Maschinenkonto.
> 2. Starten Sie die Dienste **ctxjproxy** und **ctxvda** auf der VM neu. Wenn sich der Status der VM in **Registriert** ändert, fahren Sie mit den Schritten 3 bis 5 fort.
> 3. Öffnen Sie die Datei **/var/xdl/mcs/ad_join.sh** auf der Vorlagen-VM.
> 4. Fügen Sie in der Datei **/var/xdl/mcs/ad_join.sh** nach den folgenden Zeilen die Zeile **net ads enctypes set $NEW_HOSTNAME$ <Dezimalwert des Verschlüsselungstypattributs,**

zum Beispiel 28\> -U $NEW_HOSTNAME$ -P password hinzu:

```
if [ "$AD_INTEGRATION" == "winbind" ]; then
                join_domain_samba
                restart_service winbind /usr/bin/systemctl
<!--NeedCopy-->
```

5. Erstellen Sie einen neuen Snapshot und erstellen Sie VMs mit der neuen Vorlage.

Upgrade des Linux VDAs mit MCS

Um MCS zum Aktualisieren des Linux VDA zu verwenden, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie .NET Runtime 6.0 installiert haben, bevor Sie Ihren Linux VDA auf die aktuelle Version aktualisieren.
2. Aktualisieren Sie Ihren Linux VDA auf der Vorlagenmaschine

> **Hinweis:**
>
> Mit dem Feature Linux VDA-Selbstupdate können Sie auch automatische Softwareupdates planen. Fügen Sie hierzu der Datei etc/xdl/mcs/mcs_local_setting.reg auf der Vorlagenmaschine Befehlszeilen hinzu.
> Beispiel:

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

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

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

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

RHEL 7 und CentOS 7:

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

RHEL 8.x und Rocky Linux 8.x:


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

RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

> **Hinweis:**
>
> Aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher, bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 aktualisieren.

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

SUSE:

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

Ubuntu 20.04:

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

Ubuntu 22.04:

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

3. Bearbeiten Sie `/etc/xdl/mcs/mcs.conf` und `/etc/xdl/mcs/mcs_local_setting.reg`.
4. Erstellen Sie einen neuen Snapshot.
5. Wählen Sie in Citrix Studio den neuen Snapshot aus, um Ihren Maschinenkatalog zu aktualisieren. Warten Sie auf jeden Maschineneustart. Starten Sie eine Maschine nicht manuell neu.

Kennwortaktualisierung für Maschinenkonten automatisieren

Kennwörter von Maschinenkonten laufen standardmäßig 30 Tage nach der Erstellung des Maschinenkatalogs ab. Gehen Sie folgendermaßen vor, um das Ablaufen von Kennwörtern zu verhindern und die Aktualisierung von Maschinenkennwörtern zu automatisieren:

1. Fügen Sie /etc/xdl/mcs/mcs.conf den folgenden Eintrag hinzu, bevor Sie /opt/Citrix/VDA/sbin/deploymcs.sh ausführen.

   ```
   UPDATE_MACHINE_PW="Y"
   ```


2. Öffnen Sie nach dem Ausführen von /opt/Citrix/VDA/sbin/deploymcs.sh /etc/cron.d/mcs_update_password_ um die Uhrzeit und Frequenz der Aktualisierung festzulegen. In der Standardeinstellung werden die Kennwörter von Maschinenkonten wöchentlich jeden Sonntag um 2:30 Uhr aktualisiert.

Nach jeder Kennwortaktualisierung wird der Ticketcache auf dem Delivery Controller ungültig und evtl. der folgende Fehler in /var/log/xdl/jproxy.log angezeigt:

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

Um den Fehler zu beseitigen, leeren Sie den Ticketcache regelmäßig. Sie können einen Task zur Cachebereinigung auf allen Delivery Controllern oder auf dem Domänencontroller planen.

Aktivieren von FAS auf von MCS erstellten VMs

Sie können FAS auf mit MCS erstellten VMs aktivieren, die auf den folgenden Distributionen ausgeführt werden:

	Winbind	SSSD	Centrify	PBIS
RHEL 9.2/9.0	Ja	Nein	Nein	Nein
RHEL 8.x	Ja	Nein	Nein	Ja
Rocky Linux 9.2/9.0	Ja	Nein	Nein	Nein
Rocky Linux 8.x	Ja	Nein	Nein	Nein
RHEL 7, CentOS 7	Ja	Ja	Nein	Ja
Ubuntu 22.04, Ubuntu 20.04	Ja	Nein	Nein	Nein
Debian 11.3	Ja	Nein	Nein	Nein
SUSE 15.4	Ja	Nein	Nein	Nein

Aktivieren Sie FAS, wenn Sie ein Masterimage auf der Vorlagen-VM vorbereiten

1. Importieren Sie das Stammzertifizierungsstellenzertifikat.

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

2. Führen Sie ctxfascfg.sh aus.

3. Legen Sie Variablen in `/etc/xdl/mcs/mcs.conf` fest.

   > **Hinweis:**
   >
   > Legen Sie alle erforderlichen Variablen in `/etc/xdl/mcs/mcs.conf` fest, da diese Variablen beim VM-Start aufgerufen werden.

   a) Legen Sie für `Use_AD_Configuration_Files_Of_Current_VDA` den Wert Y fest.
   b) Legen Sie für die Variable `FAS_LIST` Ihre FAS-Serveradresse oder mehrere FAS-Serveradressen fest. Trennen Sie mehrere Adressen durch Semikolons und schließen Sie die Adresse oder Adressen in einfache Anführungszeichen ein, z. B. `FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'`.
   c) Legen Sie die anderen Variablen wie erforderlich fest, z. B. `VDI_MODE`.

4. Führen Sie das Skript `/opt/Citrix/VDA/sbin/deploymcs.sh` aus.

Aktivieren von FAS auf einer von MCS erstellten VM

Wenn FAS auf dem Vorlagencomputer nicht wie zuvor beschrieben aktiviert ist, können Sie FAS auf jeder von MCS erstellten VM aktivieren.

Um FAS auf einer von MCS erstellten VM zu aktivieren, führen Sie die folgenden Schritte aus:

1. Legen Sie Variablen in /etc/xdl/mcs/mcs.conf fest.

   > **Hinweis:**
   >
   > Legen Sie alle erforderlichen Variablen in `/etc/xdl/mcs/mcs.conf` fest, da diese Variablen beim VM-Start aufgerufen werden.

   a) Legen Sie für `Use_AD_Configuration_Files_Of_Current_VDA` den Wert Y fest.
   b) Legen Sie für die Variable `FAS_LIST` Ihre FAS-Serveradresse fest.
   c) Legen Sie die anderen Variablen wie erforderlich fest, z. B. `VDI_MODE`.

2. Importieren Sie das Stammzertifizierungsstellenzertifikat.

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

3. Führen Sie das Skript `/opt/Citrix/VDA/sbin/ctxfascfg.sh` aus.

Linux-VDAs mit Citrix Provisioning erstellen

January 8, 2024

Mit Citrix Provisioning können Sie domänengebundene VDAs erstellen.

Dieser Artikel enthält Informationen zum Streaming von Linux-Zielgeräten. Mit diesem Feature können Sie virtuelle Linux-Desktops direkt in der Citrix Virtual Apps and Desktops-Umgebung bereitstellen.

Die folgenden Linux-Distributionen werden unterstützt:

- Ubuntu 22.04
- Ubuntu 20.04
- RHEL 9.2
- RHEL 9.0
- RHEL 8.8
- RHEL 8.6
- RHEL 7.9
- Rocky Linux 9.2
- Rocky Linux 9.0
- Rocky Linux 8.8
- Rocky Linux 8.6
- SUSE 15.4

> **Wichtig:**
>
> - Wir empfehlen die Verwendung des neuesten Installationspakets von Citrix Provisioning. Verwenden Sie das entsprechende Paket für Ihre Linux-Distribution. Citrix Provisioning Server 2109 oder höher ist erforderlich, um den Linux Streaming Agent 2109 und höher verwenden zu können.
> - Wenn Sie Citrix Provisioning zum Streamen von Linux-Zielgeräten verwenden, erstellen Sie eine separate Startpartition auf dem freigegebenen Datenträgerimage, damit die bereitgestellten Geräte wie erwartet gestartet werden können.
> - Vermeiden Sie es, Partitionen mit **btrfs** zu formatieren. GRUB2 hat Probleme beim Auffinden von **btrfs**-Partitionen. **GRUB** steht für **GRand Unified Bootloader**.

Weitere Informationen finden Sie unter Streaming von Linux-Zielgeräten in der Dokumentation zu Citrix Provisioning.

Linux VDAs in Citrix DaaS Standard für Azure erstellen

January 8, 2024

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

Unterstützte Linux-Distributionen

Die folgenden Linux-Distributionen unterstützen dieses Feature:

- RHEL 9.2
- RHEL 9.0
- RHEL 8.8
- RHEL 8.6
- Rocky Linux 9.2
- Rocky Linux 9.0
- Rocky Linux 8.8
- Rocky Linux 8.6
- SUSE 15.4
- Ubuntu 22.04
- Ubuntu 20.04

Schritt 1: Masterimage in Azure vorbereiten

> **Hinweis:**
>
> Mit dem Feature Linux VDA-Selbstupdate können Sie auch automatische Softwareupdates planen. Fügen Sie hierzu der Datei etc/xdl/mcs/mcs_local_setting.reg im Masterimage Befehlszeilen hinzu.
> Beispiel:

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

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

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

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

1. Erstellen Sie in Azure eine Linux-VM einer unterstützten Distribution.

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

   ```
   unlink /etc/resolv.conf

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

6. Installieren Sie das Linux VDA-Paket.
7. Geben Sie eine zu verwendende Datenbank an.

   Als experimentelles Feature können Sie SQLite zusätzlich zu PostgreSQL verwenden. Sie können nach der Installation des Linux VDA-Pakets auch zwischen SQLite und PostgreSQL wechseln. Führen Sie hierzu die folgenden Schritte aus:

   a) Führen Sie `/opt/Citrix/VDA/sbin/ctxcleanup.sh` aus. Lassen Sie diesen Schritt aus, wenn es sich um eine Neuinstallation handelt.

   b) Bearbeiten Sie `/etc/xdl/db.conf`, bevor Sie `deploymcs.sh` ausführen.

   > **Hinweis:**
   >
   > - Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.
   > - Bei Easy Install und den Maschinenerstellungsdiensten (MCS) können Sie zwischen SQLite und PostgreSQL wechseln, ohne die Systeme manuell installieren zu müssen. Sofern nicht anders durch `/etc/xdl/db.conf` angegeben, verwendet der Linux VDA standardmäßig PostgreSQL.
   > - Sie können auch `/etc/xdl/db.conf` verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

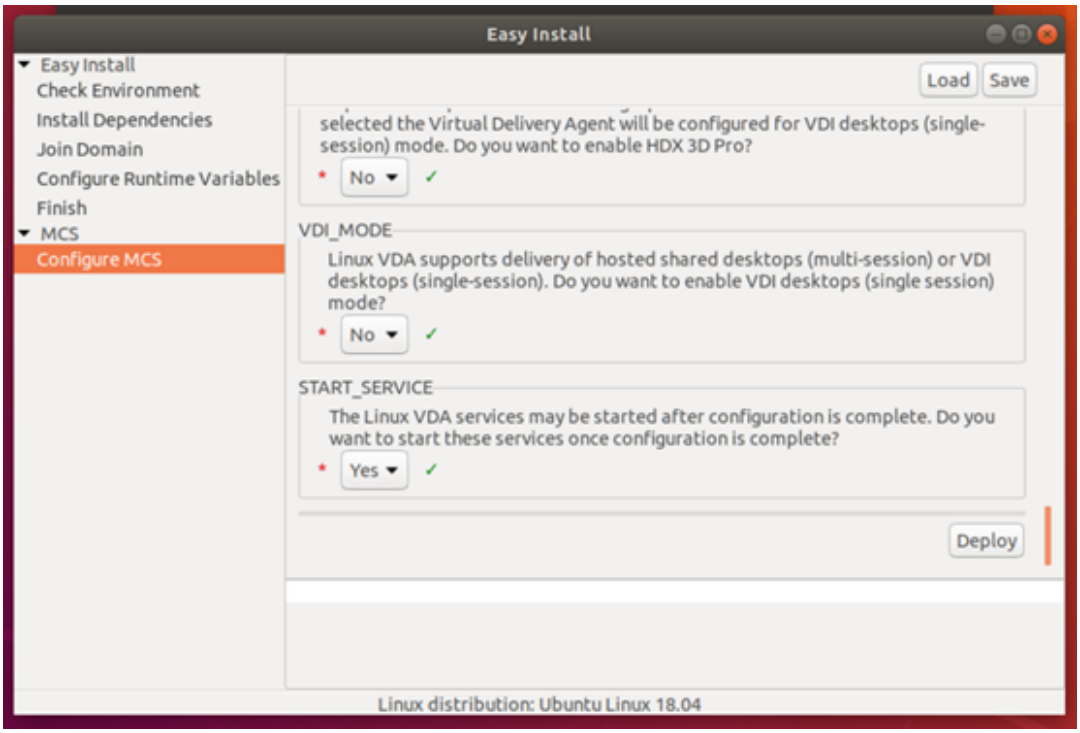
8. Ändern Sie die MCS-Variablen.

   Es gibt zwei Möglichkeiten zum Konfigurieren von MCS-Variablen:

   - Bearbeiten Sie die `/etc/xdl/mcs/mcs.conf`-Datei.
   - Verwenden Sie die GUI für Easy Install. Führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktopumgebung Ihres Linux VDA aus, um die GUI für Easy Install zu öffnen.

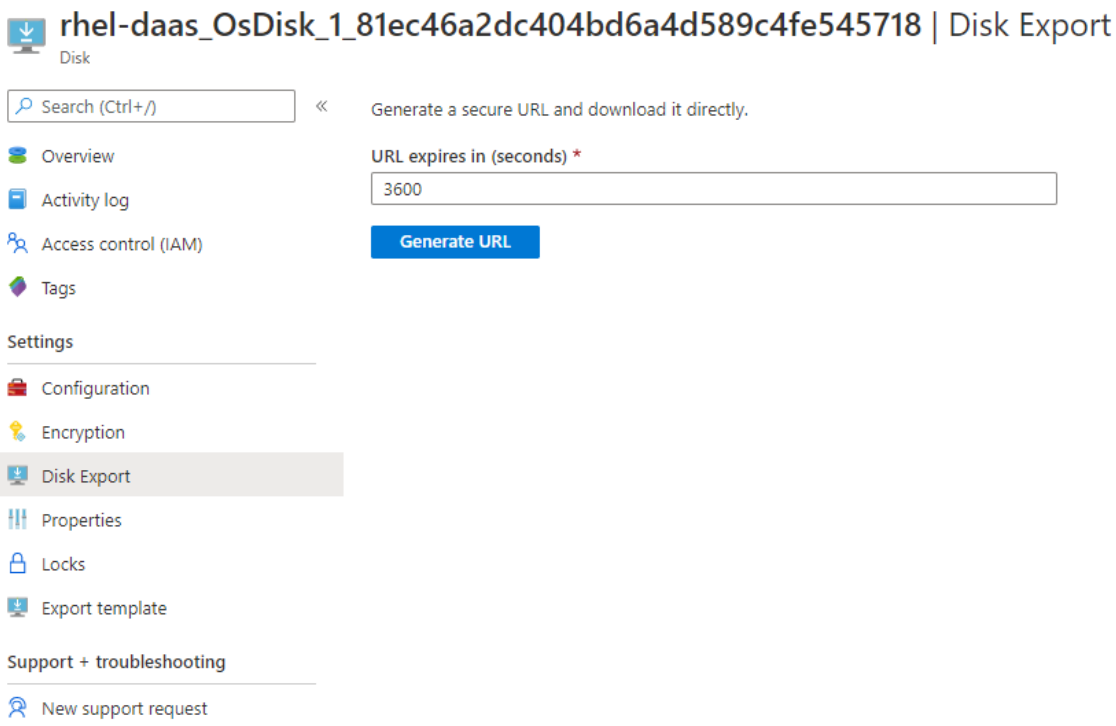
> **Hinweis:**
>
> Geben Sie die `dns`-Variable nicht an.
> Wenn Sie beim Erstellen eines Maschinenkatalogs den Typ **Statisch** oder **Zufällig** auswählen, legen Sie `VDI_MODE=Y` fest.

Wenn Sie MCS-Variablen durch Bearbeiten von `/etc/xdl/mcs/mcs.conf` konfigurieren, führen Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` aus. Wenn Sie MCS-Variablen über die GUI konfigurieren, klicken Sie auf **Bereitstellen**.



Nachdem Sie in der GUI auf **Bereitstellen** geklickt haben, werden die Variablen, die Sie in der Datei `/etc/xdl/mcs/mcs.conf` festgelegt haben, von den in der GUI festgelegten Variablen überschrieben.

9. Beenden Sie die VM in Azure (oder heben Sie die Zuordnung auf). Klicken Sie auf **Datenträgerexport**, um eine SAS-URL für die VHD-Datei zu generieren, die Sie als Masterimage zum Erstellen anderer VMs verwenden können.



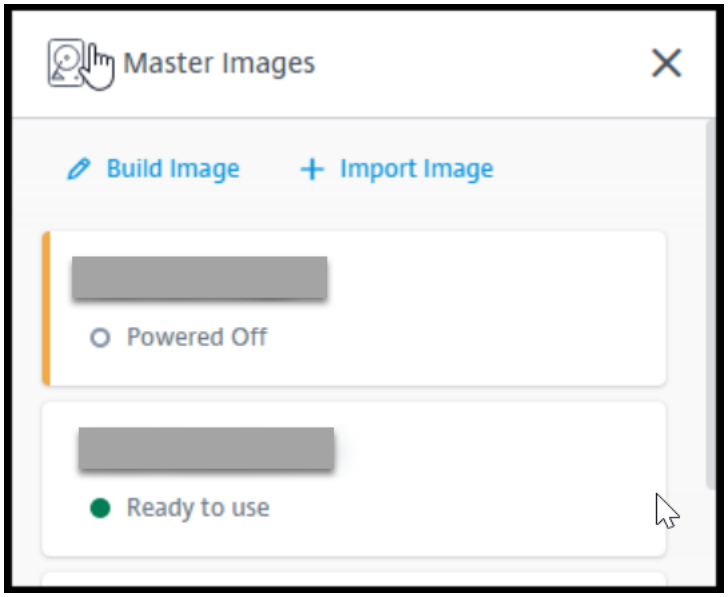
10. (Optional) Nehmen Sie Gruppenrichtlinieneinstellungen auf dem Masterimage vor. Sie können das Tool `ctxreg` verwenden, um Gruppenrichtlinieneinstellungen vorzunehmen. Mit dem folgenden Befehl wird beispielsweise die Richtlinie **Universellen PDF-Drucker automatisch erstellen** für den PDF-Druck aktiviert.

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

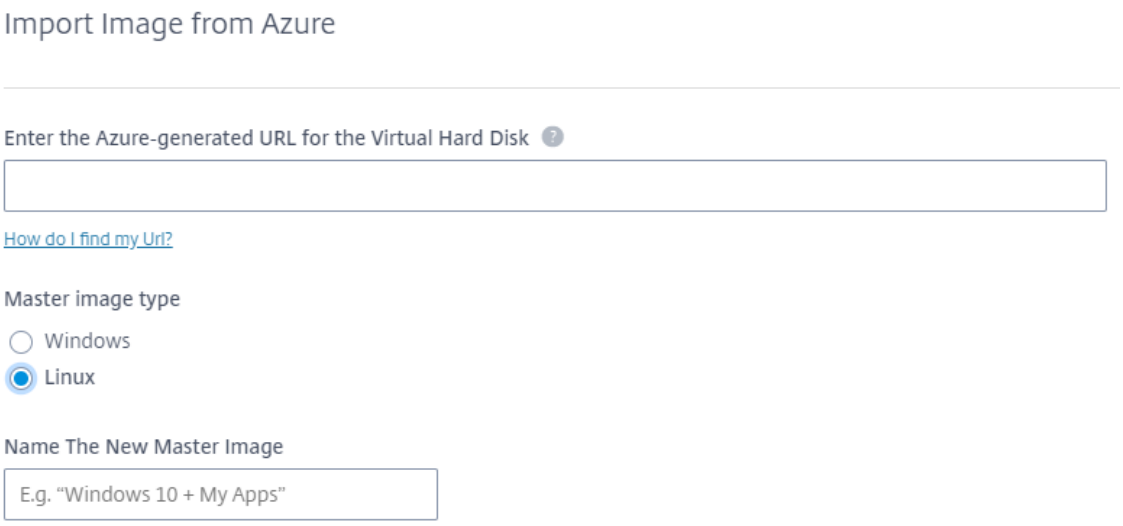
Schritt 2: Masterimage aus Azure importieren

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

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



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



4. Folgen Sie den Anweisungen im Assistenten, um den Import des Masterimages abzuschließen.

Schritt 3: Erstellen eines Maschinenkatalogs

Öffnen Sie das Dashboard Verwalten und klicken Sie auf **Katalog erstellen**. Wählen Sie beim Erstellen des Maschinenkatalogs das Masterimage aus, das Sie zuvor erstellt haben.

> **Hinweis:**
>
> Sie können nicht über SSH oder RDP auf die VM zugreifen, die als Masterimage verwendet wird. Um auf die VM zuzugreifen, verwenden Sie die serielle Konsole im Azure-Portal.

Linux VDA manuell installieren

January 8, 2024

Sie können den Linux VDA auf den folgenden Linux-Distributionen manuell installieren:

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

Linux VDA manuell auf Amazon Linux 2, CentOS, RHEL und Rocky Linux installieren

May 30, 2024

> **Wichtig:**
>
> Für Neuinstallationen empfehlen wir die Verwendung von Easy Install für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

Schritt 1: Vorbereiten der Konfigurationsinformationen und der Linux-Maschine

Schritt 1a: Überprüfen der Netzwerkkonfiguration

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

Schritt 1b: Festlegen des Hostnamens

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

```
hostname
```

Schritt 1c: Zuweisen einer Loopbackadresse für den Hostnamen

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

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

Beispiel:

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

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

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

Schritt 1d: Überprüfen des Hostnamens

Stellen Sie sicher, dass der Hostname richtig festgelegt ist:

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

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

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:


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

Dieser Befehl gibt den FQDN der Maschine zurück.

Schritt 1e: Überprüfen von Namensauflösung und Diensterreichbarkeit

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

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

Schritt 1f: Konfigurieren der Uhrsynchronisierung

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

In RHEL-Standardumgebungen wird der Chrony-Daemon (`chronyd`) für die Uhrsynchronisierung verwendet.

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

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

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

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

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

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

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

Schritt 1g: Installieren von PulseAudio (nur RHEL 9.2/9.0 und Rocky Linux 9.2/9.0)

Führen Sie den folgenden Befehl aus, um **pulseaudio** zu installieren:

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

Öffnen Sie `/etc/pulse/client.conf` und fügen Sie den folgenden Eintrag hinzu:

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

Schritt 1h: Installieren von OpenJDK 11

Der Linux VDA erfordert das Vorhandensein von OpenJDK 11.

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

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

Bestätigen Sie die richtige Version:

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

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

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

Schritt 1i: Installieren und Angeben einer zu verwendenden Datenbank

Sie können die Verwendung von SQLite oder PostgreSQL angeben, indem Sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Bei manuellen Installationen müssen Sie SQLite

und PostgreSQL manuell installieren, um diese angeben zu können.

In diesem Abschnitt wird beschrieben, wie Sie die PostgreSQL- und SQLite-Datenbanken installieren und wie Sie eine zu verwendende Datenbank angeben.

> **Hinweis:**
>
> Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.

PostgreSQL installieren Der Linux VDA erfordert PostgreSQL:

- PostgreSQL 9 für Amazon Linux 2, RHEL 7 und CentOS 7
- PostgreSQL 10 für RHEL 8.x und Rocky Linux 8.x
- PostgreSQL 13 für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0

Führen Sie zum Installieren von PostgreSQL die folgenden Befehle aus:

```
sudo yum -y install postgresql-server

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

Führen Sie für RHEL 8.x und RHEL 9.2/9.0 den folgenden Befehl aus, um `libpq` für PostgreSQL zu installieren:

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

Führen Sie den folgenden Befehl aus, um die Datenbank zu initialisieren. Mit der Aktion werden unter **/var/lib/pgsql/data** Datenbankdateien erstellt.

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

Führen Sie die folgenden Befehle aus, um PostgreSQL beim Start der Maschine bzw. sofort zu starten:

```
sudo systemctl enable postgresql

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

Überprüfen Sie die Version von PostgreSQL mit folgendem Befehl:

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

(Nur RHEL 7 und Amazon Linux 2) Stellen Sie mit dem **psql**-Befehlszeilenprogramm sicher, dass das Datenverzeichnis festgelegt ist:


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

SQLite installieren Führen Sie den folgenden Befehl aus, um SQLite zu installieren:

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

Datenbank eingeben Nachdem Sie SQLite, PostgreSQL oder beides installiert haben, können Sie eine zu verwendende Datenbank angeben, indem Sie sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Führen Sie hierzu die folgenden Schritte aus:

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Lassen Sie diesen Schritt aus, wenn es sich um eine Neuinstallation handelt.
2. Bearbeiten Sie **/etc/xdl/db.conf**, um eine zu verwendende Datenbank anzugeben.
3. Führen Sie **ctxsetup.sh** aus.

> **Hinweis:**
>
> Sie können auch **/etc/xdl/db.conf** verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

Schritt 2: Vorbereiten des Hypervisors

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

Festlegen der Zeitsynchronisierung auf Citrix Hypervisor

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

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


```
su -

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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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

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

```
xen.independent_wallclock = 1
```

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

```
su -

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

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

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

Auf dem verwaltenden Betriebssystem:

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

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

Festlegen der Zeitsynchronisierung auf ESX und ESXi

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

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

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

Schritt 3: Linux-VM zur Windows-Domäne hinzufügen

Mit den folgenden Methoden können Linux-Maschinen zur Active Directory-Domäne (AD) hinzugefügt werden:

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

Folgen Sie den Anweisungen für die von Ihnen gewählte Methode.

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

Samba Winbind

Führen Sie für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 den folgenden Befehl aus, um zu verhindern, dass **pam_winbind** den Besitzer des Stammverzeichnisses ändert:

```
usermod -d /nonexistent nobody
<!--NeedCopy-->
```

Installieren oder aktualisieren Sie die erforderlichen Pakete:

RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x:

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

Amazon Linux 2, CentOS 7 und RHEL 7:

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

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

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

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

1. Führen Sie den folgenden Befehl aus.

   RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x:

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

   Amazon Linux 2, CentOS 7 und RHEL 7:

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

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

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

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

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

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

```
kerberos method = secrets and keytab
winbind refresh tickets = true
winbind offline logon = no
```

3. (Nur RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x) 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 Systemdatei für die Schlüsseltabelle "/etc/krb5.keytab", um sich beim Delivery Controller zu authentifizieren und zu registrieren. Die vorherige Einstellung "kerberos method"zwingt Winbind zum Erstellen der Systemdatei für die Schlüsseltabelle, wenn die Maschine der Domäne beitritt.

Windows-Domäne beitreten Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto verfügen, das zum Hinzufügen von Computern zur Domäne berechtigt ist.

Führen Sie den folgenden Befehl aus, um der Windows-Domäne eine Linux-VM hinzuzufügen:


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

> **Tipp:**
>
> Linux-VMs, die unter Amazon Linux 2, RHEL 7.9 und CentOS 7.9 ausgeführt werden, können auch mit folgendem Befehl zur Windows-Domäne hinzugefügt werden:
>
> ```
> sudo net ads join REALM -U user
> <!--NeedCopy-->
> ```

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

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

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

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

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

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

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

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

Führen Sie für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 die folgenden Befehle aus, um das SELinux-Problem mit Winbind zu lösen:

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

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


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

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

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

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

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

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

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

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

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

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

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

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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


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

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

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

Um sich zu vergewissern, dass das Winbind-PAM-Modul fehlerfrei konfiguriert ist, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

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

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

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

Beenden Sie die Sitzung.

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Quest Authentication Services

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

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

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

3. Aktivieren Sie das Kontrollkästchen **Unix-enabled**.
4. Legen Sie **Primary GID Number** auf die Gruppen-ID einer vorhandenen Domänenbenutzergruppe fest.

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

Quest auf Linux VDA konfigurieren

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

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

```
SELINUX=permissive
```

Diese Änderung erfordert einen Neustart der Maschine:

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

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

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

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

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
   auth false
<!--NeedCopy-->
```

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

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

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

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

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

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

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

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

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

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

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

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

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

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


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

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

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

Beenden Sie die Sitzung.

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Centrify DirectControl

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

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

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

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

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

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

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:


```
adinfo --sysinfo all
adinfo  – diag
<!--NeedCopy-->
```

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

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

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

SSSD

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

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

1. Domänenbeitritt und Erstellen einer Hostschlüsseltabelle
2. SSSD einrichten
3. Aktivieren von SSSD
4. Überprüfen der Kerberos-Konfiguration
5. Benutzerauthentifizierung überprüfen

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

In diesem Abschnitt wird die **Samba**-Methode für Amazon Linux 2 und RHEL 7 und die `adcli`-Methode für RHEL 8.x/9.x und Rocky Linux 8.x./9.x beschrieben. Informationen über **realmd** finden Sie in der Dokumentation zu RHEL oder CentOS. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

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

  Installieren oder aktualisieren Sie die erforderlichen Pakete:

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

  Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

  - /etc/krb5.conf

- /etc/samba/smb.conf:

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

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

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

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

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

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

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

```
kerberos method = secrets and keytab
winbind offline logon = no
```

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

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

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

- **Adcli (RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x):**

  Installieren oder aktualisieren Sie die erforderlichen Pakete:

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

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

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


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

Im Abschnitt [realms]:

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

Im Abschnitt [domain_realm]:

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

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

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

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

SSSD einrichten Die Einrichtung von SSSD umfasst die folgenden Schritte:

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

Muster einer **sssd.conf**-Konfiguration für RHEL 7 (zusätzliche Optionen können bei Bedarf hinzugefügt werden):


```
[sssd]
config_file_version = 2
domains = ad.example.com
services = nss, pam

[domain/ad.example.com]
# Uncomment if you need offline logins
# cache_credentials = true

id_provider = ad
auth_provider = ad
access_provider = ad
ldap_id_mapping = true
ldap_schema = ad

# Should be specified as the lower-case version of the long version of the Active Directory domain.
ad_domain = ad.example.com

# Kerberos settings
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U

# Uncomment if service discovery is not working
# ad_server = server.ad.example.com

# Comment out if the users have the shell and home dir set on the AD side
default_shell = /bin/bash
fallback_homedir = /home/%d/%u

# Uncomment and adjust if the default principal SHORTNAME$@REALM is not available
# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

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

(Nur RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x)
Öffnen Sie **/etc/sssd/sssd.conf** und fügen Sie folgende Einträge im Abschnitt [domain/ad.example.com] hinzu:

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

Legen Sie Dateieigentümer und Berechtigungen für sssd.conf fest:

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

Aktivieren von SSSD RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x:

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

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

Amazon Linux 2, CentOS 7 und RHEL 7:

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

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

sudo service sssd start

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

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

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

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

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

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

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

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

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


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

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

Unterstützte Anmeldeformate:

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

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

```
sudo ssh localhost  – l DOMAIN\username

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

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

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

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

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

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

PBIS

Download des erforderlichen PBIS-Pakets

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

Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei

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


Ausführen des PBIS-Installationsskripts

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

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

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

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

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

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

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

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

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

```
ssh localhost -l domain\user

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

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

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

Beenden Sie die Sitzung.


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

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

Schritt 4: .NET Runtime 6.0 installieren

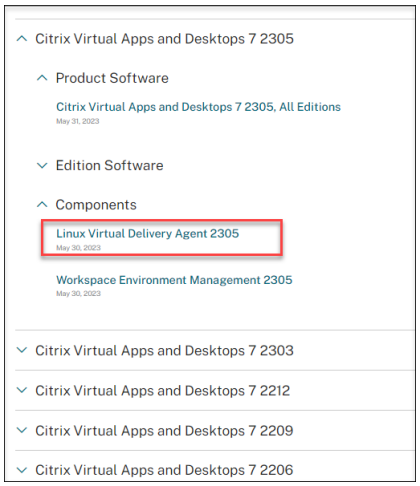
Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

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

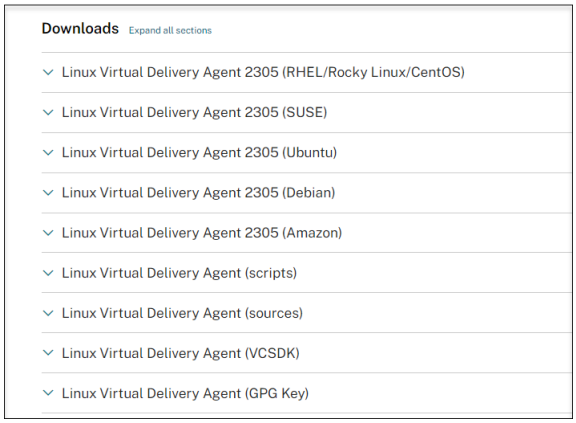
Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

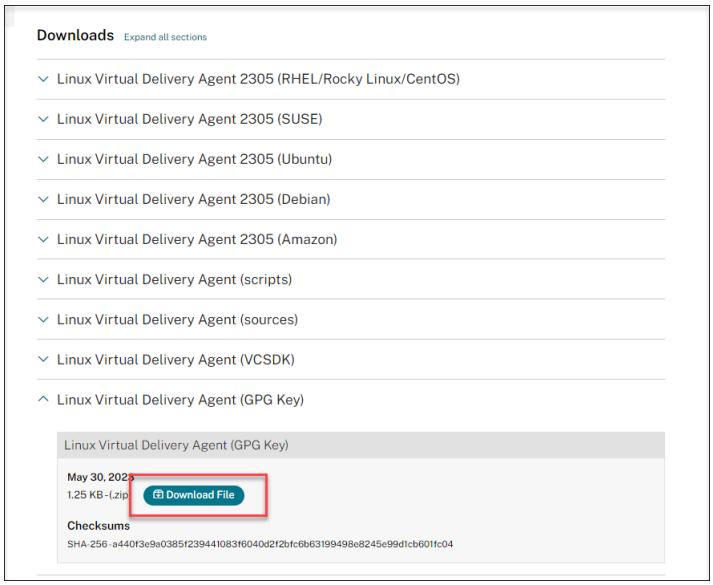
1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
2. Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. Erweitern Sie **Komponenten**, um den Linux VDA zu finden. Beispiel:



4. Klicken Sie auf den Linux VDA-Link, um auf die Linux VDA-Downloads zuzugreifen.



5. Laden Sie das Linux VDA-Paket herunter, das Ihrer Linux-Distribution entspricht.
6. Laden Sie den öffentlichen GPG-Schlüssel herunter, mit dem Sie die Integrität des Linux VDA-Pakets überprüfen können. Beispiel:



Um die Integrität des Linux VDA-Pakets zu überprüfen, führen Sie die folgenden Befehle aus, um den öffentlichen Schlüssel in die RPM-Datenbank zu importieren und die Überprüfung durchzuführen:

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

Schritt 6: Installieren des Linux VDA

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

Schritt 6a: Neuinstallation durchführen

1. (Optional) Deinstallieren Sie die alte Version

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

   a) Halten Sie die Linux VDA-Dienste an:

   ```
   sudo /sbin/service ctxvda stop

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

   > **Hinweis:**
   >
   > Führen Sie erst den Befehl **systemctl stop ctxmonitord** aus, um den Monitor Service Daemon zu stoppen, bevor Sie die Dienste **ctxvda** und **ctxhdx** stoppen. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

   b) Deinstallieren Sie das Paket:

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

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

2. Laden Sie das Linux VDA -Paket herunter

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

3. Installieren des Linux VDA

   > **Hinweis:**
   >
   > - Installieren Sie für CentOS, RHEL und Rocky Linux das EPEL-Repository, bevor Sie den Linux VDA erfolgreich installieren können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter https://docs.fedoraproject.org/en-US/epel/.
   > - Aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher, bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 installieren.

   - Installieren Sie die Linux VDA-Software mit Yum:

     Amazon Linux 2:


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

RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

```
sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
<!--NeedCopy-->
```

RHEL 8.x und Rocky Linux 8.x:

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

Für CentOS 7 und RHEL 7:

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

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

  Amazon Linux 2:

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

  RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

  ```
  sudo rpm -i XenDesktopVDA-<version>.el9_x.x86_64.rpm
  <!--NeedCopy-->
  ```

  RHEL 8.x und Rocky Linux 8.x:

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

  Für CentOS 7 und RHEL 7:

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

  RPM-Abhängigkeitsliste für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

  ```
  tzdata-java >= 2022

  java-11-openjdk >= 11

   icoutils >= 0.32

   firewalld >= 0.6.3

   policycoreutils-python >= 2.8.9
  ```



```
10
11    policycoreutils-python-utils >= 2.8
12
13    python3-policycoreutils >= 2.8
14
15    dbus >= 1.12.8
16
17    dbus-common >= 1.12.8
18
19    dbus-daemon >= 1.12.8
20
21    dbus-tools >= 1.12.8
22
23    dbus-x11 >= 1.12.8
24
25    xorg-x11-server-utils >= 7.7
26
27    xorg-x11-xinit >= 1.3.4
28
29    libXpm >= 3.5.12
30
31    libXrandr >= 1.5.1
32
33    libXtst >= 1.2.3
34
35    pam >= 1.3.1
36
37    util-linux >= 2.32.1
38
39    util-linux-user >= 2.32.1
40
41    xorg-x11-utils >= 7.5
42
43    bash >= 4.3
44
45    findutils >= 4.6
46
47    gawk >= 4.2
48
49    sed >= 4.5
50
51    cups >= 1.6.0
52
53    foomatic-filters >= 4.0.9
54
55    cups-filters >= 1.20.0
56
57    ghostscript >= 9.25
58
59    libxml2 >= 2.9
60
61    libmspack >= 0.7
62
```



```
 krb5-workstation >= 1.13

 ibus >= 1.5

 nss-tools >= 3.44.0

 gperftools-libs >= 2.4

 cyrus-sasl-gssapi >= 2.1

 python3 >= 3.6~

 qt5-qtbase >= 5.5~

 qt5-qtbase-gui >= 5.5~

 qrencode-libs >= 3.4.4

 imlib2 >= 1.4.9

<!--NeedCopy-->
```

RPM-Abhängigkeitsliste für RHEL 8.x und Rocky Linux 8.x:

```
java-11-openjdk >= 11

icoutils >= 0.32

firewalld >= 0.6.3

policycoreutils-python >= 2.8.9

policycoreutils-python-utils >= 2.8

python3-policycoreutils >= 2.8

dbus >= 1.12.8

dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1
```



```
30
31  libXtst >= 1.2.3
32
33  pam >= 1.3.1
34
35  util-linux >= 2.32.1
36
37  util-linux-user >= 2.32.1
38
39  xorg-x11-utils >= 7.5
40
41  bash >= 4.3
42
43  findutils >= 4.6
44
45  gawk >= 4.2
46
47  sed >= 4.5
48
49  cups >= 1.6.0
50
51  foomatic-filters >= 4.0.9
52
53  cups-filters >= 1.20.0
54
55  ghostscript >= 9.25
56
57  libxml2 >= 2.9
58
59  libmspack >= 0.7
60
61  krb5-workstation >= 1.13
62
63  ibus >= 1.5
64
65  nss-tools >= 3.44.0
66
67  gperftools-libs >= 2.4
68
69  cyrus-sasl-gssapi >= 2.1
70
71  python3 >= 3.6~
72
73  qt5-qtbase >= 5.5~
74
75  qt5-qtbase-gui >= 5.5~
76
77  qrencode-libs >= 3.4.4
78
79  imlib2 >= 1.4.9
80  <!--NeedCopy-->
```

RPM-Abhängigkeitsliste für CentOS 7 und RHEL 7:


```
java-11-openjdk >= 11

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

xorg-x11-server-Xorg >= 1.20.4

libXpm >= 3.5.10

libXrandr >= 1.4.1

libXtst >= 1.2.2

pam >= 1.1.8

util-linux >= 2.23.2

bash >= 4.2

findutils >= 4.5

gawk >= 4.0

sed >= 4.2

cups >= 1.6.0

foomatic-filters >= 4.0.9

libxml2 >= 2.9

libmspack >= 0.5

ibus >= 1.5

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

gperftools-libs >= 2.4

nss-tools >= 3.44.0
```



```
54
55  qt5-qtbase >= 5.5~
56
57  qt5-qtbase >= 5.5~
58
59  imlib2 >= 1.4.5
60  <!--NeedCopy-->
```

RPM-Abhängigkeitsliste für Amazon Linux 2:

```
1   java-11-openjdk >= 11
2
3   ImageMagick >= 6.7.8.9
4
5   firewalld >= 0.3.9
6
7   policycoreutils-python >= 2.0.83
8
9   dbus >= 1.6.12
10
11  dbus-x11 >= 1.6.12
12
13  xorg-x11-server-utils >= 7.7
14
15  xorg-x11-xinit >= 1.3.2
16
17  xorg-x11-server-Xorg >= 1.20.4
18
19  libXpm >= 3.5.10
20
21  libXrandr >= 1.4.1
22
23  libXtst >= 1.2.2
24
25  pam >= 1.1.8
26
27  util-linux >= 2.23.2
28
29  bash >= 4.2
30
31  findutils >= 4.5
32
33  gawk >= 4.0
34
35  sed >= 4.2
36
37  cups >= 1.6.0
38
39  foomatic-filters >= 4.0.9
40
41  libxml2 >= 2.9
42
43  libmspack >= 0.5
```



```
44
45  ibus >= 1.5
46
47  cyrus-sasl-gssapi >= 2.1
48
49  gperftools-libs >= 2.4
50
51  nss-tools >= 3.44.0
52
53  qt5-qtbase >= 5.5~
54
55  qrencode-libs >= 3.4.1
56
57  imlib2 >= 1.4.5
58  <!--NeedCopy-->
```

> **Hinweis:**
>
> Eine Übersicht der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden, finden Sie in der Tabelle Systemanforderungen.
>
> Führen Sie nach der Installation des Linux VDA unter RHEL 7.x den Befehl `sudo yum install -y python-websockify x11vnc` aus. Damit werden `python-websockify` und `x11vnc` manuell für die Verwendung der Sitzungsspiegelung installiert. Weitere Informationen finden Sie unter Sitzungen spiegeln.

Schritt 6b: Bestehende Installation aktualisieren (optional)

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

> **Hinweis:**
>
> - Durch das Upgrade einer Installation werden die Konfigurationsdateien unter /etc/xdl. überschrieben. Sichern Sie die Dateien vor jedem Upgrade.
> - Aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher, bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 aktualisieren.

- So aktualisieren Sie Ihre Software mit `Yum`:

  Amazon Linux 2:

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

  RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

  ```
  1  sudo yum install -y XenDesktopVDA-<version>.el9_x.x86_64.rpm
  ```



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

RHEL 8.x und Rocky Linux 8.x:

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

Für CentOS 7 und RHEL 7:

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

- So aktualisieren Sie Ihre Software mit RPM-Paketmanager:

  Amazon Linux 2:

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

  RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

  ```
  sudo rpm -U XenDesktopVDA-<version>.el9_x.x86_64.rpm
  <!--NeedCopy-->
  ```

  RHEL 8.x und Rocky Linux 8.x:

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

  Für CentOS 7 und RHEL 7:

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

> **Hinweis:**
>
> Bei Verwendung von RHEL 7 sind nach dem Ausführen der vorherigen Upgrade-Befehle folgende Schritte erforderlich:
>
> 1. Führen Sie `/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_SZ"-v "DotNetRuntimePath" -d "/opt/rh/rh-dotnet31/root/usr/bin/"--force` aus, um den richtigen .NET-Laufzeitpfad festzulegen.
> 2. Starten Sie den Dienst `ctxvda` neu.
>
> **Wichtig:**
>
> Starten Sie die Linux VDA-Maschine nach der Softwareaktualisierung neu.

Schritt 7: Installieren von NVIDIA GRID-Treibern

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

> **Hinweis:**
>
> Um HDX 3D Pro für Amazon Linux 2 zu verwenden, empfehlen wir die Installation des NVIDIA-Treibers 470. Weitere Informationen finden Sie unter Systemanforderungen.

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

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

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

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM in XenCenter eine GPU zu.
3. Starten Sie die VM.
4. Bereiten Sie die VM für den NVIDIA GRID-Treiber vor:

```
yum install gcc

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

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

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

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


```
nvidia-smi
```

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

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

Legen Sie die richtige Konfiguration für die Karte fest:

`etc/X11/ctx-nvidia.sh`

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

Schritt 8: Konfigurieren des Linux VDA

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

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

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

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


Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

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

Automatische Konfiguration

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

Unterstützte Umgebungsvariablen umfassen u. a.:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Standardeinstellung ist N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'**–Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist standardmäßig Port 80.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –Die Linux VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für Linux Virtual Desktop öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis** –Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt.
- **CTX_XDL_HDX_3D_PRO=Y | N** –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung grafikintensiver Anwendungen. Bei aktiviertem HDX 3D Pro wird der VDA für VDI-Desktopmodus (Einzelsitzungen) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y | N** –Legt die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell fest.

Legen Sie dies bei Umgebungen mit HDX 3D Pro auf "Y"fest. Standardmäßig ist diese Variable auf N festgelegt.

- **CTX_XDL_SITE_NAME=dns-name** –Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268 oder ad1.mycompany.com:636 ad2.mycompany.com:3269 ad3.mycompany.com:3269, wenn Sie LDAPS verwenden. Für schnellere LDAP-Abfragen in einer Active Directory-Gesamtstruktur aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben als LDAP-Portnummer 3268 bzw., sofern Sie LDAPS verwenden, 3269 an. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE=search-base-set** –Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. ctx_xdl_fas_fas_list='FAS_Server_1_URL:Port_Number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

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

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

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

   - **Für GNOME Classic-Desktop**

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

   - **Für GNOME-Desktop**

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

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

Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebung anpassen. Um dieses Feature zu aktivieren, müssen Sie umschaltbare Desktopumgebungen vorher auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen nach Sitzungsbenutzern.

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

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

```
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=winbind | quest |centrify | sssd | pbis

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

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

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

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

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:

```
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=winbind | quest |centrify | sssd | pbis \

CTX_XDL_HDX_3D_PRO=Y|N \
```



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

Entfernen von Konfigurationsänderungen

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

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

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

Entfernen von Konfigurationsänderungen:

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

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

Konfigurationsprotokolle

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

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

Schritt 9: Ausführen von XDPing

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

Schritt 10: Ausführen des Linux VDA

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

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start

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

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

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

> **Hinweis:**
>
> Führen Sie erst den Befehl **systemctl stop ctxmonitord** aus, um den Monitor Service Daemon zu stoppen, bevor Sie die Dienste **ctxvda** und **ctxhdx** stoppen. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

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


Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status

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

Schritt 11: Maschinenkataloge erstellen

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

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

- Auswahl des Betriebssystems:
  - Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

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

Schritt 12: Bereitstellungsgruppen erstellen

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

diesen Prozessen finden Sie unter Erstellen von Bereitstellungsgruppen.

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

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

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

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2308.

Linux VDA manuell auf SUSE installieren

May 30, 2024

> **Wichtig:**
>
> Für Neuinstallationen empfehlen wir die Verwendung von Easy Install für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

Schritt 1: Vorbereiten der Konfigurationsinformationen und der Linux-Maschine

Schritt 1a: Starten des YaST-Tools

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

Starten des textbasierten YaST-Tools:

```
su -

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

Starten des UI-basierten YaST-Tools:


```
su -

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

Schritt 1b: Konfigurieren des Netzwerks

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

Konfigurieren von Hostnamen und Domain Name System (DNS)

1. Starten Sie das UI-basierte YaST-Tool.
2. Wählen Sie **System** und dann **Network Settings** aus.
3. Öffnen Sie die Registerkarte **Hostname/DNS**.
4. Wählen Sie die Option **no** für **Set Hostname via DHCP**.
5. Wählen Sie für **Modify DNS Configuration** die Option **Use Custom Policy**.
6. Geben Sie die folgenden Informationen entsprechend Ihrer Netzwerkeinstellungen an:
   - **Static Hostname** –Geben Sie den DNS-Hostnamen der Maschine an.
   - **Name server**: Geben Sie die IP-Adresse des DNS-Servers an. Dies ist in der Regel die IP-Adresse des Active Directory-Domänencontrollers.
   - **Domain Search list**: Geben Sie den DNS-Domänennamen an.
7. Ändern Sie die folgende Zeile der Datei `/etc/hosts`, sodass sie den FQDN und den Hostnamen als die ersten beiden Einträge enthält:

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

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

> Hostnamen.

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

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

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

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

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

Mit diesem Befehl wird der FQDN der Maschine zurückgegeben.

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

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

Schritt 1c: Konfigurieren des NTP-Diensts

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

SUSE 15.4:

1. Starten Sie das UI-basierte YaST-Tool.
2. Wählen Sie **Network Services** und dann **NTP Configuration**.
3. Wählen Sie im Abschnitt **Start NTP Daemon** die Option **Now and on Boot**.

4. Wählen Sie für **Configuration Source** die Option **Dynamic**.
5. Fügen Sie nach Bedarf NTP-Server hinzu. Der NTP-Dienst wird normalerweise auf dem Active Directory-Domänencontroller gehostet.
6. Falls vorhanden, löschen Sie die folgende Zeile in /etc/chrony.conf oder kommentieren Sie sie aus.

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

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

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

Schritt 1d: Installieren von Linux VDA-abhängigen Paketen

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

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

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

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

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

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

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

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

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


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

Installieren und Angeben einer zu verwendenden Datenbank Sie können die Verwendung von SQLite oder PostgreSQL angeben, indem Sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Bei manuellen Installationen müssen Sie SQLite und PostgreSQL manuell installieren, um diese angeben zu können.

In diesem Abschnitt wird beschrieben, wie Sie die PostgreSQL- und SQLite-Datenbanken installieren und wie Sie eine zu verwendende Datenbank angeben.

> **Hinweis:**
>
> Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.

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

```
sudo zypper install postgresql-server

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

Führen Sie die folgenden Befehle aus, um PostgreSQL beim Start der Maschine bzw. sofort zu starten:

```
sudo systemctl enable postgresql

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

SQLite installieren Führen Sie für SUSE den folgenden Befehl aus, um SQLite zu installieren:

```
sudo zypper install sqlite3
<!--NeedCopy-->
```

Datenbank eingeben Nachdem Sie SQLite, PostgreSQL oder beides installiert haben, können Sie eine zu verwendende Datenbank angeben, indem Sie sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Führen Sie hierzu die folgenden Schritte aus:

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Lassen Sie diesen Schritt aus, wenn es sich um eine Neuinstallation handelt.
2. Bearbeiten Sie **/etc/xdl/db.conf**, um eine zu verwendende Datenbank anzugeben.

3. Führen Sie **ctxsetup.sh** aus.

> **Hinweis:**
>
> Sie können auch **/etc/xdl/db.conf** verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

Schritt 2: Vorbereiten des Hypervisors

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

Festlegen der Zeitsynchronisierung auf Citrix Hypervisor

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

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

```
su -

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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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


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

```
xen.independent_wallclock = 1
```

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

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

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

```
su -

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

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

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

Auf dem verwaltenden Betriebssystem:

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

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

Festlegen der Zeitsynchronisierung auf ESX und ESXi

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

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

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

Schritt 3: Linux-VM zur Windows-Domäne hinzufügen

Mit den folgenden Methoden können Linux-Maschinen zur Active Directory-Domäne (AD) hinzugefügt werden:

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Folgen Sie den Anweisungen für die von Ihnen gewählte Methode.

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

Samba Winbind

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

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

4. Wenn ein Domänencontroller gefunden wird, werden Sie gefragt, ob Sie der Domäne beitreten möchten. Klicken Sie auf **Ja**.
5. Wenn Sie dazu aufgefordert werden, geben Sie die Anmeldeinformationen eines Domänenbenutzers ein, der die Berechtigung hat, Maschinen der Domäne hinzuzufügen, und klicken Sie auf **OK**.
6. Starten Sie Ihre Dienste manuell neu oder starten Sie die Maschine neu. Wir empfehlen Ihnen, den Computer neu zu starten:

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

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

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

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

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

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

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

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

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

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

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unter-

schiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

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

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

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

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

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

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

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

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

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

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

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

Beenden Sie die Sitzung.

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


Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Quest Authentication Service

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

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

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

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

Quest auf Linux VDA konfigurieren

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

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

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-auth false
<!--NeedCopy-->
```

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

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

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

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

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

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

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

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

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

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

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

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

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

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


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

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

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

Beenden Sie die Sitzung.

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Centrify DirectControl

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

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

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

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

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

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

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all
```



```
2
3 adinfo  – diag
4 <!--NeedCopy-->
```

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

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

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

SSSD

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

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

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

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

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

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

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

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


3. Installieren oder aktualisieren Sie die erforderlichen Pakete:

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

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

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur 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
<!--NeedCopy-->
```

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

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

```
[global]
    workgroup = domain

```



```
    client signing = yes

    client use spnego = yes

    kerberos method = secrets and keytab

    realm = REALM

    security = ADS
<!--NeedCopy-->
```

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

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

```
passwd: compat sss

group: compat sss
<!--NeedCopy-->
```

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

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

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

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

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

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

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

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

SSSD einrichten

1. Bearbeiten Sie /etc/sssd/sssd.conf als Root-Benutzer, damit der SSSD-Daemon mit der Zieldomäne kommunizieren kann. Muster einer sssd.conf-Konfiguration (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

<!--NeedCopy-->
```

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

> **Hinweis:**
>
> ldap_id_mapping ist auf **true** festgelegt, sodass SSSD die Zuordnung von Windows SIDs zu Unix UIDs selbst vornimmt. Andernfalls muss Active Directory POSIX-Erweiterungen bereitstellen können. **ad_gpo_access_control** ist auf **permissive** festgelegt, um einen ungültigen Anmeldefehler für Linux-Sitzungen zu verhindern. Weitere Informationen finden Sie in den Manpages für sssd.conf und sssd-ad.

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

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


Aktivieren von SSSD 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
<!--NeedCopy-->
```

Domäneneigentümerschaft überprüfen

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

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

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

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

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

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

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind.

Führen Sie den Kerberos-Befehl **kinit** aus, um die Maschine mit dem Domänencontroller zu authentifizieren, die diese Schlüssel verwendet:

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

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

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

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


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

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

```
ssh localhost -l domain\username

id -u

klist

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

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

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

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

Download des erforderlichen PBIS-Pakets Beispiel:

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

Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei Beispiel:

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

Ausführen des PBIS-Installationsskripts Beispiel:

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


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

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

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

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

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

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

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

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

```
ssh localhost -l domain\user

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

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

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

Beenden Sie die Sitzung.

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

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

Schritt 4: .NET Runtime 6.0 installieren

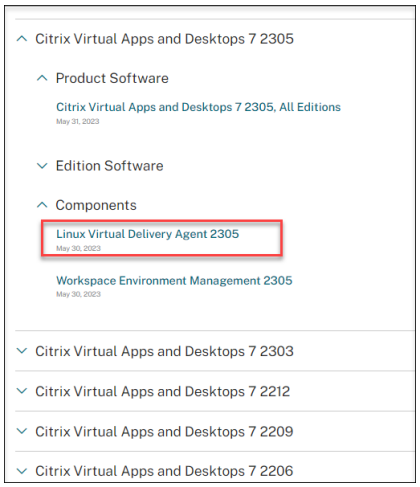
Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

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

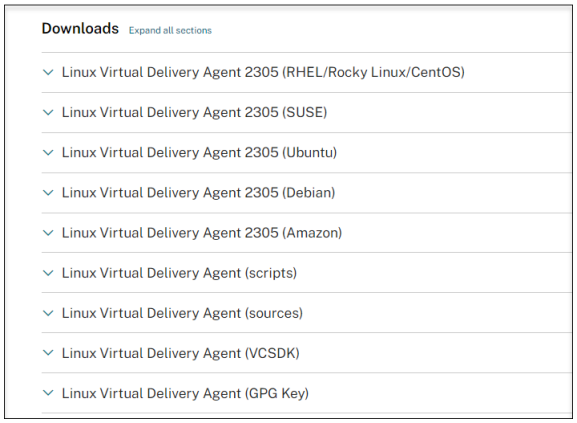
Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

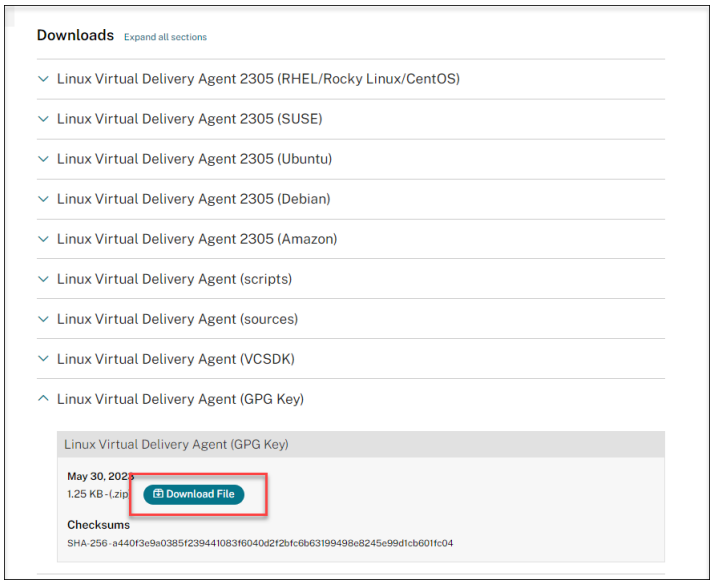
1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
2. Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. Erweitern Sie **Komponenten**, um den Linux VDA zu finden. Beispiel:



4. Klicken Sie auf den Linux VDA-Link, um auf die Linux VDA-Downloads zuzugreifen.



5. Laden Sie das Linux VDA-Paket herunter, das Ihrer Linux-Distribution entspricht.
6. Laden Sie den öffentlichen GPG-Schlüssel herunter, mit dem Sie die Integrität des Linux VDA-Pakets überprüfen können. Beispiel:



Um die Integrität des Linux VDA-Pakets mithilfe des öffentlichen Schlüssels zu überprüfen, führen Sie die folgenden Befehle aus, um den öffentlichen Schlüssel in die RPM-Datenbank zu importieren und die Überprüfung durchzuführen:

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

Schritt 6: Installieren des Linux VDA

Schritt 6a: Deinstallieren der alten Version

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

1. Halten Sie die Linux VDA-Dienste an:

```
sudo /sbin/service ctxvda stop

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

> **Hinweis:**
>
> Führen Sie erst den Befehl **systemctl stop ctxmonitord** aus, um den Monitor Service Dae-

> mon zu stoppen, bevor Sie die Dienste **ctxvda** und **ctxhdx** stoppen. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

2. Deinstallieren Sie das Paket:

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

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

Schritt 6b: Installieren des Linux VDA

Installieren der Linux VDA-Software mit Zypper:

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

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

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

Schritt 6c: Upgrade des Linux VDA (optional)

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

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

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

RPM-Abhängigkeitsliste für SUSE 15:


```
java-11-openjdk >= 11

ImageMagick >= 7.0

dbus-1 >= 1.12.2

dbus-1-x11 >= 1.12.2

xorg-x11 >= 7.6_1

libXpm4 >= 3.5.12

libXrandr2 >= 1.5.1

libXtst6 >= 1.2.3

pam >= 1.3.0

bash >= 4.4

findutils >= 4.6

gawk >= 4.2

sed >= 4.4

cups >= 2.2

cups-filters >= 1.25

libxml2-2 >= 2.9

libmspack0 >= 0.6

ibus >= 1.5

libtcmalloc4 >= 2.5

libcap-progs >= 2.26

mozilla-nss-tools >= 3.53.1

libpython3_6m1_0 >= 3.6~

libQt5Widgets5 >= 5.12

libqrencode4 >= 4.0.0

libImlib2-1 >= 1.4.10
<!--NeedCopy-->
```


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

Schritt 7: Installieren von NVIDIA GRID-Treibern

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

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

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

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

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

Schritt 8: Konfigurieren des Linux VDA

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

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

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

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


Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

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

Automatische Konfiguration

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

Unterstützte Umgebungsvariablen umfassen u. a.:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Standardeinstellung ist N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'**–Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist standardmäßig Port 80.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –Die Linux VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für den Linux VDA öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd** –Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt.
- **CTX_XDL_HDX_3D_PRO=Y | N** –Der Linux VDA unterstützt HDX 3D Pro –GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Bei aktiviertem HDX 3D Pro wird der VDA für VDI-Desktopmodus (Einzelsitzungen) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y | N** –Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmod-

ell. Legen Sie dies bei Umgebungen mit HDX 3D Pro auf "Y"fest. Standardmäßig ist diese Variable auf N festgelegt.

- **CTX_XDL_SITE_NAME=dns-name** –Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** –Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268 oder ad1.mycompany.com:636 ad2.mycompany.com:3269 ad3.mycompany.com:3269, wenn Sie LDAPS verwenden. Für schnellere LDAP-Abfragen in einer Active Directory-Gesamtstruktur aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben als LDAP-Portnummer 3268 bzw., sofern Sie LDAPS verwenden, 3269 an. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE=search-base-set** –Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** –Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** –Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

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

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

   - **Für MATE-Desktop unter SUSE 15**

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

   - **Für GNOME Classic Desktop auf SUSE 15**

     ```
     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 auf SUSE 15**

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

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

Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebung anpassen. Um dieses Feature zu aktivieren, müssen Sie umschaltbare Desktopumgebungen vorher auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen nach Sitzungsbenutzern.

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

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

```
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=winbind | quest |centrify | sssd

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

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

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

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

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

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

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

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

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

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

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:

```
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=winbind | quest |centrify | sssd \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \
```



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

Entfernen von Konfigurationsänderungen

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

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

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

Entfernen von Konfigurationsänderungen:

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

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

Konfigurationsprotokolle

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

`/tmp/xdl.configure.log`

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

Schritt 9: Ausführen von XDPing

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

Schritt 10: Ausführen des Linux VDA

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

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start

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

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

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

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

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop

sudo /sbin/service ctxhdx restart

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

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:


```
sudo /sbin/service ctxvda status

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

Schritt 11: Maschinenkataloge erstellen

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

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

- Auswahl des Betriebssystems:
  - Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

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

Schritt 12: Bereitstellungsgruppen erstellen

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

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

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

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

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2308.

Linux VDA manuell auf Ubuntu installieren

May 30, 2024

> **Wichtig:**
>
> Für Neuinstallationen empfehlen wir die Verwendung von Easy Install für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

Schritt 1: Vorbereiten der Konfigurationsinformationen und der Linux-Maschine

Schritt 1a: Überprüfen der Netzwerkkonfiguration

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

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

```
preserve_hostname: true
```


Schritt 1b: Festlegen des Hostnamens

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

```
hostname
```

Schritt 1c: Zuweisen einer Loopbackadresse für den Hostnamen

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

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

Beispiel:

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

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

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

Schritt 1d: Überprüfen des Hostnamens

Stellen Sie sicher, dass der Hostname richtig festgelegt ist:

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

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

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

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


Dieser Befehl gibt den FQDN der Maschine zurück.

Schritt 1e: Deaktivieren von Multicast-DNS

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

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

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

In:

```
hosts: files dns
```

Schritt 1f: Überprüfen von Namensauflösung und Diensterreichbarkeit

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

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

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

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

Schritt 1g: Konfigurieren der Uhrsynchronisierung (Chrony)

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

chrony installieren:

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

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


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

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

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

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

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

Schritt 1h: Installieren von OpenJDK 11

Der Linux VDA erfordert das Vorhandensein von OpenJDK 11.

Ubuntu 22.04 beinhaltet OpenJDK 11.

Führen Sie den folgenden Befehl aus, um OpenJDK 11 unter Ubuntu 20.04 zu installieren:

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

Schritt 1i: Installieren und Angeben einer zu verwendenden Datenbank

Sie können die Verwendung von SQLite oder PostgreSQL angeben, indem Sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Bei manuellen Installationen müssen Sie SQLite und PostgreSQL manuell installieren, um diese angeben zu können.

In diesem Abschnitt wird beschrieben, wie Sie die PostgreSQL- und SQLite-Datenbanken installieren und wie Sie eine zu verwendende Datenbank angeben.

> **Hinweis:**
>
> Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.

PostgreSQL installieren Führen Sie zum Installieren von PostgreSQL die folgenden Befehle aus:

```
sudo apt-get install -y postgresql

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


Führen Sie die folgenden Befehle aus, um PostgreSQL beim Start der Maschine bzw. sofort zu starten:

```
sudo systemctl enable postgresql

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

SQLite installieren Führen Sie für Ubuntu den folgenden Befehl aus, um SQLite zu installieren:

```
sudo apt-get install -y sqlite3
<!--NeedCopy-->
```

Datenbank eingeben Nachdem Sie SQLite, PostgreSQL oder beides installiert haben, können Sie eine zu verwendende Datenbank angeben, indem Sie sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Führen Sie hierzu die folgenden Schritte aus:

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Lassen Sie diesen Schritt aus, wenn es sich um eine Neuinstallation handelt.
2. Bearbeiten Sie **/etc/xdl/db.conf**, um eine zu verwendende Datenbank anzugeben.
3. Führen Sie **ctxsetup.sh** aus.

> **Hinweis:**
>
> Sie können auch **/etc/xdl/db.conf** verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

Schritt 1j: Installieren von Motif

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

Schritt 1k: Installieren weiterer Pakete

Ubuntu 22.04:

```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.5-0
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Ubuntu 20.04:


```
sudo apt-get install -y libsasl2-2
sudo apt-get install -y libsasl2-modules-gssapi-mit
sudo apt-get install -y libldap-2.4-2
sudo apt-get install -y krb5-user
sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Schritt 2: Vorbereiten des Hypervisors

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

Festlegen der Zeitsynchronisierung auf Citrix Hypervisor

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

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

```
su -

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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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


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

```
xen.independent_wallclock = 1
```

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

```
su -

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

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

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

Auf dem verwaltenden Betriebssystem:

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

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

Festlegen der Zeitsynchronisierung auf ESX und ESXi

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

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

1. Öffnen Sie den vSphere-Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Virtual Machine Properties** die Registerkarte **Options**.

4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Advanced** das Kontrollkästchen **Synchronize guest time with host**.

Schritt 3: Linux-VM zur Windows-Domäne hinzufügen

Mit den folgenden Methoden können Linux-Maschinen zur Active Directory-Domäne (AD) hinzugefügt werden:

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

Folgen Sie den Anweisungen für die von Ihnen gewählte Methode.

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

Samba Winbind

Installieren oder aktualisieren Sie die erforderlichen Pakete

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

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

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

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

Kerberos konfigurieren Öffnen Sie als Root-Benutzer **/etc/krb5.conf** und nehmen Sie folgende Einstellungen vor:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen

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

```
[libdefaults]
default_realm = REALM
dns_lookup_kdc = false
[realms]
REALM = {
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

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

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

Führen Sie den Befehl **vim /etc/samba/smb.conf** aus, um **/etc/samba/smb.conf** zu öffnen, und nehmen Sie dann die folgenden Einstellungen vor:

```
[global]
workgroup = WORKGROUP
security = ADS
realm = REALM
encrypt passwords = yes
idmap config *:range = 16777216-33554431
kerberos method = secrets and keytab
winbind refresh tickets = yes
template shell = /bin/bash
```

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

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

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

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

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

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

winbind neu starten

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

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

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

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

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

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

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

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

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


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

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

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

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

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

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

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

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

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

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

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

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

Um sich zu vergewissern, dass das Winbind-PAM-Modul fehlerfrei konfiguriert ist, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
ssh localhost -l domain\username

```



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

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

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

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

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

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

Beenden Sie die Sitzung.

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

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

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

Quest Authentication Service

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

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

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

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

Quest auf Linux VDA konfigurieren

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

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

```
SELINUX=disabled
```

Diese Änderung erfordert einen Neustart der Maschine:

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

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

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

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

sudo /opt/quest/bin/vastool configure vas vas_auth allow-disconnected-
    auth false
<!--NeedCopy-->
```


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

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

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

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

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

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

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

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

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

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

```
ERROR: No domain could be found.
ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm
default_realm not configured in vas.conf. Computer may not be joined
to domain
```

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


```
ssh localhost -l domain\username

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

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

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache gültig und nicht abgelaufen sind:

```
/opt/quest/bin/vastool klist
<!--NeedCopy-->
```

Beenden Sie die Sitzung.

```
exit
<!--NeedCopy-->
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Centrify DirectControl

Windows-Domäne beitreten Wenn der Centrify DirectControl Agent installiert ist, machen Sie die Linux-Maschine mit dem Centrify-Befehl **adjoin** zu einem Mitglied der Active Directory-Domäne:

```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

Der Parameter **user** ist ein Active Directory-Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern von **Active Directory**-Domänen zu machen. Der Parameter **domain-name** ist der Name der Domäne, der die Linux-Maschine beitritt.

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux) ein Computerobjekt in **Active Directory** haben. Mit folgendem Befehl prüfen Sie, ob eine per Centrify hinzugefügte Linux-Maschine Mitglied der Domäne ist:

```
su -

adinfo
<!--NeedCopy-->
```


Stellen Sie sicher, dass der Wert **Joined to domain** gültig ist und dass **CentrifyDC mode** den Wert **connected** zurückgibt. Wenn der Modus im Startzustand stecken bleibt, hat der Centrify-Client Serververbindungs- oder Authentifizierungsprobleme.

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all

adinfo --diag
<!--NeedCopy-->
```

Testen Sie die Verbindung mit den verschiedenen Active Directory- und Kerberos-Diensten.

```
adinfo --test
<!--NeedCopy-->
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

SSSD

Kerberos konfigurieren Führen Sie zum Installieren von Kerberos den folgenden Befehl aus:

```
sudo apt-get install krb5-user
<!--NeedCopy-->
```

Zum Konfigurieren von Kerberos öffnen Sie als Root-Benutzer **/etc/krb5.conf** und legen Sie folgende Parameter fest:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
[libdefaults]

default_realm = REALM

dns_lookup_kdc = false

[realms]

REALM = {

admin_server = domain-controller-fqdn

kdc = domain-controller-fqdn

}

[domain_realm]
```


domain-dns-name = *REALM*

.*domain-dns-name* = *REALM*

Der Parameter domain-dns-name ist in diesem Kontext der DNS-Domänenname, z. B. example.com. *REALM* ist der Kerberos-Bereichsname in Großbuchstaben, z. B. EXAMPLE.COM.

Domäne beitreten SSSD muss für die Verwendung von Active Directory als Identitätsanbieter und Kerberos zur Authentifizierung konfiguriert werden. SSSD bietet keine AD-Clientfunktionen für den Domänenbeitritt und die Verwaltung der Systemschlüsseltabelle. Sie können stattdessen **adcli**, **realmd** oder **Samba** verwenden.

> **Hinweis:**
>
> Dieser Abschnitt enthält nur Informationen für **adcli** und **Samba**.

- **Wenn Sie der Domäne mit adcli beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie **adcli**.

```
sudo apt-get install adcli
<!--NeedCopy-->
```

2. Treten Sie mit **adcli** der Domäne bei.

   Entfernen Sie die alte Systemdatei für die Schlüsseltabelle und treten Sie der Domäne mit folgenden Befehl bei:

```
su -

rm -rf /etc/krb5.keytab

adcli join domain-dns-name -U user -H hostname-fqdn
<!--NeedCopy-->
```

   user ist ein Domänenbenutzer mit der Berechtigung zum Hinzufügen von Maschinen zur Domäne. **hostname-fqdn** ist der Hostname für die Maschine im FQDN-Format.

   Die Option **-H** ist erforderlich, damit **adcli** SPN im folgenden, vom Linux VDA benötigten Format erstellen kann: host/hostname-fqdn@REALM.

3. Überprüfen Sie die Domänenmitgliedschaft.

   Führen Sie auf Maschinen mit Ubuntu 22.04 und Ubuntu 20.04 den Befehl `adcli testjoin` aus, um zu testen, ob sie mit der Domäne verbunden sind.

- **Wenn Sie der Domäne mit Samba beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.


```
sudo apt-get install samba krb5-user
<!--NeedCopy-->
```

2. Konfigurieren Sie **Samba**.

   Öffnen Sie **/etc/samba/smb.conf** und nehmen Sie folgende Einstellungen vor:

   ```
   [global]
   workgroup = WORKGROUP
   security = ADS
   realm = REALM
   client signing = yes
   client use spnego = yes
   kerberos method = secrets and keytab
   ```

   WORKGROUP ist das erste Feld in **REALM** und **REALM** ist der Kerberos-Bereichsname in Großbuchstaben.

3. Treten Sie der Domäne mit **Samba** bei.

   Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Windows-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen.

   ```
   sudo net ads join REALM -U user
   <!--NeedCopy-->
   ```

   REALM ist der Kerberos-Bereichsname in Großbuchstaben und **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

SSSD einrichten Installieren oder aktualisieren Sie die erforderlichen Pakete:

Installieren Sie ggf. die erforderlichen SSSD- und Konfigurationspakete:

```
sudo apt-get install sssd
<!--NeedCopy-->
```

Wenn die Pakete bereits installiert sind, wird die Aktualisierung empfohlen:

```
sudo apt-get install --only-upgrade sssd
<!--NeedCopy-->
```

> **Hinweis:**
>
> Beim Installationsvorgang in Ubuntu werden **nsswitch.conf** und das PAM-Anmeldemodul au-

> tomatisch konfiguriert.

SSSD konfigurieren Vor dem Start des SSSD-Daemon sind SSSD-Konfigurationsänderungen erforderlich. Für einige Versionen von SSSD ist die Konfigurationsdatei **/etc/sssd/sssd.conf** nicht standardmäßig installiert und muss manuell erstellt werden. Öffnen oder erstellen Sie als Root-Benutzer **/etc/sssd/sssd.conf** und nehmen Sie folgende Einstellungen vor:

```
[sssd]
services = nss, pam
config_file_version = 2
domains = domain-dns-name
[domain/domain-dns-name]
id_provider = ad
access_provider = ad
auth_provider = krb5
krb5_realm = REALM
# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days
krb5_renewable_lifetime = 14d
# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours
krb5_renew_interval = 1h
krb5_ccachedir = /tmp
krb5_ccname_template = FILE:%d/krb5cc_%U
# This ldap_id_mapping setting is also the default value
ldap_id_mapping = true
override_homedir = /home/%d/%u
default_shell = /bin/bash
ad_gpo_map_remote_interactive = +ctxhdx
```

> **Hinweis:**
>
> ldap_id_mapping ist auf **true** festgelegt, sodass SSSD die Zuordnung von Windows SIDs zu Unix UIDs selbst vornimmt. Andernfalls muss Active Directory POSIX-Erweiterungen bereitstellen kön-

> nen. Der PAM-Dienst `ctxhdx` wird ad_gpo_map_remote_interactive hinzugefügt.
>
> Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. example.com. **REALM** ist der Kerberos-Bereichsname in Großbuchstaben, z. B. EXAMPLE.COM. Die Konfiguration des NetBIOS-Domänennamens ist nicht erforderlich.
>
> Weitere Informationen zu den Konfigurationseinstellungen finden Sie auf den Manpages über sssd.conf und `sssd-ad`.

Für den SSSD-Daemon muss die Konfigurationsdatei Besitzer-Leseberechtigung haben:

```
sudo chmod 0600 /etc/sssd/sssd.conf
<!--NeedCopy-->
```

SSSD-Daemon starten Führen Sie die folgenden Befehle aus, um den SSSD-Daemon zu starten und den Daemon beim Systemstart der Maschine zu aktivieren:

```
sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```

PAM-Konfiguration Führen Sie den folgenden Befehl aus. Stellen Sie sicher, dass die Optionen **SSS authentication** und **Create home directory on login** aktiviert sind:

```
sudo pam-auth-update
<!--NeedCopy-->
```

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux VDAs) ein Computerobjekt in `Active Directory` haben.

- Wenn Sie die Domänenmitgliedschaft mit **adcli** überprüfen, führen Sie den Befehl `sudo adcli info domain-dns-name` aus, um die Domäneninformationen anzuzeigen.
- Wenn Sie die Domänenmitgliedschaft mit **Samba** überprüfen, führen Sie den Befehl `sudo net ads testjoin` aus, um zu überprüfen, ob die Maschine Mitglied einer Domäne ist, und den Befehl `sudo net ads info` zum Überprüfen zusätzlicher Domänen- und Computerobjektinformationen.

Kerberos-Konfiguration überprüfen Überprüfen Sie, ob Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, indem Sie sicherstellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde und gültige Schlüssel enthält:


```
sudo klist -ke
<!--NeedCopy-->
```

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller mit diesen Schlüsseln zu authentifizieren:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT für das Maschinenkonto zwischengespeichert wurde:

```
sudo klist
<!--NeedCopy-->
```

Benutzerauthentifizierung überprüfen SSSD bietet kein Befehlszeilentool zum direkten Testen der Authentifizierung mit dem Daemon, daher kann der Test nur mit PAM ausgeführt werden.

Um sich zu vergewissern, dass das SSSD-PAM-Modul fehlerfrei konfiguriert wurde, melden Sie sich mit einem bislang noch nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
ssh localhost -l domain\username

id -u

klist

exit
<!--NeedCopy-->
```

Stellen Sie sicher, dass die vom Befehl **klist** zurückgegebenen Kerberos-Tickets für den Benutzer richtig und nicht abgelaufen sind.

Überprüfen Sie als Root-Benutzer, dass eine entsprechende Ticketcachedatei für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```


Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt am KDE- oder Gnome-Anzeigemanager anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

Download des erforderlichen PBIS-Pakets

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
    /9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Ausführen des PBIS-Installationsskripts

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Windows-Domäne beitreten Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
<!--NeedCopy-->
```

user ist ein Domänenbenutzer mit der Berechtigung, Computer zur Active Directory-Domäne hinzuzufügen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Hinweis: Führen Sie den Befehl **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** aus, um Bash als Standardshell festzulegen.

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux VDAs) ein Computerobjekt in `Active Directory` haben. Mit folgendem Befehl prüfen Sie, ob eine per PBIS angemeldete Linux-Maschine zur Domäne gehört:

```
/opt/pbis/bin/domainjoin-cli query
<!--NeedCopy-->
```

Wenn die Maschine einer Domäne beigetreten ist, werden mit diesem Befehl Informationen zur aktuell beigetretenen AD-Domäne und Organisationseinheit abgefragt. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen Um sicherzustellen, dass PBIS Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
sudo ssh localhost -l domain\user

id -u
<!--NeedCopy-->
```

Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Beenden Sie die Sitzung.

```
exit
<!--NeedCopy-->
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Schritt 4: .NET Runtime 6.0 installieren

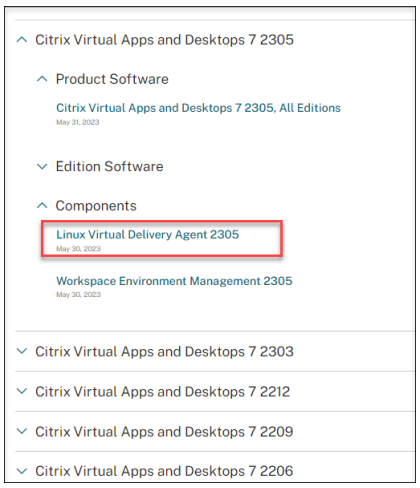
Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

Führen Sie nach der Installation von .NET Runtime 6.0 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

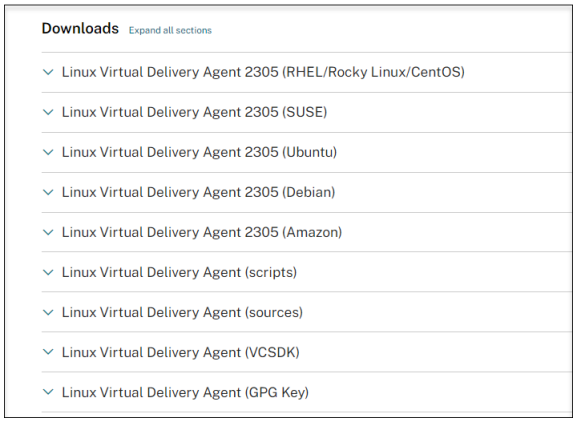
Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Herunterladen des Linux VDA-Pakets

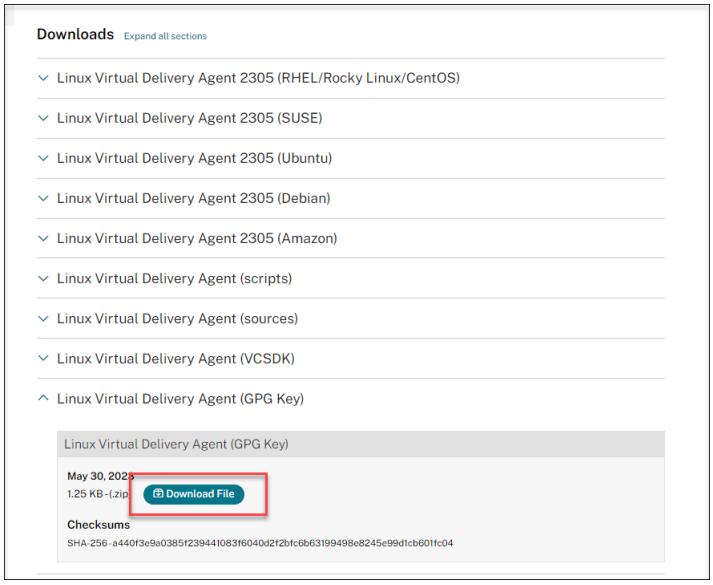
1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
2. Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. Erweitern Sie **Komponenten**, um den Linux VDA zu finden. Beispiel:



4. Klicken Sie auf den Linux VDA-Link, um auf die Linux VDA-Downloads zuzugreifen.



5. Laden Sie das Linux VDA-Paket herunter, das Ihrer Linux-Distribution entspricht.
6. Laden Sie den öffentlichen GPG-Schlüssel herunter, mit dem Sie die Integrität des Linux VDA-Pakets überprüfen können. Beispiel:



Um die Integrität des Linux VDA-Pakets zu überprüfen, führen Sie die folgenden Befehle aus, um den öffentlichen Schlüssel in die DEB-Datenbank zu importieren und die Überprüfung durchzuführen:

```
sudo apt-get install dpkg-sig
gpg --import <path to the public key>
dpkg-sig --verify <path to the Linux VDA package>
<!--NeedCopy-->
```

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 <PATH>/<Linux VDA DEB>
apt-get install -f
<!--NeedCopy-->
```

> **Hinweis:**
>
> Deaktivieren Sie RDNS für Ubuntu 20.04 auf GCP. Fügen Sie dazu in /etc/krb5.conf die Zeile **rdns = false** unter **[libdefaults]** hinzu.

Debian-Abhängigkeitsliste für Ubuntu 22.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.11

```



```
libgtkmm-3.0-1v5 >= 3.24.5

ufw >= 0.36

ubuntu-desktop >= 1.481

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.37

gtk3-nocsd >= 3

bash >= 5.1

findutils >= 4.8.0

sed >= 4.8

cups >= 2.4

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.9~

libpython3.10 >= 3.10~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.68

libqt5widgets5 >= 5.15~

libqrencode4 >= 4.1.1

libimlib2 >= 1.7.4
<!--NeedCopy-->
```

Debian-Abhängigkeitsliste für Ubuntu 20.04:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

libgtkmm-3.0-1v5 >= 3.24.2

ufw >= 0.36

```



```
ubuntu-desktop >= 1.450

libxrandr2 >= 2:1.5.2

libxtst6 >= 2:1.2.3

libxm4 >= 2.3.8

util-linux >= 2.34

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.7.0

sed >= 4.7

cups >= 2.3

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.8 >= 3.8~

libsasl2-modules-gssapi-mit >= 2.1.~

libnss3-tools >= 2:3.49

libqt5widgets5 >= 5.7~

libqrencode4 >= 4.0.0

libimlib2 >= 1.6.1
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine Übersicht der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden, finden Sie in der Tabelle Systemanforderungen.

Schritt 6b: Upgrade des Linux VDA (optional)

Sie können ein Upgrade für ein vorhandene Installation der vorherigen beiden Versionen und von einer LTSR-Version durchführen.

```
sudo dpkg -i <PATH>/<Linux VDA deb>
<!--NeedCopy-->
```


> **Hinweis:**
>
> Durch das Upgrade einer Installation werden die Konfigurationsdateien unter /etc/xdl. überschrieben. Sichern Sie die Dateien vor jedem Upgrade.

Schritt 7: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro müssen Sie die NVIDIA GRID-Treiber auf Ihrem Hypervisor und auf den VDA-Maschinen installieren.

Informationen zum Installieren und Konfigurieren des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Handbüchern:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Zum Installieren und Konfigurieren der NVIDIA GRID-Gast-VM-Treiber führen Sie die folgenden allgemeinen Schritte aus:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM in der Hypervisor-Systemsteuerung eine GPU zu.
3. Starten Sie die VM.
4. Installieren Sie den Gast-VM-Treiber auf der VM.

Schritt 8: Konfigurieren des Linux VDA

> **Hinweis:**
>
> Stellen Sie vor dem Einrichten der Laufzeitumgebung sicher, dass das Gebietsschema **en_US.UTF-8** in Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema im Betriebssystem nicht verfügbar ist, führen Sie den Befehl **sudo locale-gen en_US.UTF-8** aus. Für Debian bearbeiten Sie die Datei **/etc/locale.gen** durch Auskommentierung der Zeile **# en_US.UTF-8 UTF-8**. Führen Sie dann den Befehl **sudo locale-gen** aus.

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Das Skript überprüft die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Führen Sie Änderungen erst danach durch. Sie können das Skript nach Bedarf jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell unter Reaktion auf Aufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript durch, bevor Sie fortfahren:


```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
<!--NeedCopy-->
```

Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Automatische Konfiguration

Bei einer automatischen Installation können die für das Setupskript erforderlichen Optionen mit Umgebungsvariablen angegeben werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript keine weiteren Informationen vom Benutzer und der Installationsvorgang wird per Skript ausgeführt.

Unterstützte Umgebungsvariablen umfassen u. a.:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Standardeinstellung ist N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'**–Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist standardmäßig Port 80.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –Die Linux VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für den Linux VDA öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis** –Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt.

- **CTX_XDL_HDX_3D_PRO=Y | N** – Der Linux VDA unterstützt HDX 3D Pro – GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Bei aktiviertem HDX 3D Pro wird der VDA für VDI-Desktopmodus (Einzelsitzungen) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y | N** – Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Legen Sie dies bei Umgebungen mit HDX 3D Pro auf "Y"fest. Standardmäßig ist diese Variable auf N festgelegt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268 oder ad1.mycompany.com:636 ad2.mycompany.com:3269 ad3.mycompany.com:3269, wenn Sie LDAPS verwenden. Für schnellere LDAP-Abfragen in einer Active Directory-Gesamtstruktur aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben als LDAP-Portnummer 3268 bzw., sofern Sie LDAPS verwenden, 3269 an. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI, DC=mycompany,DC=com). Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (`ctxvda`). Der Standardpfad ist /usr/bin.

- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

  Sie können die Desktopumgebung für Sitzungsbenutzer auch über die folgenden Schritte ändern:

  1. Erstellen Sie die Datei `.xsession` auf dem VDA im Verzeichnis **$HOME/<username>**.
  2. Geben Sie in der Datei `.xsession` eine auf Distributionen basierende Desktopumgebung an.

     - **Für MATE-Desktop**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

     - **Für GNOME Classic-Desktop**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     ```

     - **Für GNOME-Desktop**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     exec gnome-session
     fi
     ```

  3. Teilen Sie die 700-Dateiberechtigung mit dem Zielsitzungsbenutzer.

  Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebung anpassen. Um dieses Feature zu aktivieren, müssen Sie umschaltbare Desktopumgebungen vorher auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen nach Sitzungsbenutzern.

- **CTX_XDL_START_SERVICE=Y | N** –Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Die Standardeinstellung ist Y.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
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=winbind | quest |centrify | sssd | pbis

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
    none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
<!--NeedCopy-->
```

Sie müssen die Option **-E** mit dem Befehl “sudo”angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:

```
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 \
```



```
8
9  CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
36 <!--NeedCopy-->
```

Entfernen von Konfigurationsänderungen

In einigen Fällen müssen die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernt werden, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

Entfernen von Konfigurationsänderungen:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--NeedCopy-->
```

> **Wichtig:**
>
> Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank, sodass der Linux VDA nicht funktionsfähig ist.

Konfigurationsprotokolle

Die Skripts **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an und schreiben weitere Informationen in die Konfigurationsprotokolldatei **/tmp/xdl.configure.log**.

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

Deinstallieren der Linux VDA-Software

Überprüfen, ob der Linux VDA installiert ist, und Anzeigen der Version des installierten Pakets:

```
dpkg -l xendesktopvda
<!--NeedCopy-->
```

Anzeigen weiterer Details:

```
apt-cache show xendesktopvda
<!--NeedCopy-->
```

Deinstallieren der Linux VDA-Software:

```
dpkg -r xendesktopvda
<!--NeedCopy-->
```

> **Hinweis:**
>
> Beim Deinstallieren der Linux VDA-Software werden die damit verknüpften PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden nicht gelöscht.
>
> **Tipp:**
>
> Die Informationen in diesem Abschnitt beziehen sich nicht auf das Entfernen von abhängigen Paketen einschließlich PostgreSQL.

Schritt 9: Ausführen von XDPing

Mit `sudo /opt/Citrix/VDA/bin/xdping` können Sie Linux VDA-Umgebungen auf häufige Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 10: Ausführen des Linux VDA

Wenn Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, können Sie den Linux VDA mit den folgenden Befehlen steuern.

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

> **Hinweis:**
>
> Führen Sie erst den Befehl **systemctl stop ctxmonitord** aus, um den Monitor Service Daemon zu stoppen, bevor Sie die Dienste **ctxvda** und **ctxhdx** stoppen. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```

Schritt 11: Maschinenkataloge erstellen

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt der traditionellen Windows VDA-Methode. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.

Beim Erstellen von Maschinenkatalogen mit Linux VDA-Maschinen gibt es einige Einschränkungen,

durch die sich der Prozess von der Maschinenkatalogerstellung für Windows VDA-Maschinen unterscheidet:

- Auswahl des Betriebssystems:
  - Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

> **Hinweis:**
>
> In früheren Citrix Studio-Versionen wurde Linux als Betriebssystem nicht unterstützt. Durch die Auswahl von **Windows-Serverbetriebssystem** oder **Serverbetriebssystem** wird jedoch ein äquivalentes gehostetes, freigegebenes Desktopbereitstellungsmodell bereitgestellt. Durch die Auswahl von **Windows-Desktopbetriebssystem** oder **Desktopbetriebssystem** wird ein Bereitstellungsmodell für Einzelbenutzermaschinen bereitgestellt.
>
> **Tipp:**
>
> Wenn Sie eine Maschine aus einer Active Directory-Domäne entfernen und sie ihr dann wieder hinzufügen, muss die Maschine auch aus dem Maschinenkatalog entfernt und ihm dann erneut hinzugefügt werden.

Schritt 12: Bereitstellungsgruppen erstellen

Die Prozesse zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen mit Linux VDA- bzw. Windows VDA-Maschinen sind fast identisch. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Bereitstellungsgruppen.

Beim Erstellen von Bereitstellungsgruppen mit Linux VDA-Maschinenkatalogen gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.
- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2308.

Linux VDA manuell auf Debian installieren

May 30, 2024

> **Wichtig:**
>
> Für Neuinstallationen empfehlen wir die Verwendung von Easy Install für eine schnelle Installation. Easy Install spart Zeit und Arbeitskraft und ist weniger fehleranfällig als die hier beschriebene manuelle Installation.

Schritt 1: Vorbereiten der Konfigurationsinformationen und der Linux-Maschine

Schritt 1a: Festlegen des Hostnamens

Damit der Hostname der Maschine richtig gemeldet wird, ändern Sie die Datei **/etc/hostname**, sodass sie nur den Hostnamen der Maschine enthält.

```
hostname
```

Schritt 1b: Zuweisen einer Loopbackadresse für den Hostnamen

Vergewissern Sie sich, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine korrekt gemeldet werden. Sie können hierfür die folgende Zeile der Datei **/etc/hosts** durch den FQDN und den Hostnamen als erste beiden Einträge erweitern:

```
127.0.0.1 hostname-fqdn hostname localhost
```

Beispiel:

```
127.0.0.1 vda01.example.com vda01 localhost
```

Entfernen Sie alle anderen Verweise auf `hostname-fqdn` oder `hostname` aus anderen Einträgen in der Datei.

> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit nicht das Abschneiden von NetBIOS-Namen. Der Hostname darf nicht länger als 15 Zeichen sein.
>
> **Tipp:**
>
> Verwenden Sie nur Buchstaben (a-z oder A-Z), Ziffern (0-9) und Bindestriche (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Hostnamen sollten nicht mit einer Zahl be-

> ginnen und nicht mit einem Bindestrich enden. Diese Regel gilt auch für Delivery Controller-Hostnamen.

Schritt 1c: Überprüfen des Hostnamens

Starten Sie die Maschine neu und überprüfen Sie, ob der Hostname richtig festgelegt ist:

```
hostname
<!--NeedCopy-->
```

Dieser Befehl gibt nur den Hostnamen der Maschine zurück und nicht den vollqualifizierten Domänennamen (FQDN).

Stellen Sie sicher, dass der FQDN richtig festgelegt ist:

```
hostname -f
<!--NeedCopy-->
```

Dieser Befehl gibt den FQDN der Maschine zurück.

Schritt 1d: Deaktivieren von Multicast-DNS

In den Standardeinstellungen ist Multicast-DNS (**mDNS**) aktiviert, was zu inkonsistenten Ergebnissen bei der Namensauflösung führen kann.

Um **mDNS** zu deaktivieren, bearbeiten Sie **/etc/nsswitch.conf** und ändern die Zeile:

```
hosts: files mdns_minimal [NOTFOUND=return] dns
```

In:

```
hosts: files dns
```

Schritt 1e: Überprüfen von Namensauflösung und Diensterreichbarkeit

Stellen Sie sicher, dass Sie den FQDN auflösen können und pingen Sie den Domänencontroller und den Delivery Controller:

```
nslookup domain-controller-fqdn

ping domain-controller-fqdn

nslookup delivery-controller-fqdn

ping delivery-controller-fqdn
<!--NeedCopy-->
```


Wenn Sie den FQDN nicht auflösen und eine der beiden Maschinen nicht pingen können, überprüfen Sie die vorherigen Schritte, bevor Sie fortfahren.

Schritt 1f: Konfigurieren der Uhrsynchronisierung (Chrony)

Es ist wichtig, dass die Uhrsynchronisierung zwischen den VDAs, den Delivery Controllern und den Domänencontrollern genau ist. Beim Hosten eines Linux VDAs als virtuelle Maschine (VM) kann es zu Zeitabweichungen kommen. Aus diesem Grund sollte die Zeit remote von einem Zeitdienst synchronisiert werden.

chrony installieren:

```
apt-get install chrony
<!--NeedCopy-->
```

Bearbeiten Sie als Root-Benutzer die Datei **/etc/chrony/chrony.conf** und fügen Sie pro Remote-Zeitserver einen Servereintrag hinzu:

```
server peer1-fqdn-or-ip-address iburst
server peer2-fqdn-or-ip-address iburst
```

In einer typischen Bereitstellung synchronisieren Sie die Zeit von den lokalen Domänencontrollern und nicht direkt von öffentlichen NTP-Poolservern. Fügen Sie pro Active Directory-Domänencontroller in der Domäne einen Servereintrag hinzu.

Entfernen Sie alle **server**- oder **pool**-Einträge, einschließlich Einträge für Loopback-IP-Adressen, Localhost und öffentliche Servereinträge wie ***.pool.ntp.org**.

Speichern Sie die Änderungen und starten Sie den Chrony-Daemon neu:

```
sudo systemctl restart chrony
<!--NeedCopy-->
```

Schritt 1g: Installieren von Paketen

```
sudo apt-get install -y libsasl2-2

sudo apt-get install -y libgtk2.0-0
<!--NeedCopy-->
```

Schritt 1h: Hinzufügen von Repositorys zur Installation notwendiger Abhängigkeiten

Für Debian 11.3 fügen Sie die Zeile `deb http://deb.debian.org/debian/ bullseye main` zur Datei /etc/apt/sources.list hinzu.

Schritt 1i: Installieren und Angeben einer zu verwendenden Datenbank

Sie können die Verwendung von SQLite oder PostgreSQL angeben, indem Sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Bei manuellen Installationen müssen Sie SQLite und PostgreSQL manuell installieren, um diese angeben zu können.

In diesem Abschnitt wird beschrieben, wie Sie die PostgreSQL- und SQLite-Datenbanken installieren und wie Sie eine zu verwendende Datenbank angeben.

> **Hinweis:**
>
> Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.

PostgreSQL installieren Führen Sie zum Installieren von PostgreSQL die folgenden Befehle aus:

```
sudo apt-get update

sudo apt-get install -y postgresql

sudo apt-get install -y libpostgresql-jdbc-java
<!--NeedCopy-->
```

Führen Sie die folgenden Befehle aus, um PostgreSQL beim Start der Maschine bzw. sofort zu starten:

```
sudo systemctl enable postgresql

sudo systemctl start postgresql
<!--NeedCopy-->
```

SQLite installieren Führen Sie für Debian den folgenden Befehl aus, um SQLite zu installieren:

```
sudo apt-get install -y sqlite3
<!--NeedCopy-->
```

Datenbank eingeben **Nach der Installation des Linux VDA-Pakets** können Sie durch Bearbeiten von **/etc/xdl/db.conf** eine Datenbank angeben, die verwendet werden soll. Führen Sie hierzu die folgenden Schritte aus:

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Lassen Sie diesen Schritt aus, wenn es sich um eine Neuinstallation handelt.
2. Bearbeiten Sie **/etc/xdl/db.conf**, um eine zu verwendende Datenbank anzugeben.
3. Führen Sie **ctxsetup.sh** aus.

> **Hinweis:**
>
> Sie können auch **/etc/xdl/db.conf** verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

Schritt 2: Vorbereiten des Hypervisors

Wenn Sie den Linux VDA als VM auf einem unterstützten Hypervisor ausführen, sind einige Änderungen erforderlich. Nehmen Sie basierend auf der verwendeten Hypervisorplattform die folgenden Änderungen vor. Wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen, sind keine Änderungen erforderlich.

Festlegen der Zeitsynchronisierung auf Citrix Hypervisor

Wenn das Zeitsynchronisierungsfeature auf Citrix Hypervisor aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme mit NTP und Citrix Hypervisor auf. Beide versuchen, die Systemuhr zu verwalten. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Wenn ein paravirtualisierter Linux-Kernel mit installierten Citrix VM Tools ausgeführt wird, können Sie direkt in der Linux-VM prüfen, ob das Citrix Hypervisor-Zeitsynchronisierungsfeature vorhanden und aktiviert ist:

```
su -
cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Dieser Befehl gibt 0 oder 1 zurück:

- 0: Das Zeitsynchronisierungsfeature ist aktiviert und muss deaktiviert werden.
- 1: Das Zeitsynchronisierungsfeature ist deaktiviert und keine weitere Aktion ist erforderlich.

Wenn die Datei /proc/sys/xen/independent_wallclock nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

Deaktivieren Sie gegebenenfalls das Zeitsynchronisierungsfeature, indem Sie 1 in die Datei schreiben:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Damit die Änderung permanent wird und nach dem Neustart erhalten bleibt, fügen Sie in der Datei **/etc/sysctl.conf** die folgende Zeile hinzu:


```
xen.independent_wallclock = 1
```

Starten Sie das System neu, um die Änderungen zu überprüfen:

```
su -
cat /proc/sys/xen/independent_wallclock
<!--NeedCopy-->
```

Dieser Befehl gibt den Wert 1 zurück.

Festlegen der Zeitsynchronisierung auf Microsoft Hyper-V

Linux-VMs, auf denen Hyper-V Linux-Integrationsdienste installiert sind, können mit dem Hyper-V-Zeitsynchronisierungsfeature die Systemzeit des Hostbetriebssystems verwenden. Aktivieren Sie das Feature zusätzlich zu den NTP-Diensten, um sicherzustellen, dass die Betriebssystemzeit korrekt ist.

Auf dem verwaltenden Betriebssystem:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Wählen Sie für die Einstellungen einer Linux-VM **Integration Services** aus.
3. Stellen Sie sicher, dass **Time synchronization** ausgewählt ist.

> **Hinweis:**
>
> Diese Methode unterscheidet sich von VMware und Citrix Hypervisor, wo die Hostzeitsynchronisierung deaktiviert ist, um Konflikte mit dem NTP zu vermeiden. Hyper-V-Zeitsynchronisierung kann gleichzeitig mit der NTP-Zeitsynchronisierung bestehen und sie ergänzen.

Festlegen der Zeitsynchronisierung auf ESX und ESXi

Wenn das VMware-Zeitsynchronisierungsfeature aktiviert ist, treten auf den paravirtualisierten Linux-VMs Probleme mit NTP und Hypervisor auf. Beide versuchen, die Systemuhr zu synchronisieren. Damit es nicht zu Zeitabweichungen zwischen der Uhr und den anderen Servern kommt, muss die Systemuhr aller Linux-Gäste mit dem NTP synchronisiert werden. In diesem Fall muss die Hostzeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel ausführen und VMware-Tools installiert sind:

1. Öffnen Sie den vSphere-Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Virtual Machine Properties** die Registerkarte **Options**.
4. Wählen Sie **VMware Tools**.
5. Deaktivieren Sie im Feld **Advanced** das Kontrollkästchen **Synchronize guest time with host**.

Schritt 3: Linux-VM zur Windows-Domäne hinzufügen

Mit den folgenden Methoden können Linux-Maschinen zur Active Directory-Domäne (AD) hinzugefügt werden:

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Folgen Sie den Anweisungen für die von Ihnen gewählte Methode.

> **Hinweis:**
>
> Der Sitzungsstart kann fehlschlagen, wenn für das lokale Konto auf dem Linux VDA und das AD-Konto derselbe Benutzername verwendet wird.

Samba Winbind

Installieren oder aktualisieren Sie die erforderlichen Pakete

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
<!--NeedCopy-->
```

Starten des Winbind-Daemon beim Systemstart Der Winbind-Daemon muss beim Systemstart gestartet werden:

```
sudo systemctl enable winbind
<!--NeedCopy-->
```

> **Hinweis:**
>
> Stellen Sie sicher, dass das `winbind`-Skript unter `/etc/init.d` ist.

Kerberos konfigurieren Öffnen Sie als Root-Benutzer **/etc/krb5.conf** und nehmen Sie folgende Einstellungen vor:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
[libdefaults]

default_realm = REALM
```



```
dns_lookup_kdc = false

[realms]

REALM = {

admin_server = domain-controller-fqdn

kdc = domain-controller-fqdn

}

[domain_realm]

domain-dns-name = REALM

.domain-dns-name = REALM
```

Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. **example.com**. **REALM** ist der Kerberos-Bereichsname in Großbuchstaben, z. B. **EXAMPLE.COM**.

Konfigurieren der Winbind-Authentifizierung Führen Sie den Befehl **vim /etc/samba/smb.conf** aus, um **/etc/samba/smb.conf** zu öffnen, und nehmen Sie dann die folgenden Einstellungen vor:

```
[global]

workgroup = WORKGROUP

security = ADS

realm = REALM

encrypt passwords = yes

idmap config *:range = 16777216-33554431

kerberos method = secrets and keytab

winbind refresh tickets = yes

template shell = /bin/bash
```

WORKGROUP ist das erste Feld in **REALM** und **REALM** ist der Kerberos-Bereichsname in Großbuchstaben.

Konfigurieren von nsswitch Öffnen Sie **/etc/nsswitch.conf** und fügen Sie `winbind` in den folgenden Zeilen hinzu:

```
passwd: files systemd winbind
group: files systemd winbind
```


Windows-Domäne beitreten Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo net ads join <Kerberos realm name in uppercase> -U <domain user
    with permission to add computers to the domain>
<!--NeedCopy-->
```

Neustarten von Winbind

```
sudo systemctl restart winbind
<!--NeedCopy-->
```

PAM für Winbind konfigurieren Führen Sie den folgenden Befehl aus. Stellen Sie sicher, dass die Optionen **Winbind NT/Active Directory authentication** und **Create home directory on login** aktiviert sind:

```
sudo pam-auth-update
<!--NeedCopy-->
```

> **Tipp:**
>
> Der **winbind**-Daemon wird nur weiterhin ausgeführt, wenn die Maschine zu einer Domäne gehört.

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen, Windows und Linux, ein Computerobjekt in `Active Directory` haben.

Führen Sie den **Samba**-Befehl **net ads** aus, um zu prüfen, ob die Maschine zu einer Domäne gehört:

```
sudo net ads testjoin
<!--NeedCopy-->
```

Führen Sie den folgenden Befehl aus, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen:

```
sudo net ads info
<!--NeedCopy-->
```

Kerberos-Konfiguration überprüfen Überprüfen Sie, ob Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, indem Sie sicherstellen, dass die Systemdatei **keytab** erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
<!--NeedCopy-->
```


Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl **kinit** aus, um die Maschine mit dem Domänencontroller zu authentifizieren, die diese Schlüssel verwendet:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

```
sudo klist
<!--NeedCopy-->
```

Überprüfen Sie die Maschinenkontodetails mit folgendem Befehl:

```
sudo net ads status
<!--NeedCopy-->
```

Benutzerauthentifizierung überprüfen Überprüfen Sie mit dem **wbinfo**-Tool, dass Domänenbenutzer sich bei der Domäne authentifizieren können:

```
wbinfo --krb5auth=domain\username%password
<!--NeedCopy-->
```

Die hier angegebene Domäne ist der AD-Domänenname und nicht der Kerberos-Bereichsname. Für die Bash-Shell muss der umgekehrte Schrägstrich (\) durch einen weiteren umgekehrten Schrägstrich geschützt werden. Bei diesem Befehl wird eine Erfolgs- oder Fehlermeldung zurückgegeben.

Um sich zu vergewissern, dass das Winbind-PAM-Modul fehlerfrei konfiguriert ist, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
ssh localhost -l domain\username

id -u
<!--NeedCopy-->
```

> **Hinweis:**

> Um einen SSH-Befehl erfolgreich auszuführen, stellen Sie sicher, dass SSH aktiviert ist und ordnungsgemäß funktioniert.

Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache gültig und nicht abgelaufen sind:

```
klist
<!--NeedCopy-->
```

Beenden Sie die Sitzung.

```
exit
<!--NeedCopy-->
```

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

> **Tipp:**
>
> Wenn die Benutzerauthentifizierung erfolgreich ist, aber der Desktop nach der Anmeldung mit einem Domänenkonto nicht angezeigt wird, starten Sie die Maschine neu und wiederholen Sie die Anmeldung.

Centrify DirectControl

Windows-Domäne beitreten Wenn der Centrify DirectControl Agent installiert ist, machen Sie die Linux-Maschine mit dem Centrify-Befehl `adjoin` zu einem Mitglied der Active Directory-Domäne:

```
su -
adjoin -w -V -u user domain-name
<!--NeedCopy-->
```

Der Parameter **user** ist ein Active Directory-Domänenbenutzer mit der Berechtigung, Computer zu Mitgliedern von Active Directory-Domänen zu machen. Der Parameter **domain-name** ist der Name der Domäne, der die Linux-Maschine beitritt.

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux) ein Computerobjekt in Active Directory haben. Mit folgendem Befehl prüfen Sie, ob eine per Centrify hinzugefügte Linux-Maschine Mitglied der Domäne ist:


```
su -

adinfo
<!--NeedCopy-->
```

Stellen Sie sicher, dass der Wert **Joined to domain** gültig ist und dass **CentrifyDC mode** den Wert **connected** zurückgibt. Wenn der Modus im Startzustand stecken bleibt, hat der Centrify-Client Serververbindungs- oder Authentifizierungsprobleme.

Umfassendere System- und Diagnoseinformationen sind mit folgenden Befehlen verfügbar:

```
adinfo --sysinfo all

adinfo --diag
<!--NeedCopy-->
```

Testen Sie die Verbindung mit den verschiedenen Active Directory- und Kerberos-Diensten.

```
adinfo --test
<!--NeedCopy-->
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

SSSD

Kerberos konfigurieren Führen Sie zum Installieren von Kerberos den folgenden Befehl aus:

```
sudo apt-get install krb5-user
<!--NeedCopy-->
```

Zum Konfigurieren von Kerberos öffnen Sie als Root-Benutzer **/etc/krb5.conf** und legen Sie folgende Parameter fest:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Modell mit einer Domäne und einer Gesamtstruktur vorgesehen.

```
[libdefaults]

default_realm = REALM

dns_lookup_kdc = false

rdns = false

[realms]

REALM = {
```



```
admin_server = domain-controller-fqdn
kdc = domain-controller-fqdn
}
[domain_realm]
domain-dns-name = REALM
.domain-dns-name = REALM
```

Der Parameter `domain-dns-name` ist in diesem Kontext der DNS-Domänenname, z. B. example.com. *REALM* ist der Kerberos-Bereichsname in Großbuchstaben, z. B. EXAMPLE.COM.

Domäne beitreten SSSD muss für die Verwendung von Active Directory als Identitätsanbieter und Kerberos zur Authentifizierung konfiguriert werden. SSSD bietet keine AD-Clientfunktionen für den Domänenbeitritt und die Verwaltung der Systemschlüsseltabelle. Sie können stattdessen **adcli**, **realmd** oder **Samba** verwenden.

> **Hinweis:**
>
> Dieser Abschnitt enthält nur Informationen für **adcli** und **Samba**.

- **Wenn Sie der Domäne mit adcli beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie **adcli**.

   ```
   sudo apt-get install adcli
   <!--NeedCopy-->
   ```

2. Treten Sie mit **adcli** der Domäne bei.

   Entfernen Sie die alte Systemdatei für die Schlüsseltabelle und treten Sie der Domäne mit folgenden Befehl bei:

   ```
   su -

   rm -rf /etc/krb5.keytab

   adcli join domain-dns-name -U user -H hostname-fqdn
   <!--NeedCopy-->
   ```

   user ist ein Domänenbenutzer mit der Berechtigung zum Hinzufügen von Maschinen zur Domäne. **hostname-fqdn** ist der Hostname für die Maschine im FQDN-Format.

   Die Option **-H** ist erforderlich, damit **adcli** SPN im folgenden, vom Linux VDA benötigten Format erstellen kann: host/hostname-fqdn@REALM.

3. Überprüfen Sie die Systemschlüsseltabelle.

Führen Sie den Befehl `sudo klist -ket` aus, um sicherzustellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde.

Prüfen Sie, ob die Zeitstempel der einzelnen Schlüssel mit der Zeit übereinstimmen, zu der der Domänenbeitritt der Maschine erfolgte.

- **Wenn Sie der Domäne mit Samba beitreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.

```
sudo apt-get install samba krb5-user
<!--NeedCopy-->
```

2. Konfigurieren Sie **Samba**.

   Öffnen Sie **/etc/samba/smb.conf** und nehmen Sie folgende Einstellungen vor:

   ```
   [global]
   workgroup = WORKGROUP
   security = ADS
   realm = REALM
   client signing = yes
   client use spnego = yes
   kerberos method = secrets and keytab
   ```

   WORKGROUP ist das erste Feld in *REALM* und *REALM* ist der Kerberos-Bereichsname in Großbuchstaben.

3. Treten Sie der Domäne mit **Samba** bei.

   Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Windows-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen.

```
sudo net ads join <the Kerberos realm name in uppercase> -U <
    domain user with permission to add computers to the domain>
<!--NeedCopy-->
```

SSSD einrichten **Installieren oder aktualisieren Sie die erforderlichen Pakete:**

Installieren Sie ggf. die erforderlichen SSSD- und Konfigurationspakete:

```
sudo apt-get install sssd
<!--NeedCopy-->
```

Wenn die Pakete bereits installiert sind, wird die Aktualisierung empfohlen:


```
sudo apt-get install --only-upgrade sssd
<!--NeedCopy-->
```

SSSD konfigurieren Vor dem Start des SSSD-Daemon sind SSSD-Konfigurationsänderungen erforderlich. Für einige Versionen von SSSD ist die Konfigurationsdatei **/etc/sssd/sssd.conf** nicht standardmäßig installiert und muss manuell erstellt werden. Öffnen oder erstellen Sie als Root-Benutzer **/etc/sssd/sssd.conf** und nehmen Sie folgende Einstellungen vor:

```
[sssd]

services = nss, pam

config_file_version = 2

domains = domain-dns-name

[domain/domain-dns-name]

id_provider = ad

access_provider = ad

auth_provider = krb5

krb5_realm = REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer
than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is
shorter than 2 hours

krb5_renew_interval = 1h

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U

# This ldap_id_mapping setting is also the default value

ldap_id_mapping = true

override_homedir = /home/%d/%u

default_shell = /bin/bash

ad_gpo_map_remote_interactive = +ctxhdx
```


> **Hinweis:**
>
> ldap_id_mapping ist auf **true** festgelegt, sodass SSSD die Zuordnung von Windows SIDs zu Unix UIDs selbst vornimmt. Andernfalls muss `Active Directory` POSIX-Erweiterungen bereitstellen können. Der PAM-Dienst `ctxhdx` wird ad_gpo_map_remote_interactive hinzugefügt.
>
> Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. example.com. *REALM* ist der Kerberos-Bereichsname in Großbuchstaben, z. B. EXAMPLE.COM. Die Konfiguration des NetBIOS-Domänennamens ist nicht erforderlich.
>
> Weitere Informationen zu den Konfigurationseinstellungen finden Sie auf den Manpages über sssd.conf und `sssd-ad`.

Für den SSSD-Daemon muss die Konfigurationsdatei Besitzer-Leseberechtigung haben:

```
sudo chmod 0600 /etc/sssd/sssd.conf
<!--NeedCopy-->
```

SSSD-Daemon starten Führen Sie die folgenden Befehle aus, um den SSSD-Daemon zu starten und den Daemon beim Systemstart der Maschine zu aktivieren:

```
sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```

PAM-Konfiguration Führen Sie den folgenden Befehl aus. Stellen Sie sicher, dass die Optionen **SSS authentication** und **Create home directory on login** aktiviert sind:

```
sudo pam-auth-update
<!--NeedCopy-->
```

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux VDAs) ein Computerobjekt in `Active Directory` haben.

- Wenn Sie die Domänenmitgliedschaft mit **adcli** überprüfen, führen Sie den Befehl `sudo adcli info domain-dns-name` aus, um die Domäneninformationen anzuzeigen.
- Wenn Sie die Domänenmitgliedschaft mit **Samba** überprüfen, führen Sie den Befehl `sudo net ads testjoin` aus, um zu überprüfen, ob die Maschine Mitglied einer Domäne ist, und den Befehl `sudo net ads info` zum Überprüfen zusätzlicher Domänen- und Computerobjektinformationen.

Kerberos-Konfiguration überprüfen Überprüfen Sie, ob Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, indem Sie sicherstellen, dass die Systemdatei für die Schlüsseltabelle erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
<!--NeedCopy-->
```

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um die Maschine mit dem Domänencontroller mit diesen Schlüsseln zu authentifizieren:

```
sudo kinit -k MACHINE$@REALM
<!--NeedCopy-->
```

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT für das Maschinenkonto zwischengespeichert wurde:

```
sudo klist
<!--NeedCopy-->
```

Benutzerauthentifizierung überprüfen SSSD bietet kein Befehlszeilentool zum direkten Testen der Authentifizierung mit dem Daemon, daher kann der Test nur mit PAM ausgeführt werden.

Um sich zu vergewissern, dass das SSSD-PAM-Modul fehlerfrei konfiguriert wurde, melden Sie sich mit einem bislang noch nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
ssh localhost -l domain\username

id -u

klist

exit
<!--NeedCopy-->
```

Stellen Sie sicher, dass die vom Befehl **klist** zurückgegebenen Kerberos-Tickets für den Benutzer richtig und nicht abgelaufen sind.

Überprüfen Sie als Root-Benutzer, dass eine entsprechende Ticketcachedatei für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:


```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Ein ähnlicher Test kann ausgeführt werden, wenn Sie sich direkt am KDE- oder Gnome-Anzeigemanager anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

Download des erforderlichen PBIS-Pakets

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download
    /9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Umwandeln des PBIS-Installationsskripts in eine ausführbare Datei

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Ausführen des PBIS-Installationsskripts

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
<!--NeedCopy-->
```

Windows-Domäne beitreten Es wird vorausgesetzt, dass der Domänencontroller erreichbar ist und dass Sie über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
<!--NeedCopy-->
```

user ist ein Domänenbenutzer mit der Berechtigung, Computer zur Active Directory-Domäne hinzuzufügen. **domain-name** ist der DNS-Name der Domäne, z. B. example.com.

Hinweis: Führen Sie den Befehl **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** aus, um Bash als Standardshell festzulegen.

Domäneneigentümerschaft überprüfen Für den Delivery Controller ist es erforderlich, dass alle VDA-Maschinen (Windows und Linux VDAs) ein Computerobjekt in `Active Directory` haben. Mit folgendem Befehl prüfen Sie, ob eine per PBIS angemeldete Linux-Maschine zur Domäne gehört:

```
/opt/pbis/bin/domainjoin-cli query
<!--NeedCopy-->
```


Wenn die Maschine einer Domäne beigetreten ist, werden mit diesem Befehl Informationen zur aktuell beigetretenen AD-Domäne und Organisationseinheit abgefragt. Andernfalls wird nur der Hostname angezeigt.

Benutzerauthentifizierung überprüfen Um sicherzustellen, dass PBIS Domänenbenutzer mit PAM authentifizieren kann, melden Sie sich mit einem bislang nicht verwendeten Domänenbenutzerkonto am Linux VDA an.

```
sudo ssh localhost -l domain\user

id -u
<!--NeedCopy-->
```

Vergewissern Sie sich, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **id -u** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_uid
<!--NeedCopy-->
```

Beenden Sie die Sitzung.

```
exit
<!--NeedCopy-->
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Schritt 4: .NET Runtime 6.0 installieren

Installieren Sie .NET Runtime 6.0 vor der Installation von Linux VDA gemäß den Anweisungen unter https://docs.microsoft.com/en-us/dotnet/core/install/linux-package-managers.

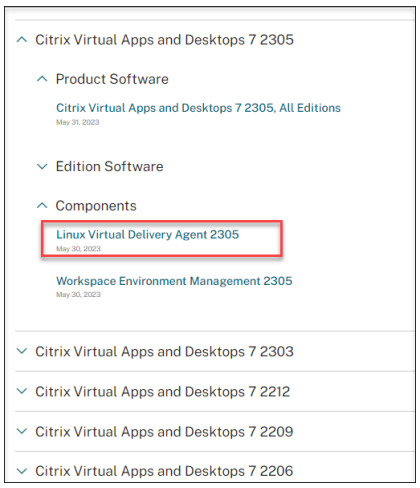
Führen Sie nach der Installation von .NET Runtime 6.0 den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

Legen Sie basierend auf der Ausgabe des Befehls den Binärpfad für die .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet ist, verwenden Sie /aa/bb als .NET-Binärpfad.

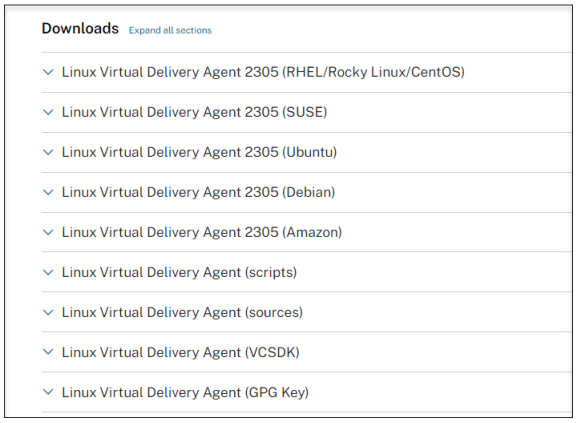
Schritt 5: Herunterladen des Linux VDA-Pakets

1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
2. Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.

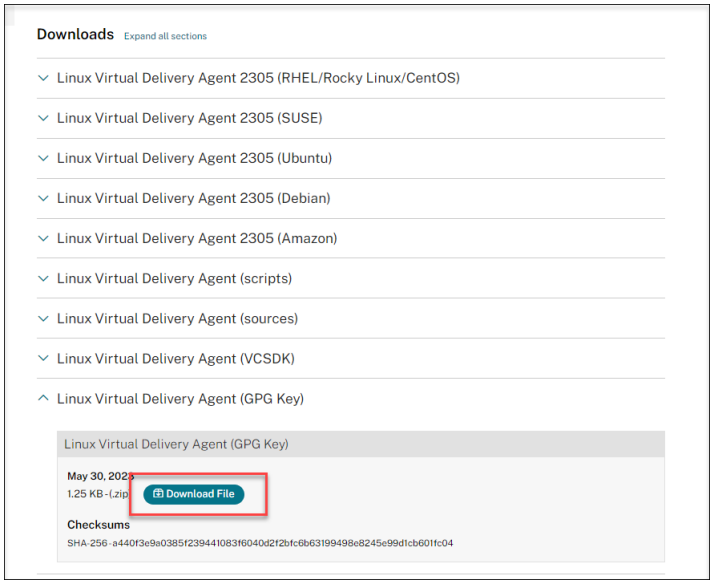
3. Erweitern Sie **Komponenten**, um den Linux VDA zu finden. Beispiel:



4. Klicken Sie auf den Linux VDA-Link, um auf die Linux VDA-Downloads zuzugreifen.



5. Laden Sie das Linux VDA-Paket herunter, das Ihrer Linux-Distribution entspricht.
6. Laden Sie den öffentlichen GPG-Schlüssel herunter, mit dem Sie die Integrität des Linux VDA-Pakets überprüfen können. Beispiel:



Um die Integrität des Linux VDA-Pakets zu überprüfen, führen Sie die folgenden Befehle aus, um den öffentlichen Schlüssel in die DEB-Datenbank zu importieren und die Überprüfung durchzuführen:

```
sudo apt-get install dpkg-sig
gpg --import <path to the public key>
dpkg-sig --verify <path to the Linux VDA package>
<!--NeedCopy-->
```

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
<!--NeedCopy-->
```

Abhängigkeitsliste für Debian 11.3:

```
openjdk-11-jdk >= 11

imagemagick >= 8:6.9.10

ufw >= 0.36

desktop-base >= 10.0.2

libxrandr2 >= 2:1.5.1

libxtst6 >= 2:1.2.3
```



```
libxm4 >= 2.3.8

util-linux >= 2.33

gtk3-nocsd >= 3

bash >= 5.0

findutils >= 4.6.0

sed >= 4.7

cups >= 2.2

ghostscript >= 9.53~

libmspack0 >= 0.10

ibus >= 1.5

libgoogle-perftools4 >= 2.7~

libpython3.9 >= 3.9~

libsasl2-modules-gssapi-mit >= 2.1.~

libqt5widgets5 >= 5.5~

mutter >= 3.38.6~

libqrencode4 >= 4.0.0

libimlib2 >= 1.5.1
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine Übersicht der Linux-Distributionen und Xorg-Versionen, die von dieser Version des Linux VDA unterstützt werden, finden Sie in der Tabelle Systemanforderungen.

Schritt 6b: Upgrade des Linux VDA (optional)

Sie können ein Upgrade für ein vorhandene Installation der vorherigen beiden Versionen und von einer LTSR-Version durchführen.

```
sudo dpkg -i <PATH>/<Linux VDA deb>
<!--NeedCopy-->
```


> **Hinweis:**
>
> Durch das Upgrade einer Installation werden die Konfigurationsdateien unter /etc/xdl. überschrieben. Sichern Sie die Dateien vor jedem Upgrade.

Schritt 7: Installieren von NVIDIA GRID-Treibern

Zum Aktivieren von HDX 3D Pro müssen Sie die NVIDIA GRID-Treiber auf Ihrem Hypervisor und auf den VDA-Maschinen installieren.

Informationen zum Installieren und Konfigurieren des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Handbüchern:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Zum Installieren und Konfigurieren der NVIDIA GRID-Gast-VM-Treiber führen Sie die folgenden allgemeinen Schritte aus:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM in der Hypervisor-Systemsteuerung eine GPU zu.
3. Starten Sie die VM.
4. Installieren Sie den Gast-VM-Treiber auf der VM.

Schritt 8: Konfigurieren des Linux VDA

> **Hinweis:**
>
> Stellen Sie vor dem Einrichten der Laufzeitumgebung sicher, dass das Gebietsschema **en_US.UTF-8** in Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema im Betriebssystem nicht verfügbar ist, führen Sie den Befehl **sudo locale-gen en_US.UTF-8** aus. Für Debian bearbeiten Sie die Datei **/etc/locale.gen** durch Auskommentierung der Zeile **# en_US.UTF-8 UTF-8**. Führen Sie dann den Befehl **sudo locale-gen** aus.

Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Das Skript überprüft die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Führen Sie Änderungen erst danach durch. Sie können das Skript nach Bedarf jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell unter Reaktion auf Aufforderungen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript durch, bevor Sie fortfahren:


```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
<!--NeedCopy-->
```

Konfiguration mit Aufforderungen

Führen Sie eine manuelle Konfiguration mit Aufforderungen aus:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
<!--NeedCopy-->
```

Automatische Konfiguration

Bei einer automatischen Installation können die für das Setupskript erforderlichen Optionen mit Umgebungsvariablen angegeben werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript keine weiteren Informationen vom Benutzer und der Installationsvorgang wird per Skript ausgeführt.

Unterstützte Umgebungsvariablen umfassen u. a.:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y | N** –Der Linux VDA unterstützt die Angabe des Namens eines Delivery Controllers mit einem DNS CNAME-Datensatz. Die Standardeinstellung ist N.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'**–Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste vollqualifizierter Domänennamen (FQDNs) für die Registrierung bei einem Delivery Controller. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** –Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port. Dies ist standardmäßig Port 80.
- **CTX_XDL_REGISTER_SERVICE=Y | N** –Die Linux VDA-Dienste werden nach dem Systemstart gestartet. Die Standardeinstellung ist Y.
- **CTX_XDL_ADD_FIREWALL_RULES=Y | N** –Für die Linux VDA-Dienste muss die Systemfirewall eingehende Netzwerkverbindungen zulassen. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) in der Systemfirewall automatisch für den Linux VDA öffnen. Die Standardeinstellung ist Y.
- **CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis** –Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen für die Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird durch das auf dem System installierte und konfigurierte Active Directory-Integrationstool bestimmt.

- **CTX_XDL_HDX_3D_PRO=Y | N** – Der Linux VDA unterstützt HDX 3D Pro – GPU-Beschleunigungstechnologien zum Optimieren der Virtualisierung reichhaltiger Grafikanwendungen. Bei aktiviertem HDX 3D Pro wird der VDA für VDI-Desktopmodus (Einzelsitzungen) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y | N** – Ermöglicht die Konfiguration der Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes, freigegebenes Desktopbereitstellungsmodell. Legen Sie dies bei Umgebungen mit HDX 3D Pro auf "Y"fest. Standardmäßig ist diese Variable auf N festgelegt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Geben Sie einen DNS-Sitenamen an, wenn Sie die Suchergebnisse auf eine lokale Site beschränken möchten. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS zur Erkennung von LDAP-Servern ab. Falls DNS keine LDAP-Diensteinträge bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste der FQDNs mit LDAP-Port angeben. Beispiel: ad1.mycompany.com:389 ad2.mycompany.com:3268 ad3.mycompany.com:3268 oder ad1.mycompany.com:636 ad2.mycompany.com:3269 ad3.mycompany.com:3269, wenn Sie LDAPS verwenden. Für schnellere LDAP-Abfragen in einer Active Directory-Gesamtstruktur aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben als LDAP-Portnummer 3268 bzw., sofern Sie LDAPS verwenden, 3269 an. Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Die Suchbasis bei LDAP-Abfragen des Linux VDA ist das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com). Zur Verbesserung der Suchleistung können Sie eine Suchbasis angeben (z. B. OU=VDI, DC=mycompany,DC=com). Die Standardeinstellung für diese Variable ist **<none>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Server für den Verbundauthentifizierungsdienst (FAS) werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, Sie können jedoch stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern angeben. Die Reihenfolge muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen. Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und ändern nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit den FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen Portnummer übereinstimmt, z. B. CTX_XDL_FAS_LIST='fas_server_1_url:port_number; fas_server_2_url: port_number; fas_server_3_url: port_number'.
- **CTX_XDL_DOTNET_ RUNTIME_PATH=path-to-install-dotnet-runtime** – Der Pfad für die Installation von .NET Runtime 6.0 zur Unterstützung des neuen Brokeragentdiensts (`ctxvda`). Der Standardpfad ist /usr/bin.

- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate**: Legt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung zur Verwendung in Sitzungen fest. Wenn Sie die Variable nicht spezifizieren, wird der aktuell auf dem VDA installierte Desktop verwendet. Ist der aktuell installierte Desktop MATE, müssen Sie allerdings die Variable auf **mate** festlegen.

  Sie können die Desktopumgebung für Sitzungsbenutzer auch über die folgenden Schritte ändern:

  1. Erstellen Sie die Datei `.xsession` auf dem VDA im Verzeichnis **$HOME/<username>**.
  2. Geben Sie in der Datei `.xsession` eine auf Distributionen basierende Desktopumgebung an.

     - **Für MATE-Desktop**

     ```
     MSESSION="$(type -p mate-session)"
     if [ -n "$MSESSION" ]; then
       exec mate-session
     fi
     ```

     - **Für GNOME Classic-Desktop**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     export GNOME_SHELL_SESSION_MODE=classic
     exec gnome-session --session=gnome-classic
     fi
     ```

     - **Für GNOME-Desktop**

     ```
     GSESSION="$(type -p gnome-session)"
     if [ -n "$GSESSION" ]; then
     exec gnome-session
     fi
     ```

  3. Teilen Sie die 700-Dateiberechtigung mit dem Zielsitzungsbenutzer.

  Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebung anpassen. Um dieses Feature zu aktivieren, müssen Sie umschaltbare Desktopumgebungen vorher auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen nach Sitzungsbenutzern.

- **CTX_XDL_START_SERVICE=Y | N** –Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Die Standardeinstellung ist Y.
- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
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=winbind | quest |centrify | sssd | pbis

export CTX_XDL_HDX_3D_PRO=Y|N

export CTX_XDL_VDI_MODE=Y|N

export CTX_XDL_SITE_NAME=dns-site-name | '<none>'

export CTX_XDL_LDAP_LIST='list-ldap-servers' | '<none>'

export CTX_XDL_SEARCH_BASE=search-base-set | '<none>'

export CTX_XDL_FAS_LIST='list-fas-servers' | '<none>'

export CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime

export CTX_XDL_DESKTOP_ENVIRONMENT= gnome | gnome-classic | mate | '<
    none>'

export CTX_XDL_TELEMETRY_SOCKET_PORT=port-number

export CTX_XDL_TELEMETRY_PORT=port-number

export CTX_XDL_START_SERVICE=Y|N

sudo -E /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
<!--NeedCopy-->
```

Sie müssen die Option **-E** mit dem Befehl “sudo”angeben, damit die vorhandenen Umgebungsvariablen an die neu erstellte Shell weitergegeben werden. Wir empfehlen, dass Sie mit den oben aufgeführten Befehlen eine Shellskriptdatei erstellen, deren erste Zeile **#!/bin/bash** enthält.

Alternativ können Sie alle Parameter mit einem einzigen Befehl festlegen:

```
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 \
```



```
8
9  CTX_XDL_ADD_FIREWALL_RULES=Y|N \
10
11 CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \
12
13 CTX_XDL_HDX_3D_PRO=Y|N \
14
15 CTX_XDL_VDI_MODE=Y|N \
16
17 CTX_XDL_SITE_NAME=dns-name \
18
19 CTX_XDL_LDAP_LIST='list-ldap-servers' \
20
21 CTX_XDL_SEARCH_BASE=search-base-set \
22
23 CTX_XDL_FAS_LIST='list-fas-servers' \
24
25 CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \
26
27 CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \
28
29 CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
30
31 CTX_XDL_TELEMETRY_PORT=port-number \
32
33 CTX_XDL_START_SERVICE=Y|N \
34
35 /opt/Citrix/VDA/sbin/ctxsetup.sh --silent
36 <!--NeedCopy-->
```

Entfernen von Konfigurationsänderungen

In einigen Fällen müssen die vom Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernt werden, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript durch, bevor Sie fortfahren:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
2 <!--NeedCopy-->
```

Entfernen von Konfigurationsänderungen:

```
1 sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
2 <!--NeedCopy-->
```

> **Wichtig:**
>
> Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank, sodass der Linux VDA nicht funktionsfähig ist.

Konfigurationsprotokolle

Die Skripts **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an und schreiben weitere Informationen in die Konfigurationsprotokolldatei **/tmp/xdl.configure.log**.

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

Deinstallieren der Linux VDA-Software

Überprüfen, ob der Linux VDA installiert ist, und Anzeigen der Version des installierten Pakets:

```
dpkg -l xendesktopvda
<!--NeedCopy-->
```

Anzeigen weiterer Details:

```
apt-cache show xendesktopvda
<!--NeedCopy-->
```

Deinstallieren der Linux VDA-Software:

```
dpkg -r xendesktopvda
<!--NeedCopy-->
```

> **Hinweis:**
>
> Beim Deinstallieren der Linux VDA-Software werden die damit verknüpften PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden nicht gelöscht.
>
> **Tipp:**
>
> Die Informationen in diesem Abschnitt beziehen sich nicht auf das Entfernen von abhängigen Paketen einschließlich PostgreSQL.

Schritt 9: Ausführen von XDPing

Mit `sudo /opt/Citrix/VDA/bin/xdping` können Sie Linux VDA-Umgebungen auf häufige Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 10: Ausführen des Linux VDA

Wenn Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, können Sie den Linux VDA mit den folgenden Befehlen steuern.

Starten Sie den Linux VDA:

Starten der Linux VDA-Dienste:

```
sudo systemctl start ctxhdx

sudo systemctl start ctxvda
<!--NeedCopy-->
```

Halten Sie den Linux VDA an:

Anhalten der Linux VDA-Dienste:

```
sudo systemctl stop ctxvda

sudo systemctl stop ctxhdx
<!--NeedCopy-->
```

> **Hinweis:**
>
> Führen Sie erst den Befehl **systemctl stop ctxmonitord** aus, um den Monitor Service Daemon zu stoppen, bevor Sie die Dienste **ctxvda** und **ctxhdx** stoppen. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Starten Sie den Linux VDA neu:

Neustarten der Linux VDA-Dienste:

```
sudo systemctl stop ctxvda

sudo systemctl restart ctxhdx

sudo systemctl restart ctxvda
<!--NeedCopy-->
```

Überprüfen Sie den Linux VDA-Status:

Überprüfen des Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda

sudo systemctl status ctxhdx
<!--NeedCopy-->
```

Schritt 11: Maschinenkataloge erstellen

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt der traditionellen Windows VDA-Methode. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Maschinenkatalogen und Verwalten von Maschinenkatalogen.

Beim Erstellen von Maschinenkatalogen mit Linux VDA-Maschinen gibt es einige Einschränkungen,

durch die sich der Prozess von der Maschinenkatalogerstellung für Windows VDA-Maschinen unterscheidet:

- Auswahl des Betriebssystems:
  - Die Option **Betriebssystem für mehrere Sitzungen** für ein gehostetes, freigegebenes Desktopbereitstellungsmodell.
  - Die Option **Betriebssystem für Einzelsitzungen** für ein VDI-dediziertes Desktopbereitstellungsmodell.
- In einem Maschinenkatalog darf sich keine Mischung aus Linux und Windows VDA-Maschinen befinden.

> **Hinweis:**
>
> In früheren Citrix Studio-Versionen wurde Linux als Betriebssystem nicht unterstützt. Durch die Auswahl von **Windows-Serverbetriebssystem** oder **Serverbetriebssystem** wird jedoch ein äquivalentes gehostetes, freigegebenes Desktopbereitstellungsmodell bereitgestellt. Durch die Auswahl von **Windows-Desktopbetriebssystem** oder **Desktopbetriebssystem** wird ein Bereitstellungsmodell für Einzelbenutzermaschinen bereitgestellt.
>
> **Tipp:**
>
> Wenn Sie eine Maschine aus einer Active Directory-Domäne entfernen und sie ihr dann wieder hinzufügen, muss die Maschine auch aus dem Maschinenkatalog entfernt und ihm dann erneut hinzugefügt werden.

Schritt 12: Bereitstellungsgruppen erstellen

Die Prozesse zum Erstellen einer Bereitstellungsgruppe und zum Hinzufügen von Maschinenkatalogen mit Linux VDA- bzw. Windows VDA-Maschinen sind fast identisch. Umfassendere Informationen zu diesen Prozessen finden Sie unter Erstellen von Bereitstellungsgruppen.

Beim Erstellen von Bereitstellungsgruppen mit Linux VDA-Maschinenkatalogen gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die ausgewählten Active Directory-Benutzer und -Gruppen für die Anmeldung an Linux VDA-Maschinen richtig konfiguriert wurden.
- Lassen Sie nicht die Anmeldung nicht authentifizierter (anonymer) Benutzer zu.
- Die Bereitstellungsgruppe darf keine Maschinenkataloge mit Windows Maschinen enthalten.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2308.

Konfigurieren

January 8, 2024

In diesem Abschnitt werden die Features des Linux VDA, ihre Konfiguration und die Problembehandlung beschrieben.

Verwaltung

February 9, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- CEIP
- HDX Insight
- Integration in den Citrix Telemetriedienst
- Linux VDA-Selbstupdate für Citrix DaaS Standard für Azure
- Metriken für Linux-VMs und Linux-Sitzungen
- Protokollsammlung
- Sitzungsspiegelung
- Monitor Service Daemon
- Tools und Hilfsprogramme
- Sonstige
  - Unterstützung für die Citrix Workspace-App für HTML5
  - Virtuelle **Python3**-Umgebung erstellen
  - Integration von NIS in Active Directory
  - **IPv6**
  - LDAPS
  - **Xauthority**

Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

January 8, 2024

Wenn Sie an dem Programm teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, um die Qualität und Leistung der Citrix Produkte zu verbessern. Außerdem wird eine Kopie der anonymen Daten zur schnellen und effizienten Analyse an Google Analytics (GA) gesendet. GA ist standardmäßig deaktiviert.

Registrierungseinstellungen

Standardmäßig nehmen Sie bei der Installation des Linux VDA automatisch am CEIP teil. Der erste Datenupload erfolgt ca. sieben Tage nach der Installation des Linux VDAs. Sie können die Standardeinstellung über eine Registrierungseinstellung ändern.

- **CEIPSwitch**

Die Registrierungseinstellung, mit der das CEIP aktiviert oder deaktiviert wird (Standardwert = 0):

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: **CEIPSwitch**

Wert: 1 = deaktiviert , 0 = aktiviert

Wenn nicht angegeben, ist CEIP aktiviert.

Sie können auf einem Client den folgenden Befehl ausführen, um das CEIP zu deaktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\CEIP" -v "CEIPSwitch" -d "1"
<!--NeedCopy-->
```

- **GASwitch**

Die Registrierungseinstellung, mit der das GA aktiviert oder deaktiviert wird (Standardwert = 1):

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: **GASwitch**

Wert: 1 = deaktiviert , 0 = aktiviert

Wenn nicht angegeben, ist GA deaktiviert.

Sie können auf einem Client den folgenden Befehl ausführen, um GA zu aktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\CEIP" -v "GASwitch" -d "0"
<!--NeedCopy-->
```


- **DataPersistPath**

Die Registrierungseinstellung zur Steuerung des Datenspeicherpfads (Standard = /var/xdl/ceip):

Speicherort: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP

Name: DataPersistPath

Wert: Zeichenfolge

Legen Sie den Pfad mit folgendem Befehl fest:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     Citrix\CEIP" -v "DataPersistPath" -d "your_path"
2 <!--NeedCopy-->
```

Wenn der konfigurierte Pfad nicht vorhanden ist oder nicht darauf zugegriffen werden kann, werden die Daten im Standardpfad gespeichert.

Vom Linux VDA gesammelte CEIP-Daten

In der folgende Tabelle sehen Sie Beispiele für die Art der anonymen Informationen, die gesammelt werden. Die Daten enthalten keine Informationen, die Sie als Kunden identifizieren.

Datenpunkt	Schlüsselname	Beschreibung
Maschinen-GUID	**machine_guid**	Eine GUID-Zeichenfolge identifiziert die Maschine, von der die Daten stammen
AD-Lösung	**ad_solution**	Eine Zeichenfolge, die für die Domänenbeitrittsmethode der Maschine steht
Linux-Kernelversion	**kernel_version**	Eine Zeichenfolge, die für die Kernelversion der Maschine steht
LVDA-Version	**vda_version**	Eine Zeichenfolge, die für die installierte Version des Linux VDA steht.
LVDA-Update oder Neuinstallation	**update_or_fresh_install**	Eine Zeichenfolge, die für das aktuelle Linux VDA-Paket steht, das installiert oder aktualisiert wird

Datenpunkt	Schlüsselname	Beschreibung
LVDA-Installiermethode	install_method	Eine Textzeichenfolge, die angibt, wie das aktuelle Linux VDA-Paket installiert wurde: MCS, PVS, einfache oder manuelle Installation.
HDX 3D Pro aktiviert oder nicht	**hdx_3d_pro**	Eine Zeichenfolge, die anzeigt, ob HDX 3D Pro auf der Maschine aktiviert ist
VDI-Modus aktiviert oder nicht	**vdi_mode**	Eine Textzeichenfolge, die angibt, ob der VDI-Modus aktiviert ist
Gebietsschema des Systems	**system_locale**	Eine Zeichenfolge, die das Gebietsschema der Maschine angibt
Letzter Neustart der LVDA-Schlüsseldienste	**ctxhdx ctxvda**	Die Zeit des letzten Neustarts der `ctxhdx`- und `ctxvda`-Dienste im Format tt-hh:mm:ss, z. B. 10-17:22:19
GPU-Typ	**gpu_type**	Der GPU-Typ der Maschine.
CPU-Kerne	**cpu_cores**	Eine Ganzzahl, die die Anzahl der CPU-Kerne des Computers angibt
CPU-Frequenz	**cpu_frequency**	Gleitkommazahl, die die CPU-Frequenz in MHz angibt.
Größe des physischen Speichers	**memory_size**	Eine Ganzzahl, die die Größe des physischen Speichers in KB angibt
Anzahl der gestarteten Sitzungen	**session_launch**	Eine Ganzzahl, die die Anzahl der gestarteten Sitzungen (angemeldet oder wieder verbunden) auf der Maschine zum Zeitpunkt der Datenerfassung angibt
Linux-OS-Name und -Version	**os_name_version**	Eine Zeichenfolge, die den Linux-OS-Namen und die Linux-OS-Version der Maschine angibt

Datenpunkt	Schlüsselname	Beschreibung
Sitzungsschlüssel	**session_key**	Identifiziert die Sitzung, aus der die Daten stammen.
Ressourcentyp	**resource_type**	Eine Textzeichenfolge, die den Ressourcentyp der gestarteten Sitzung angibt: Desktop oder <appname>
Aktive Sitzungszeiten	**active_session_time**	Speichert die aktiven Zeiten der Sitzung. Eine Sitzung kann mehrere aktive Zeiten haben, da die Sitzung getrennt und wieder verbunden werden kann
Sitzungsdauer	**session_duration_time**	Speichert die Sitzungsdauer von der Anmeldung bis zur Abmeldung
Receiver-Clienttyp	**receiver_type**	Eine Ganzzahl, die den zum Starten der Sitzung verwendeten Typ der Citrix Workspace-App angibt.
Receiver-Clientversion	**receiver_version**	Textzeichenfolge, die die Version der Citrix Workspace-App angibt, die zum Starten der Sitzung verwendet wurde
Druckzähler	**printing_count**	Eine Ganzzahl, die angibt, wie oft die Druckfunktion in der Sitzung verwendet wurde.
USB-Umleitungszähler	**usb_redirecting_count**	Eine Ganzzahl, die angibt, wie oft ein USB-Gerät in der Sitzung verwendet wurde.
GFX-Anbietertyp	**gfx_provider_type**	Zeichenfolge, die den Grafikanbietertyp der Sitzung angibt
Zahl der Spiegelungen	**shadow_count**	Eine Ganzzahl, die angibt, wie oft eine Sitzung gespiegelt wurde.

Datenpunkt	Schlüsselname	Beschreibung
Vom Benutzer ausgewählte Sprache	**ctxism_select**	Zusammengesetzte lange Zeichenfolge, die alle von den Benutzern ausgewählten Sprachen enthält
Anzahl der Smartcardumleitungen	**scard_redirecting_count**	Eine Ganzzahl, die angibt, wie oft die Smartcardumleitung für Sitzungsanmeldungen und Benutzerauthentifizierung für Apps in der Sitzung verwendet wird

HDX Insight

April 18, 2024

Übersicht

Der Linux VDA unterstützt teilweise das HDX Insight-Feature.

Installation

Keine abhängigen Pakete müssen installiert werden.

Verwendung

HDX Insight analysiert die ICA-Meldungen, die über den Citrix ADC zwischen der Citrix Workspace-App und dem Linux VDA weitergeleitet werden. Alle HDX Insight-Daten entstammen dem virtuellen NSAP-Kanal und werden unkomprimiert gesendet. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert.

Mit den folgenden Befehlen deaktivieren bzw. aktivieren Sie den virtuellen NSAP-Kanal:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000000"
     --force
2 <!--NeedCopy-->
```



```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP" -d "0x00000001"
    --force
<!--NeedCopy-->
```

Problembehandlung

Es werden keine Datenpunkte angezeigt

Es gibt zwei mögliche Ursachen:

- HDX Insight ist nicht richtig konfiguriert.

  Möglicherweise ist AppFlow nicht auf dem Citrix ADC aktiviert oder eine falsche Citrix ADC-Instanz ist in Citrix ADM konfiguriert.

- Der virtuelle ICA-Steuerungskanal wurde auf dem Linux VDA nicht gestartet.

  `ps aux | grep -i ctxctl`

  Wenn `ctxctl` nicht ausgeführt wird, wenden Sie sich an den Administrator, um einen Fehler an Citrix zu melden.

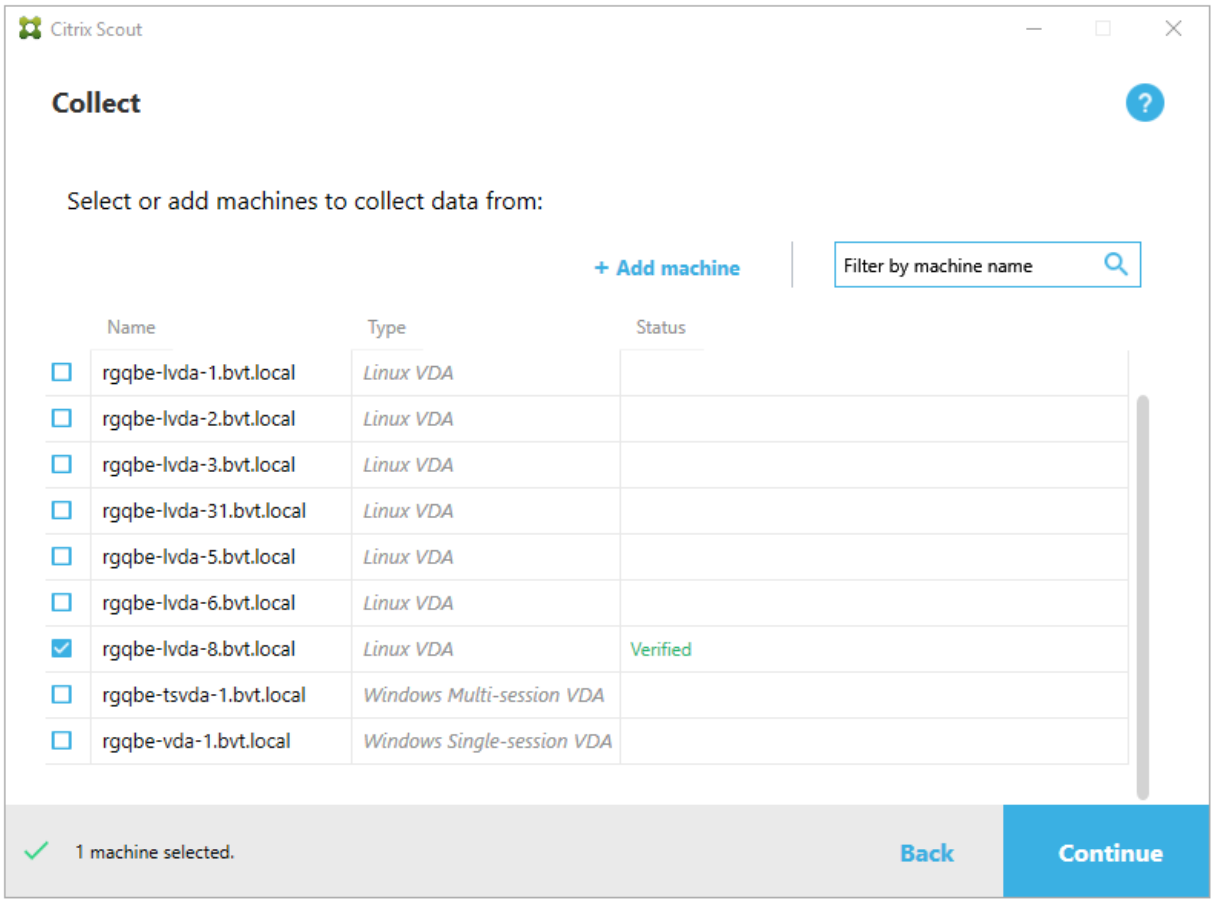
Es werden keine Anwendungsdatenpunkte angezeigt

Stellen Sie sicher, dass der virtuelle Seamlesskanal aktiviert ist und eine Seamlessanwendung ausgeführt wird.

Integration in den Citrix Telemetriedienst

February 9, 2024

Wenn der Citrix Telemetriedienst (`ctxtelemetry`) in die Linux VDA-Software integriert ist, können Sie Citrix Scout ausführen, um mit dem Skript /opt/Citrix/vda/bin/xdlcollect.sh Protokolle zum Linux VDA zu erfassen.



> **Hinweis:**
>
> Nach dem Upgrade von einer Linux VDA-Version bis einschließlich 1912 müssen Sie /opt/Citrix/VDA/sbin/ctxsetup.sh erneut ausführen, um die Variablen für den Citrix Telemetriedienst (`ctxtelemetry`) zu konfigurieren. Weitere Hinweise zu den Variablen finden Sie unter Easy Install.

Aktivieren und Deaktivieren des Citrix Telemetriedienst

- Um den Dienst zu aktivieren, führen Sie den Befehl **sudo systemctl enable ctxtelemetry.socket** aus.
- Um den Dienst zu deaktivieren, führen Sie **sudo systemctl disable ctxtelemetry.socket** aus.

Ports

Der Citrix Telemetriedienst (`ctxtelemetry`) verwendet standardmäßig den TCP/IP-Port 7503, um auf Citrix Scout zu überwachen. Er verwendet den TCP/IP-Port 7502 auf dem Delivery Controller, um mit Citrix Scout zu kommunizieren.

Sie können die Standardports verwenden oder bei der Installation des Linux VDA die Ports über die folgenden Variablen ändern.

- **CTX_XDL_TELEMETRY_SOCKET_PORT:** Der Socketport zur Überwachung auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT:** Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

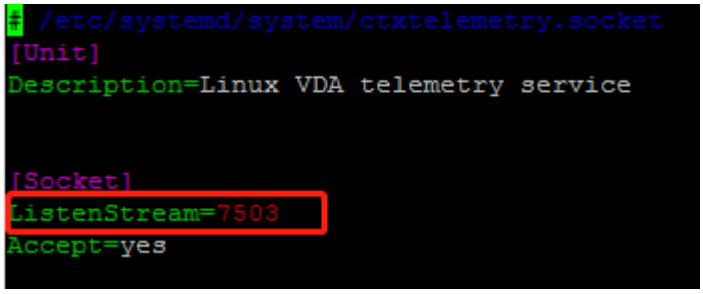
Gehen Sie folgendermaßen vor, um die Ports nach der Installation des Linux VDA zu ändern:

1. Führen Sie den folgenden Befehl aus, um den Port für die Kommunikation mit Scout zu ändern.

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "TelemetryServicePort" -d <port number>
      -t REG_DWORD
2 <!--NeedCopy-->
```

2. Um den Socketport für das Überwachen auf Scout zu ändern, führen Sie den folgenden Befehl aus, um die Datei ctxtelemetry.socket zu öffnen und zu bearbeiten.

```
1 sudo vi /etc/systemd/system/ctxtelemetry.socket
2 <!--NeedCopy-->
```



3. Führen Sie die folgenden Befehle aus, um den Socketport neu zu starten.

```
1 sudo systemctl daemon-reload
2 sudo systemctl stop ctxtelemetry.socket
3 sudo systemctl start ctxtelemetry.socket
4 <!--NeedCopy-->
```

4. Aktivieren Sie die neuen Ports in Ihrer Firewall-Konfiguration.

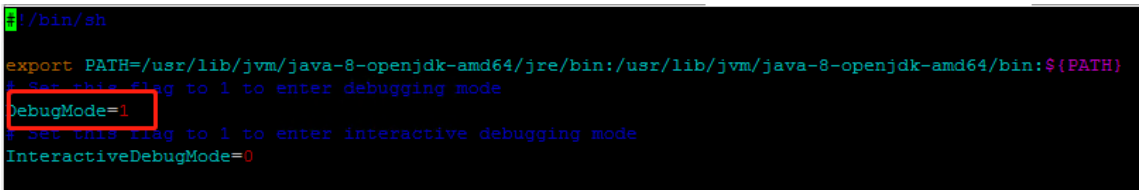
   Wenn Sie beispielsweise Ubuntu verwenden, führen Sie den Befehl **sudo ufw allow 7503** aus, um Port 7503 zu aktivieren.

Debugmodus

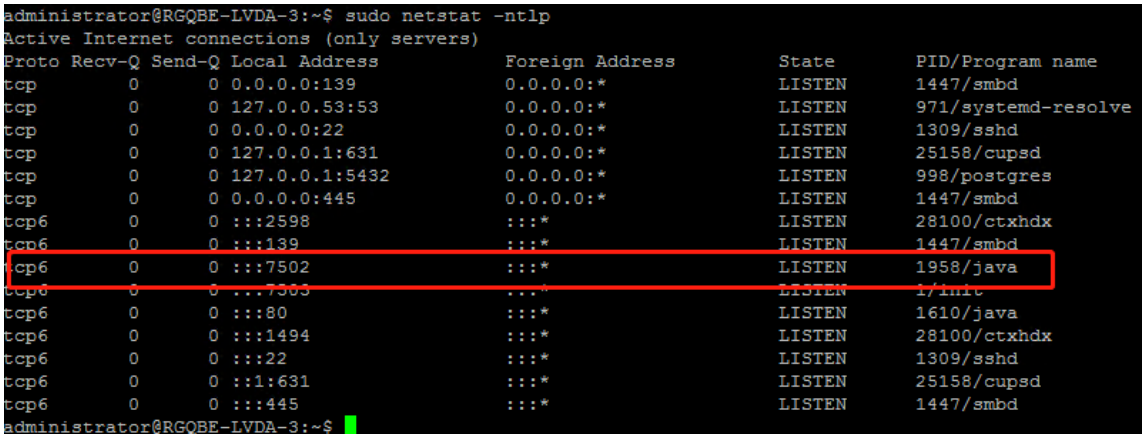
Wenn der Citrix Telemetriedienst nicht einwandfrei funktioniert, können Sie den Debugmodus aktivieren, um die Ursache zu ermitteln.

1. Um den Debugmodus zu aktivieren, führen Sie den folgenden Befehl aus, um die Datei `ctxtelemetry` zu öffnen, und ändern Sie dann den Wert für "DebugMode"in 1.

```
sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
<!--NeedCopy-->
```



2. Beenden Sie den Citrix Telemetriedienst manuell oder warten Sie 15 Minuten, bis der Dienst automatisch beendet wird.



   In diesem Beispiel können Sie die folgenden Befehle ausführen, um den Citrix Telemetriedienst zu beenden.

```
sudo netstat -ntlp
Kill -9 1958
<!--NeedCopy-->
```

3. Um den Citrix Telemetriedienst neu zu starten, wählen Sie den Linux VDA in Scout und suchen Sie telemetry-debug.log in /var/log/xdl/.

Dienstwartezeit

Der `systemd`-Daemon, der den Socketport öffnet, startet standardmäßig und nutzt nur wenige Ressourcen. Der Citrix Telemetriedienst wird standardmäßig beendet und nur gestartet, wenn eine Protokollsammlungsanforderung vom Delivery Controller eintrifft. Nach Abschluss der Protokollsammlung wird der Dienst beendet, sofern für eine Dauer von 15 Minuten keine neue Sammlungsanforderung eingeht. Sie können die Wartezeit über den folgenden Befehl konfigurieren. Der Mindestwert beträgt 10 Minuten. Wenn Sie einen unter 10 Minuten Wert festlegen, wird der

Mindestwert von 10 Minuten wirksam. Nachdem Sie die Wartezeit festgelegt haben, beenden Sie den Dienst und starten Sie ihn neu.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -v "TelemetryServiceIdleTimeoutInMinutes" -d <
   number> -t REG_DWORD
<!--NeedCopy-->
```

Tests zur Überprüfung

Vor Ausführung einer Sammlung wird automatisch jede ausgewählte Maschine überprüft. Diese Prüfung gewährleistet, dass die Anforderungen erfüllt sind. Besteht eine Maschine den Test nicht, wird in Scout eine Meldung mit einem Maßnahmenvorschlag angezeigt. Weitere Informationen finden Sie unter Tests zur Überprüfung in der Citrix Scout-Dokumentation.

Linux VDA-Selfupdate über Azure

May 30, 2024

Mit diesem Feature wird die Linux VDA-Software automatisch sofort oder zu einem geplanten Zeitpunkt aktualisiert. Dies ist dann von Vorteil, wenn Sie Linux VDAs in Citrix DaaS Standard für Azure (früher Citrix Virtual Apps and Desktops Standard für Azure) erstellen. Sie benötigen keine Administratorprivilegien für die VMs in Azure. Weitere Informationen finden Sie unter Erstellen von Linux VDAs in Citrix DaaS Standard für Azure.

Konfiguration

Führen Sie die folgenden Schritte aus, um die Funktion zu nutzen:

Schritt 1: Hochladen von Updateinformationen und neuen VDA-Paketen in den Azure-Container

Schritt 1a: Erstellen Sie einen Container für Ihr Azure-Speicherkonto und legen Sie die Container-Zugriffsebene auf **Blob (anonymer Lesezugriff nur für Blobs)**.

> **Hinweis:**
>
> Azure-Container und Blobs werden ausschließlich von Kunden gepflegt und verwaltet. Citrix haftet nicht für deren Sicherheit. Um Datensicherheit und Kosteneffizienz zu gewährleisten,

> legen Sie die Container-Zugriffsebene nach jedem **Selbstupdate** auf **Privat (kein anonymer Zugriff)** fest.

Schritt 1b: Geben Sie die VDA-Updateinformationen in eine JSON-Datei mit dem Namen "Update-Info.json"ein. Beispiel:

```
{

 "Version": "21.04.200.4",
"Distributions":[
{

"TargetOS": "RHEL7_9",
"PackageName": "",
"PackageHash": ""
 }
 ,
{

"TargetOS": "UBUNTU20_04",
"PackageName": "",
"PackageHash": ""
 }

]
 }

<!--NeedCopy-->
```

Version gibt die neue VDA-Version an und **Distributions** ein Array von Updateobjekten. Jedes Objekt enthält drei Elemente:

- **TargetOS**: muss "RHEL7_9"(für RHEL 7, CentOS 7 und Amazon Linux 2) oder "UBUNTU20_04" sein. **ctxmonitord** erkennt keine anderen Distributionen.
- **PackageName**: Vollständiger Name des VDAs -Pakets der angegebenen Version.
- **PackageHash**: mit dem Befehl `shasum -a 256 <pkgname>` berechneter SHA-256-Wert.

Schritt 1c: Laden Sie die JSON-Datei und die neue Version der Linux VDA-Pakete in Ihren Azure-Container hoch.

Schritt 2: Aktivieren des Selfupdate-Features für das Masterimage oder auf jedem VDA

Standardmäßig ist **Selfupdate** deaktiviert. Wenn Sie Linux VDAs in Citrix DaaS Standard für Azure erstellen, muss die Feature-Aktivierung für das Masterimage durchgeführt werden. Aktivieren Sie andernfalls das Feature direkt für jeden Ziel-VDA.

Zum Aktivieren des **Selbstupdates** führen Sie einen Befehl nach dem folgenden Muster zum Bearbeiten des Registrierungsschlüssels unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Self

aus.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0
   x00000001" --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
<!--NeedCopy-->
```

In der folgenden Tabelle werden die Registrierungseinstellungen beschrieben.

Registrierungseinstellung	Beschreibung
fEnabled	Diese Einstellung ist erforderlich. Standardmäßig ist der Wert 0 und das **Selbstupdate** damit deaktiviert. Sie können den Wert auf 1 setzen, um das **Selbstupdate** zu aktivieren.
URL	Diese Einstellung ist erforderlich. Sie legt die URL des Azure-Containers zum Abrufen von Updateinformationen und neuen VDA-Paketen fest.
ScheduledTime	Diese Einstellung ist erforderlich. Sie können sie auf **Immediately** oder **NextStart** festlegen. **Immediately** bedeutet, dass ein Update sofort nach dem Herunterladen von VDA-Paketen ausgeführt wird. Diese Option eignet sich für hohe Download-Geschwindigkeiten und dringliche Updates. Sie kann jedoch Benutzer stören, wenn beim Herunterladen von Paketen Sitzungen laufen. **NextStart** bedeutet, dass ein Update beim nächsten Start von **ctxmonitord** ausgeführt wird. Diese Option eignet sich für niedrige Download-Geschwindigkeiten und nicht dringliche Updates.

Registrierungseinstellung	Beschreibung
CaCertificate	Diese Einstellung ist optional. Sie legt den vollständigen Pfad eines PEM-Zertifikats zur Prüfung der URL des Azure-Containers fest. Bei Azure-Blobs kann dies das Zertifikat von portal.azure.com sein, das aus dem Browser abgerufen und dann in PEM konvertiert wird. Aus Sicherheitsgründen empfehlen wir, diese Registrierungseinstellung hinzuzufügen. Sie wird jedoch nur unter Ubuntu unterstützt. Unter RHEL fehlt die Verknüpfung von NSS-Bibliotheken für den Befehl `curl`. Legen Sie auf jeden Fall die minimalen Privilegien für das Zertifikat fest.

Wenn **ctxmonitord** neu gestartet wird, ruft es zuerst über **Url** die Datei UpdateInfo.json und aus dieser dann die Updateversion ab. **ctxmonitord** vergleicht dann die Updateversion mit der aktuellen Version. Ist die aktuelle Version älter, lädt der Dienst die neue Version des VDAs -Pakets von Azure herunter und speichert sie lokal. Danach führt er ein Update gemäß der Einstellung **Scheduled-Time** aus. In On-Premises-Bereitstellungen können Sie **ctxmonitord** neu starten, um ein Update auszulösen. In Citrix DaaS Standard für Azure haben Sie hingegen keine Administratorprivilegien für VMs und **ctxmonitord** kann erst nach dem Neustart der VDA-Maschine neu gestartet werden. Wenn ein Update fehlschlägt, wird der VDA auf die bestehende Version zurückgesetzt.

> **Hinweis:**
>
> - Die für das Masterimage konfigurierten Registrierungseinstellungen können nicht geändert werden.
> - Wenn alle VMs in einer Umgebung gleichzeitig ein Paket herunterladen, kann dies zur Überlastung des lokalen Netzwerks führen.
> - Benutzerdaten gehen verloren, wenn sowohl ein Update als auch das Rollback fehlschlagen.
> - Wenn ein Update fehlschlägt, das Rollback jedoch gelingt, haben Benutzer im selben Netzwerk möglicherweise verschiedene Linux VDA-Versionen. Das ist nicht optimal.
> - Updates erfordern in der Regel mehrere Minuten. In Citrix Studio gibt es keine Statusanzeige.

Metriken für Linux-VMs und Linux-Sitzungen

January 8, 2024

Die folgende Tabelle enthält Metriken, die für Linux-VMs und Linux-Sitzungen verfügbar sind.

Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Anmeldedauer	2109	Der Wert gibt an, wie lange Benutzer bei der Anmeldung über die Citrix Workspace-App warten müssen, bis eine Sitzung einsatzbereit ist. Um die Metrik einer Sitzung anzuzeigen, gehen Sie zur Registerkarte Überwachen von Citrix DaaS (früher Citrix Virtual Apps and Desktops Service). Überwachen ist als Director-Konsole verfügbar, um Citrix Virtual Apps and Desktops-Bereitstellungen (Aktuelles Release und LTSR) zu überwachen und zu warten. Klicken Sie auf der Registerkarte Überwachen im Bereich **Durchschnittl. Anmeldedauer** auf **Verlaufstrend anzeigen**. Legen Sie auf der Seite **Anmeldungsleistung** Filterbedingungen fest und klicken Sie auf **Übernehmen**, um Metriken darzustellen.	Nur in “Überwachen” verfügbar.

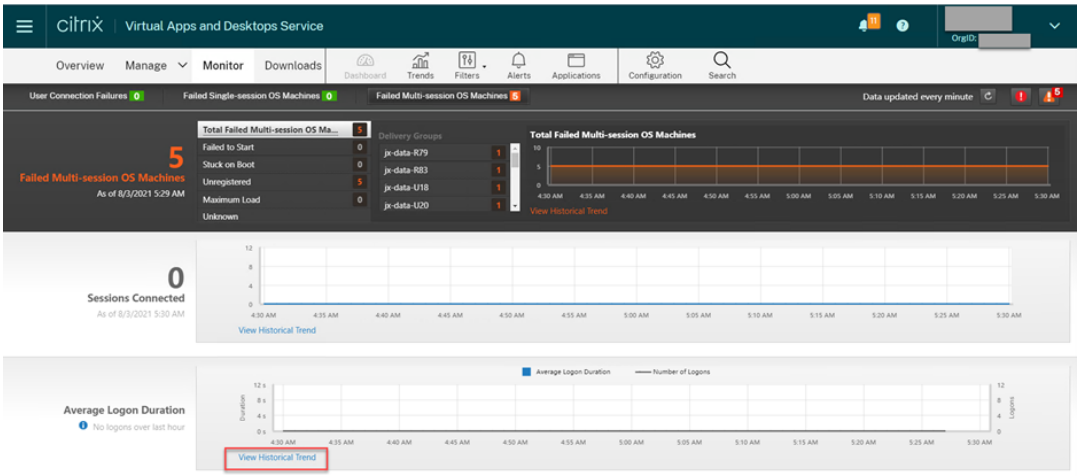
Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Anzahl autom. Sitzungswiederverbindungen	2109	In der Ansicht **Trends** können Sie die Anzahl automatischer Wiederverbindungen einer Sitzung anzeigen. Legen Sie Bedingungen fest und klicken Sie auf **Übernehmen**, um die Suchergebnisse zu beschränken. In der Spalte **Anzahl autom. Sitzungswiederverbindungen** wird die Anzahl der automatischen Wiederverbindungen einer Sitzung angezeigt. Die **automatische Wiederverbindung** ist aktiviert, wenn die Richtlinie **Sitzungszuverlässigkeit** oder **Client automatisch wieder verbinden** aktiviert ist. Weitere Hinweise zur Wiederverbindung von Sitzungen finden Sie unter Sitzungen. Weitere Informationen zu Richtlinien finden Sie unter Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients" und Einstellungen der Richtlinie "Sitzungszuverlässigkeit".	Verfügbar in Citrix Director und in "Überwachen".

Metrik	Min. VDA-Version erforderlich	Beschreibung	Bemerkungen
Leerlaufzeit	2103	Um auf diese Metrik zuzugreifen, öffnen Sie die Seite **Alle Sitzungen** durch Auswahl von **Filter > Sitzungen > Alle Sitzungen**.	Verfügbar in Citrix Director und in “Überwachen”.
Metriken einer Linux-VM	2103	Die folgenden Metriken für Linux-VMs sind verfügbar: Anzahl der CPU-Kerne, Speichergröße, Festplattenkapazität sowie aktuelle und historische CPU- und Speicherauslastung	Verfügbar in Citrix Director und in “Überwachen”.
Protokoll	1909	Das Transportprotokoll einer Linux-Sitzung wird im Bereich **Sitzungsdetails** als UDP oder TCP angezeigt.	Verfügbar in Citrix Director und in “Überwachen”.
ICA RTT	1903	Die ICA-Rundtripzeit (RTT) misst die Zeit zwischen dem Drücken einer Taste und der Anzeige der Reaktion am Endpunkt. Um ICA RTT-Metriken zu erhalten, erstellen Sie in Citrix Studio die Richtlinien **ICA-Roundtripberechnung** und **Intervall für ICA-Roundtripberechnung**.	Verfügbar in Citrix Director und in “Überwachen”.

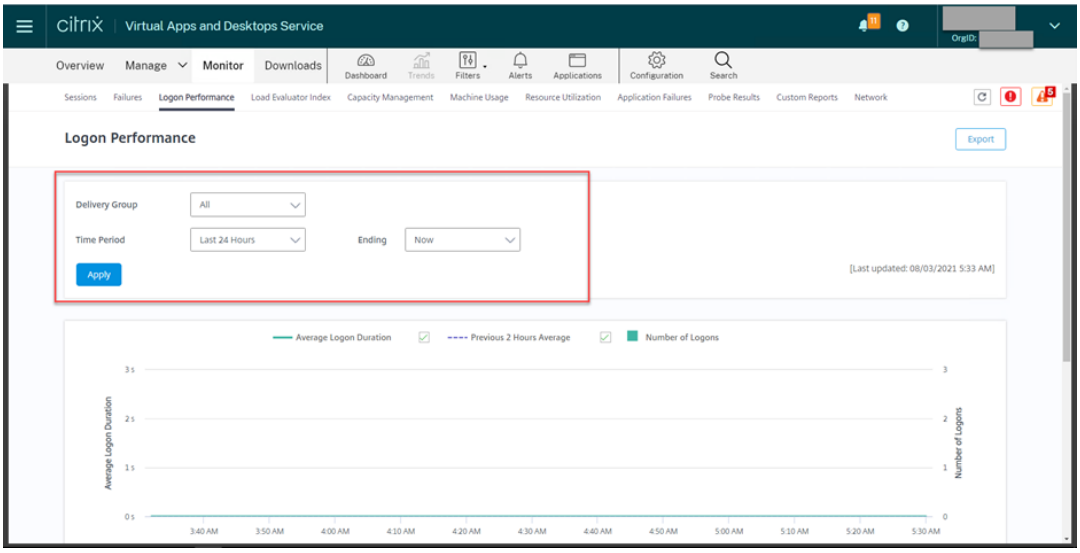
Beispiele für den Zugriff auf verschiedene Metriken in Citrix Director und in “Überwachen”

- **Anmeldedauer**

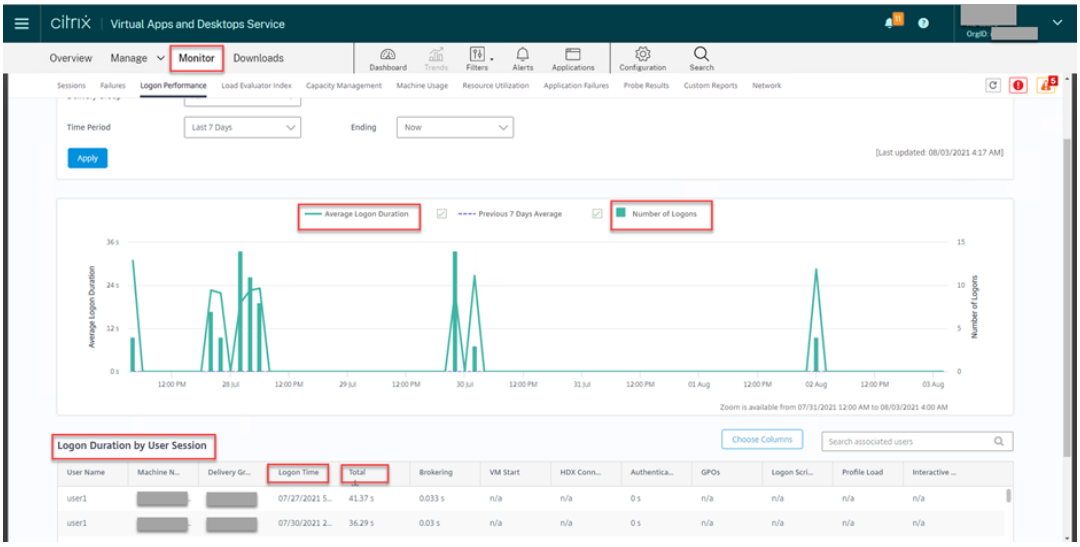
1. Klicken Sie auf der Registerkarte Überwachen von Citrix DaaS im Bereich **Durchschnittl. Anmeldedauer** auf **Verlaufstrend anzeigen**.



2. Legen Sie auf der Seite **Anmeldungsleistung** Filterbedingungen fest.

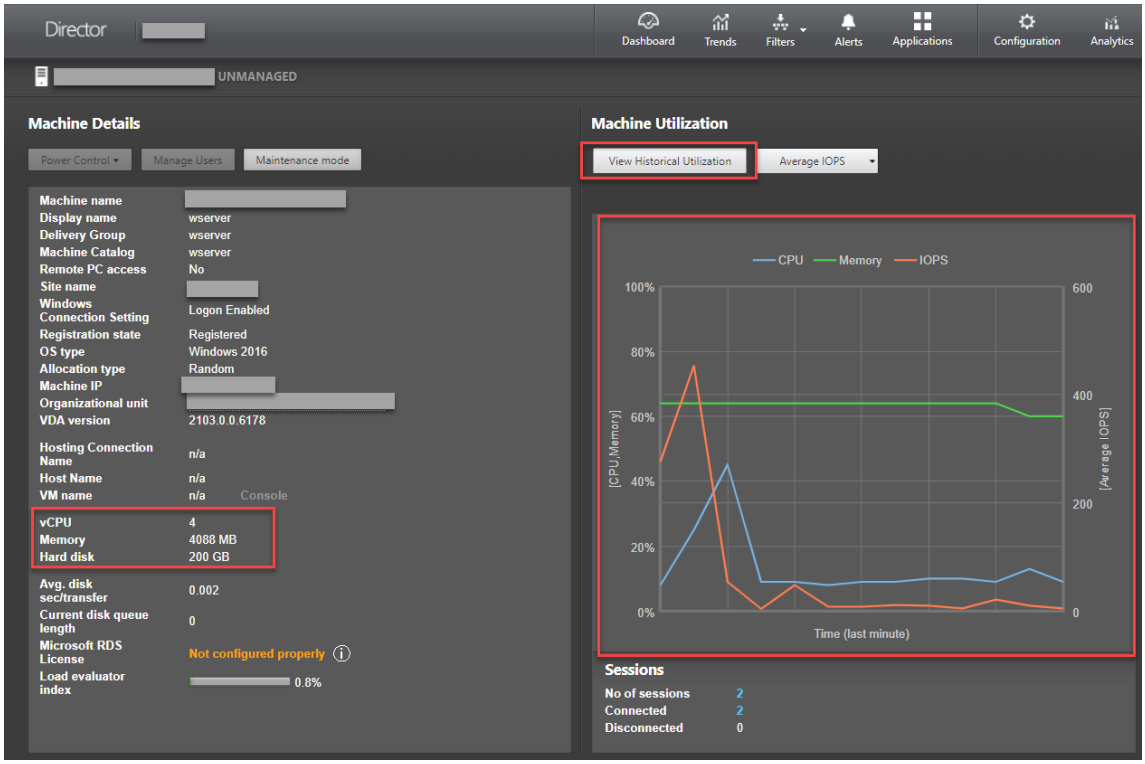


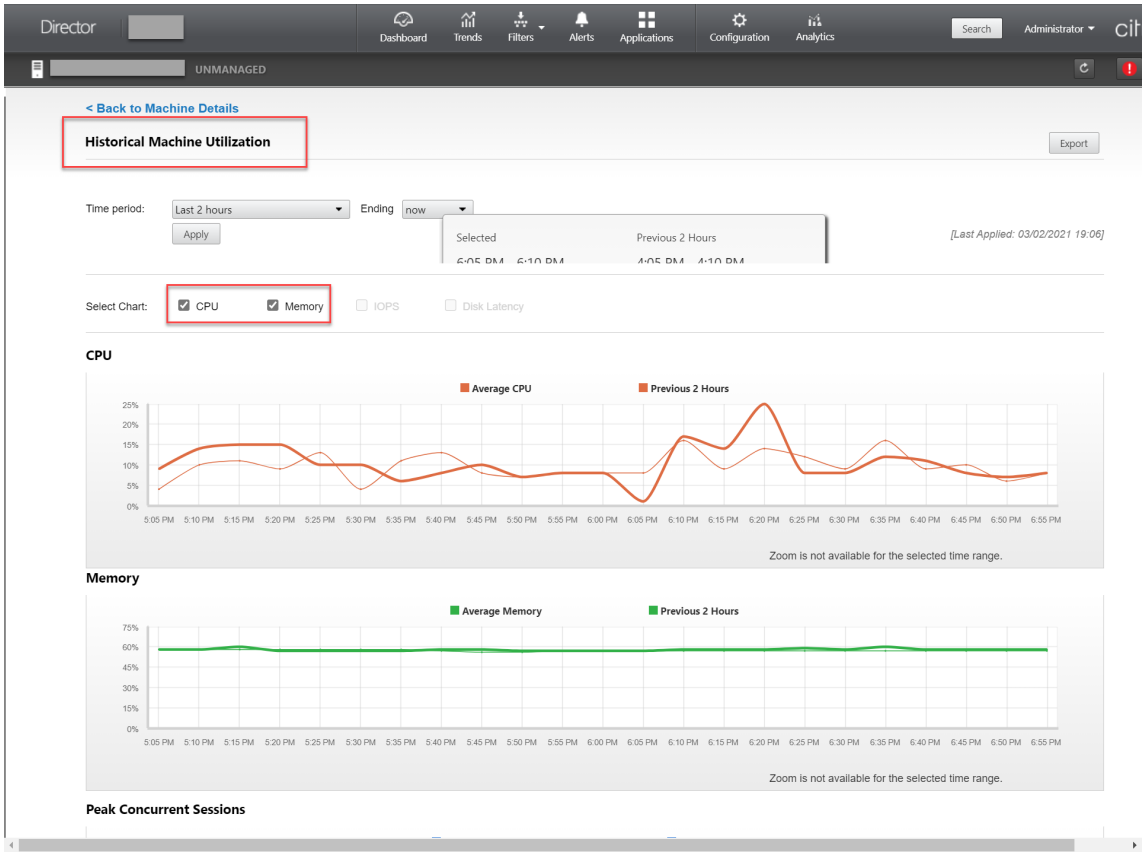
3. Klicken Sie auf **Übernehmen**, um die Metriken zur Anmeldedauer darzustellen.



- **Angaben zur Anzahl der CPU-Kerne, Speichergröße und Festplattenkapazität sowie aktuelle und historische Daten zur CPU- und Speicherauslastung**

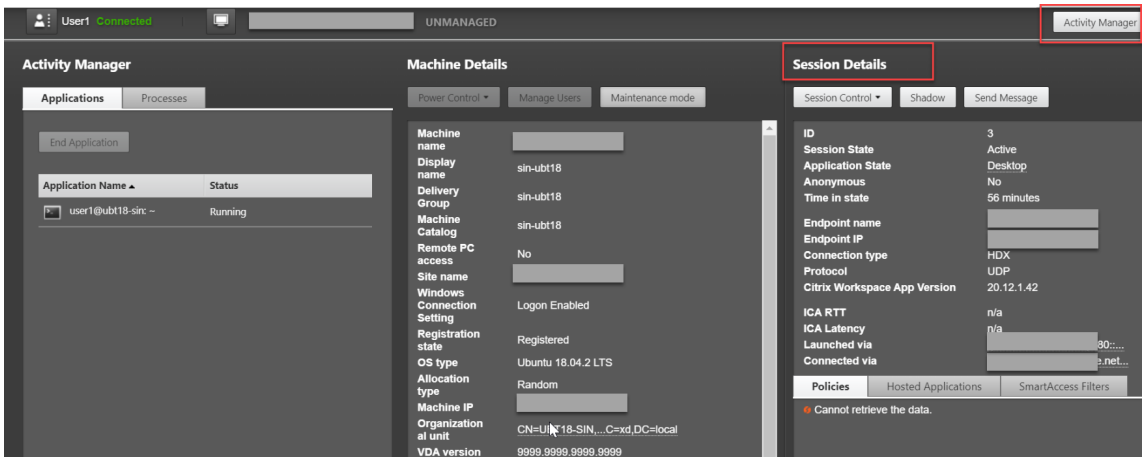
  Um auf diese Metriken einer Linux-VM zuzugreifen, suchen Sie die VM in Citrix Director oder in Überwachen und überprüfen dann den Bereich **Maschinendetails**. Beispiel:





- **ICA RTT und Protokoll**

  Um die Metriken einer Linux-Sitzung anzuzeigen, öffnen Sie die Seite **Alle Sitzungen** durch Auswahl von **Filter > Sitzungen > Alle Sitzungen**, oder greifen Sie auf den Bereich **Sitzungsdetails** zu. Um auf den Bereich **Sitzungsdetails** zuzugreifen, öffnen Sie die Seite **Alle Sitzungen** und klicken Sie auf eine Zielsitzung, um die Ansicht **Aktivitätsmanager** aufzurufen. Beispiel:

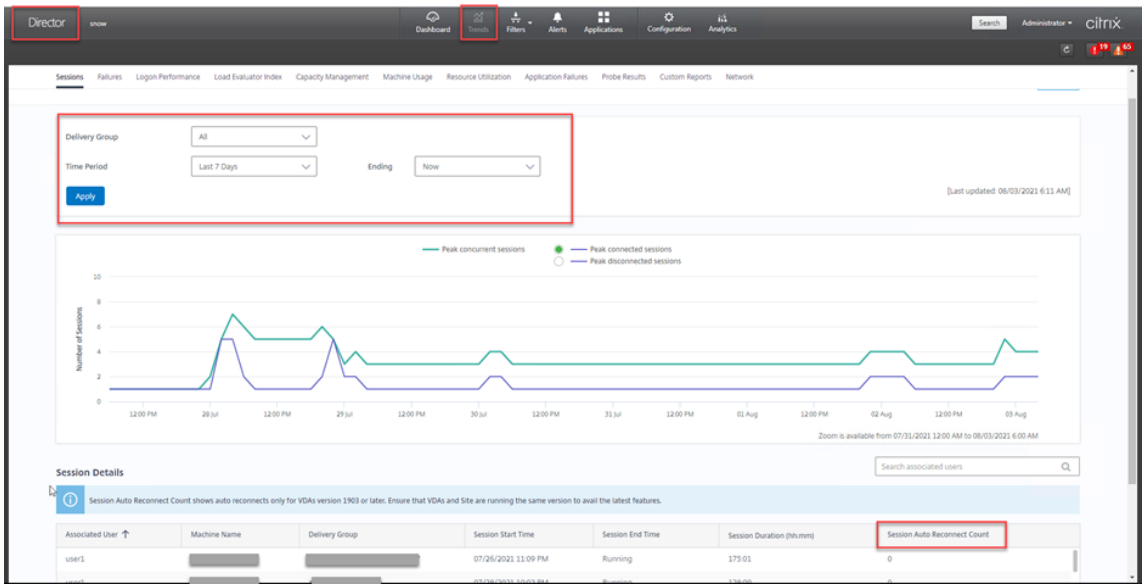


- **Anzahl autom. Sitzungswiederverbindungen**

  In der Ansicht **Trends** können Sie die Anzahl automatischer Wiederverbindungen einer Sitzung

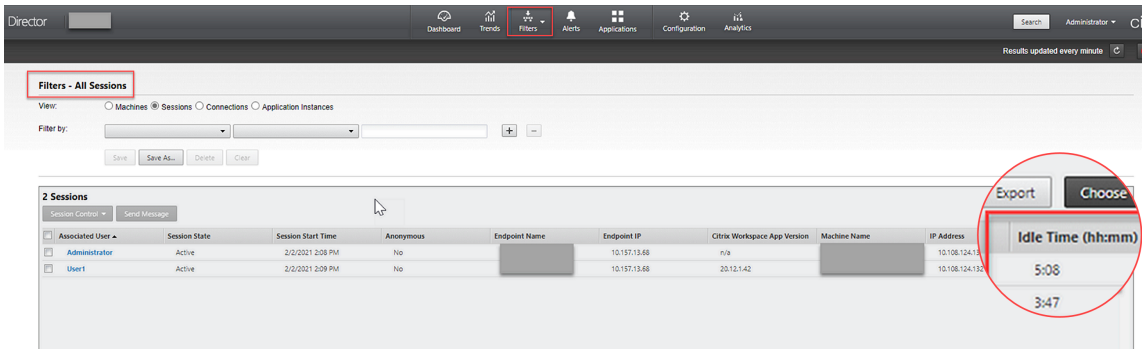
anzeigen. Legen Sie Bedingungen fest und klicken Sie auf **Übernehmen**, um die Suchergebnisse zu beschränken.

In der Spalte **Anzahl autom. Sitzungswiederverbindungen** wird die Anzahl der automatischen Wiederverbindungen einer Sitzung angezeigt. Beispiel:



- **Leerlaufzeit**

  Beispiel:



Protokollsammlung

January 8, 2024

Übersicht

Das Sammeln von Protokollen ist für den Linux VDA standardmäßig aktiviert.

Konfiguration

Der ctxlogd-Daemon und das setlog-Hilfsprogramm sind im Linux VDA-Releasepaket enthalten. Standardmäßig wird der ctxlogd-Daemon nach der Installation und Konfiguration des Linux VDA gestartet.

ctxlogd-Daemon

Alle anderen Dienste, deren Ablauf verfolgt wird, hängen vom ctxlogd-Daemon ab. Sie können den ctxlogd-Daemon anhalten, wenn Sie den Ablauf des Linux VDA nicht verfolgen möchten.

setlog-Hilfsprogramm

Das Sammeln von Protokollen wird mit dem setlog-Hilfsprogramm konfiguriert. Es ist an folgendem Pfad: **/opt/Citrix/VDA/bin/**. Nur Root-Benutzer können es ausführen. Verwenden Sie zum Anzeigen und Ändern von Konfigurationen die grafische Benutzeroberfläche oder Befehle. Führen Sie den folgenden Befehl aus, um Hilfe zum setlog-Dienstprogramm aufzurufen:

```
setlog help
<!--NeedCopy-->
```

Werte Standardmäßig ist **Log Output Path** auf **/var/log/xdl/hdx.log** und **Max Log Size** auf 200 MB festgelegt. Sie können zwei alte Protokolldateien unter **Log Output Path** speichern.

Anzeigen der aktuellen setlog-Werte:

```
setlog values

log_path (Log Output Path) = /var/log/xdl/hdx.log

log_size (Max Log Size (MiB)) = 200

log_count (Max Old Log Files) = 2
<!--NeedCopy-->
```

Anzeigen oder Festlegen eines einzelnen setlog-Werts:

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

Beispiel:

```
setlog value log_size 100
<!--NeedCopy-->
```


Ebenen Standardmäßig sind Protokollebenen auf **warning** festgelegt (Groß-/Kleinschreibung wird nicht beachtet).

Führen Sie den folgenden Befehl aus, um Protokollebenen für verschiedene Komponenten anzuzeigen:

```
setlog levels
<!--NeedCopy-->
```

Sie können die Protokollebenen (einschließlich Disabled, Inherited, Verbose, Information, Warnings, Errors und Fatal Errors) mit dem folgenden Befehl festlegen:

```
setlog level <class> [<level>]
<!--NeedCopy-->
```

Protokollebene	Befehlsparameter (Groß-/Kleinschreibung unerheblich)
Deaktiviert	none
Geerbt	inherit
Verbose	verbose
Informationen	Info
Warnungen	Warnung
Fehler	Fehler
Schwerwiegende Fehler	fatal

Mit der Variable **<class>** wird eine Komponente des Linux VDA angegeben. Um alle Komponenten einzubeziehen, legen Sie “all”fest: Beispiel:

```
setlog level all error
<!--NeedCopy-->
```

Flags Flags werden wie folgt festgelegt:

```
setlog flags

DATE = true

TIME = true

NAME = true

PID = true

```



```
TID = false

SID = true

UID = false

GID = false

CLASS = false

LEVEL = false

FUNC = true

FILE = false
<!--NeedCopy-->
```

Anzeigen der aktuellen Flags:

```
setlog flags
<!--NeedCopy-->
```

Anzeigen oder Festlegen eines einzelnen Protokoll-Flags:

```
setlog flag <flag> [<state>]
<!--NeedCopy-->
```

Standardeinstellungen wiederherstellen Wiederherstellen der Standardeinstellungen für alle Ebenen, Flags und Werte:

```
setlog default
<!--NeedCopy-->
```

> **Wichtig:**
>
> Der `ctxlogd`-Dienst wird mit der Datei **/var/xdl/.ctxlog** konfiguriert, die nur von Root-Benutzern erstellt werden kann. Andere Benutzer haben keine Schreibrechte für diese Datei. Wir empfehlen Root-Benutzern, anderen Benutzern keine Schreibrechte zu geben. Die versehentliche oder mutwillige Fehlkonfiguration von `ctxlogd` kann sich negativ auf die Serverleistung und die Benutzererfahrung auswirken.

Problembehandlung

Wenn die Datei **/var/xdl/.ctxlog** nicht vorhanden ist (z. B. versehentlich gelöscht wurde), schlägt der `ctxlogd`-Daemon fehl und Sie können den `ctxlogd`-Dienst nicht neu starten.

/var/log/messages:


```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
   configuration file.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited, code
   =exited, status=1/FAILURE

Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.

Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
<!--NeedCopy-->
```

Sie lösen das Problem, indem Sie `setlog` als Root-Benutzer ausführen, um die Datei **/var/xdl/.ctxlog** neu zu erstellen. Starten Sie dann den `ctxlogd`-Dienst neu, da andere Dienste von ihm abhängen.

Sitzungsspiegelung

April 19, 2024

Die Sitzungsspiegelung ermöglicht es Domänenadministratoren, ICA-Sitzungen von Benutzern in einem Intranet anzuzeigen. Dabei wird unter Einsatz von noVNC eine Verbindung mit den ICA-Sitzungen hergestellt.

> **Hinweis:**
>
> Zur Verwendung des Features ist `Citrix Director` 7.16 oder höher erforderlich.

Installation und Konfiguration

Abhängigkeiten

Für die Sitzungsspiegelung sind zwei neue Elemente, `python-websockify` und `x11vnc`, erforderlich. Installieren Sie `python-websockify` und `x11vnc` nach der Installation des Linux VDA manuell.

Für RHEL 7.x und Amazon Linux2:

Führen Sie die nachstehenden Befehle aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

(Für RHEL 7.x) Lösen Sie `python-websockify` und `x11vnc` auf, indem Sie das EPEL-Repository (Extra Packages for Enterprise Linux) und das optionale RPMs-Repository aktivieren:

- EPEL

  Das EPEL-Repository ist für x11vnc erforderlich. Führen Sie folgenden Befehl aus, um das EPEL-Repository zu aktivieren:

```
yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
<!--NeedCopy-->
```

- Optionale RPMs

  Führen Sie den folgenden Befehl aus, um das optionale RPMs-Repository zum Installieren einiger Abhängigkeitspakete von x11vnc zu aktivieren:

```
subscription-manager repos --enable rhel-7-server-optional-rpms --enable rhel-7-server-extras-rpms
<!--NeedCopy-->
```

RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x:

Führen Sie die nachstehenden Befehle aus, um python-websockify und x11vnc (x11vnc Version 0.9.13 oder höher) zu installieren.

```
sudo pip3 install websockify
sudo yum install x11vnc
<!--NeedCopy-->
```

Zum Auflösen von x11vnc aktivieren Sie die EPEL- und CodeReady Linux Builder-Repositorys:

```
dnf install -y --nogpgcheck https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

subscription-manager repos --enable "codeready-builder  -for-rhel-8-x86_64-rpms"
<!--NeedCopy-->
```

Ubuntu:

Führen Sie die nachstehenden Befehle aus, um python-websockify und x11vnc (x11vnc Version 0.9.13 oder höher) zu installieren:

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--NeedCopy-->
```

SUSE:

Führen Sie die nachstehenden Befehle aus, um python-websockify und x11vnc (x11vnc Version 0.9.13 oder höher) zu installieren:

```
sudo pip3 install websockify
sudo zypper install x11vnc
```



```
<!--NeedCopy-->
```

Für Debian:

Führen Sie die nachstehenden Befehle aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
sudo pip3 install websockify
sudo apt-get install x11vnc
<!--NeedCopy-->
```

Port

Die Sitzungsspiegelung wählt automatisch verfügbare Ports aus dem Bereich 6001–6099 für den Aufbau von Verbindungen vom Linux VDA mit `Citrix Director` aus. Daher ist die Anzahl der ICA-Sitzungen, die Sie gleichzeitig spiegeln können, auf 99 begrenzt. Stellen Sie sicher, dass genügend Ports zur Verfügung stehen, insbesondere wenn mehrere Sitzungen gespiegelt werden.

Registrierung

Die folgende Tabelle enthält die relevanten Registrierungseinträge:

Registrierung	Beschreibung	Standardwert
EnableSessionShadowing	Aktiviert oder deaktiviert die Sitzungsspiegelung	1 (aktiviert)
ShadowingUseSSL	Legt fest, ob die Verbindung zwischen Linux VDA und Citrix Director verschlüsselt werden soll.	0 (deaktiviert)

Führen Sie den Befehl `ctxreg` auf dem Linux VDA aus, um die Registrierungswerte zu ändern. Um beispielsweise die Sitzungsspiegelung zu deaktivieren, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -v "EnableSessionShadowing" -d 0x00000000
```

SSL

Für die noVNC-Verbindung zwischen Linux VDA und Citrix Director wird das WebSocket-Protokoll verwendet. Ob bei der Sitzungsspiegelung `ws://` oder `wss://` ausgewählt wird, hängt vom o. g. Reg-

istrierungswert “ShadowingUseSSL”ab. Standardmäßig wird `ws://` ausgewählt. Aus Sicherheitsgründen empfehlen wir jedoch die Verwendung von `wss://` und die Installation von Zertifikaten auf jedem Citrix Director-Client und jedem Linux VDA-Server. Citrix übernimmt keinerlei Haftung für die Sicherheit bei Spiegelung von Linux VDA-Sitzungen mit `ws://`.

Beschaffung von Server- und SSL-Stammzertifikat Zertifikate müssen von einer vertrauenswürdigen Zertifizierungsstelle signiert werden.

Ein separates Serverzertifikat einschließlich Schlüssel ist für jeden Linux VDA-Server erforderlich, auf dem Sie SSL konfigurieren möchten. Da durch ein Serverzertifikat ein ganz bestimmter Computer identifiziert wird, müssen Sie den vollqualifizierten Domänennamen (FQDN) jedes Servers kennen. Sie können stattdessen ein Platzhalterzertifikat für die gesamte Domäne verwenden. In diesem Fall müssen Sie zumindest den Domänennamen kennen.

Ein Stammzertifikat ist auch für jeden Citrix Director-Client erforderlich, der mit dem Linux VDA kommuniziert. Stammzertifikate erhalten Sie von derselben Zertifizierungsstelle, die auch die Serverzertifikate ausgibt.

Sie können Server- und Clientzertifikate von den folgenden Zertifizierungsstellen installieren:

- Eine Zertifizierungsstelle, die mit Ihrem Betriebssystem gebündelt ist
- Eine Unternehmenszertifizierungsstelle (eine Zertifizierungsstelle, die Ihr Unternehmen Ihnen zugänglich macht)
- Eine Zertifizierungsstelle, die nicht mit Ihrem Betriebssystem gebündelt ist

Fragen Sie das Sicherheitsteam Ihres Unternehmens, mit welcher Methode Zertifikate abgerufen werden.

Wichtig:

- Der allgemeine Name (CN) für ein Serverzertifikat muss in Form des FQDN des Linux VDA oder mindestens eines richtigen Platzhalterzeichens plus Domänenzeichen angegeben werden. Beispiel: vda1.basedomain.com oder *.basedomain.com.
- Hashalgorithmen einschließlich SHA1 und MD5 sind für einige Browser zu schwach für Signaturen in digitalen Zertifikaten. Daher wird SHA-256 als Mindeststandard angegeben.

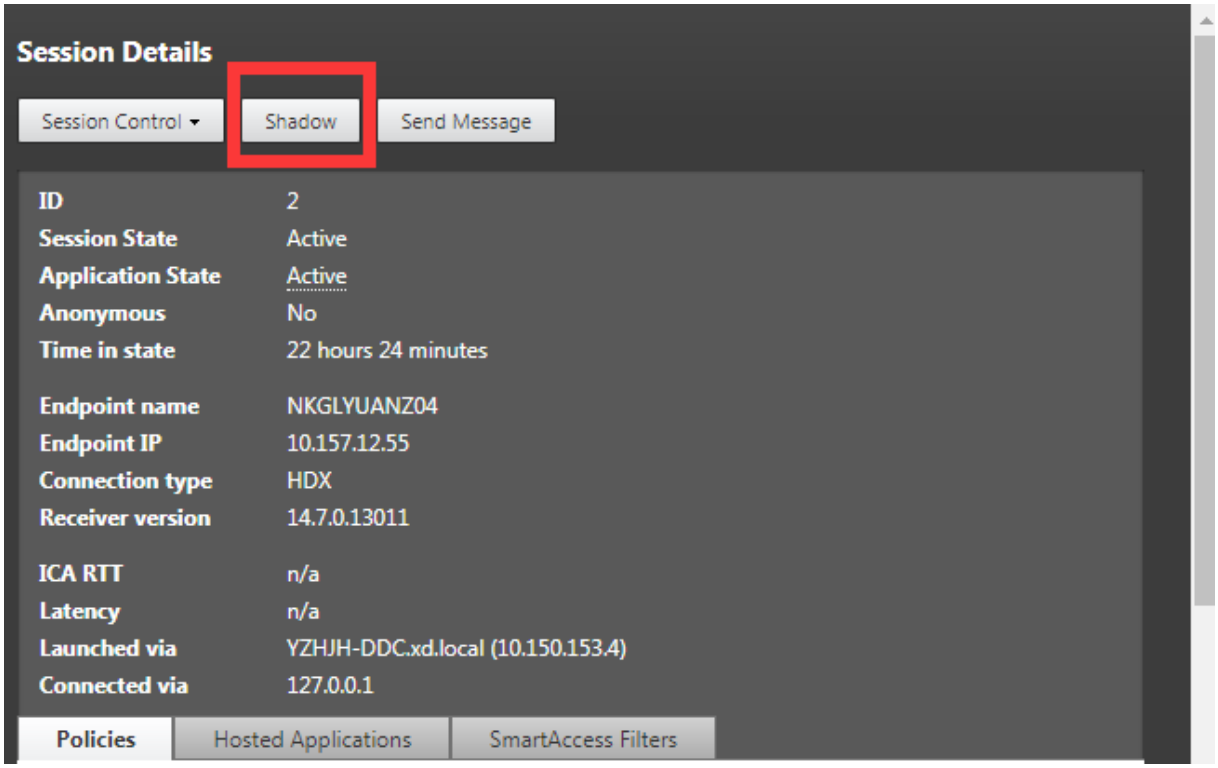
Installieren eines Stammzertifikats auf jedem Citrix Director-Client Die Sitzungsspiegelung verwendet denselben registrierungsbasierten Zertifikatsspeicher wie IIS. Sie können daher Zertifikate wahlweise mit IIS oder dem Zertifikat-Snap-In der Microsoft Management Console (MMC) installieren. Wenn Sie ein Zertifikat von einer Zertifizierungsstelle erhalten haben, rufen Sie den IIS-Assistenten für Webserverzertifikate wieder auf. Der Assistent führt den Prozess fort und installiert das Zertifikat. Sie können auch Zertifikate mit der MMC anzeigen und importieren und das Zertifikat als eigenständiges

Snap-In hinzufügen. Bei Internet Explorer und Google Chrome werden die unter dem Betriebssystem installierten Zertifikate standardmäßig importiert. Bei Mozilla Firefox müssen Sie die Root-SSL-Zertifikate über die Registerkarte **Berechtigungen** des Zertifikatsmanagers importieren.

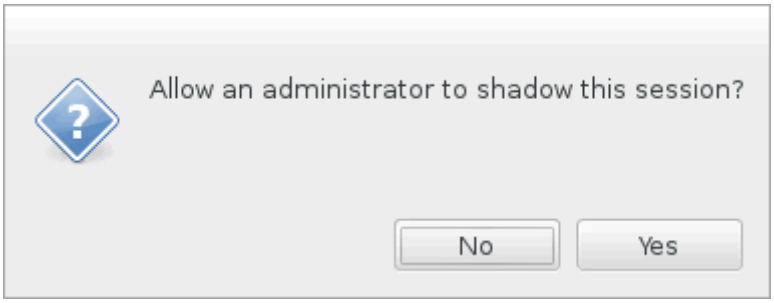
Installieren Sie ein Serverzertifikat und den zugehörigen Schlüssel auf jedem Linux VDA-Server
Benennen Sie die Serverzertifikate "shadowingcert.*"und die Schlüsseldatei "shadowingkey.*"(* gibt das Format an, z. B. shadowingcert.pem und shadowingkey.key). Legen Sie Serverzertifikate und Schlüsseldateien im Pfad **/etc/xdl/shadowingssl** ab und schützen Sie sie ordnungsgemäß mit eingeschränkten Berechtigungen. Ein Fehler bei Namen oder Pfad führt dazu, dass der Linux VDA das Zertifikat bzw. die Schlüsseldatei nicht findet und einen Verbindungsfehler mit `Citrix Director` verursacht.

Verwendung

Suchen Sie in `Citrix Director` die Zielsitzung und klicken Sie in der Ansicht **Sitzungsdetails** auf **Spiegeln**, um eine Spiegelungsanforderung an den Linux VDA zu senden.



Wenn die Verbindung initialisiert wurde, wird auf dem ICA-Sitzungsclient (nicht dem `Citrix Director`-Client) eine Aufforderung an den Benutzer zur Autorisierung des Spiegelns der Sitzung angezeigt.



Wenn der Benutzer auf **Ja** klickt, wird unter Citrix Director ein Fenster mit dem Hinweis angezeigt, dass die ICA-Sitzung gespiegelt wird.

Weitere Informationen zur Verwendung finden Sie in der Dokumentation für Citrix Director.

Einschränkungen

- Die Sitzungsspiegelung ist nur für die Verwendung in einem Intranet vorgesehen. Sie funktioniert nicht in externen Netzwerken, auch nicht über Citrix Gateway. Citrix übernimmt keinerlei Haftung bei Spiegelung von Linux VDA-Sitzungen in einem externen Netzwerk.
- Wenn die Sitzungsspiegelung aktiviert ist, kann ein Domänenadministrator die ICA-Sitzungen anzeigen, hat jedoch keine Berechtigung zum Schreiben oder Steuern.
- Wenn ein Administrator in Citrix Director auf **Spiegeln** klickt, wird dem Benutzer eine Aufforderung zum Zulassen der Spiegelung der Sitzung angezeigt. Eine Sitzung kann nur gespiegelt werden, wenn der Sitzungsbenutzer die Berechtigung erteilt.
- Für die o. g. Aufforderung gilt ein Timeout von 20 Sekunden. Nach Ablauf des Timeouts schlägt sie fehl.
- Eine Sitzung kann nur von einem Administrator gespiegelt werden. Wenn Administrator B beispielsweise eine Spiegelungsanforderung für einen Sitzungsadministrator A sendet, wird die Aufforderung zum Zulassen erneut auf dem Benutzergerät angezeigt. Stimmt der Benutzer zu, wird die Spiegelungsverbindung von Administrator A beendet und eine neue Spiegelungsverbindung für Administrator B erstellt. Wenn ein Administrator eine weitere Spiegelungsanforderung für dieselbe Sitzung sendet, kann auch eine neue Spiegelungsverbindung erstellt werden.
- Installieren Sie zum Verwenden der Sitzungsspiegelung Citrix Director 7.16 oder höher.
- Citrix Director-Clients verwenden beim Herstellen einer Verbindung mit dem Linux VDA-Server den FQDN anstelle der IP-Adresse. Daher muss der Citrix Director-Client in der Lage sein, den FQDN des Linux VDA-Servers aufzulösen.

Problembehandlung

Wenn die Sitzungsspiegelung fehlschlägt, debuggen Sie sowohl auf dem `Citrix Director`-Client als auch auf dem Linux VDA.

Citrix Director-Client

Prüfen Sie mit den Entwicklertools des Browsers die Ausgabeprotokolle auf der Registerkarte **Konsole**. Oder überprüfen Sie die Antwort der ShadowLinuxSession-API auf der Registerkarte **Netzwerk**. Wenn die Aufforderung zum Abrufen der Zulassung beim Benutzer angezeigt wird, der Verbindungsaufbau jedoch fehlschlägt, senden Sie manuell einen Ping an den FQDN des VDAs , um zu überprüfen, ob `Citrix Director` den FQDN auflösen kann. Bei Problemen mit der `wss://`-Verbindung sollten Sie Ihre Zertifikate überprüfen.

Linux VDA

Vergewissern Sie sich, dass auf eine Spiegelungsanforderung hin die Aufforderung zum Abrufen der Zulassung beim Benutzer angezeigt wird. Ist dies nicht der Fall, überprüfen Sie die Dateien vda.log und hdx.log auf Hinweise. Gehen Sie folgendermaßen vor, um die Datei vda.log zu erhalten:

1. Suchen Sie die Datei /etc/xdl/ctx-vda.conf. Kommentieren Sie die folgende Zeile aus, um die vda.log-Konfiguration zu aktivieren:

   ```
   Log4jConfig="/etc/xdl/log4j.xml"
   ```

2. Öffnen Sie /etc/xdl/log4j.xml, suchen Sie den Teil com.citrix.dmc und ändern Sie “info”wie folgt in “trace”:

   ```
   <!-- Broker Agent Plugin - Director VDA plugin Logger -->

    <logger name="com.citrix.dmc">

      <level value="trace"/>

    </logger>
   <!--NeedCopy-->
   ```

3. Führen Sie den Befehl `service ctxvda restart` aus, um den `ctxvda`-Dienst neu zu starten.

Im Fall eines Fehlers beim Verbindungsaufbau:

1. Überprüfen Sie, ob eine Firewall-Beschränkung vorliegt, die das Öffnen des Ports durch die Sitzungsspiegelung verhindert.

2. Vergewissern Sie sich, dass Sie die Zertifikate und Schlüsseldateien ordnungsgemäß benannt und für das SSL-Szenario im richtigen Verzeichnis abgelegt haben.
3. Stellen Sie sicher, dass zwischen 6001 und 6099 genügend Ports für neue Spiegelungsanforderungen vorhanden sind.

Monitor Service Daemon

May 30, 2024

Der Monitor Service Daemon **ctxmonitord** überwacht wichtige Dienste durch periodisch durchgeführte Scans. Beim Erkennen einer Ausnahme werden Dienstprozesse vom Daemon angehalten oder neu gestartet, und Prozesse werden zur Freigabe von Ressourcen bereinigt. Die erkannten Ausnahmen werden in der Datei **/var/log/xdl/ms.log** aufgezeichnet.

Konfiguration

Der Monitor Service Daemon wird automatisch gestartet, wenn Sie den VDA starten.

Sie können das Feature mit Administratorrechten über die Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** unter **/opt/Citrix/VDA/sbin** konfigurieren.

Starten Sie den Monitor Service Daemon über folgenden Befehl neu, damit die Änderungen in den Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** wirksam werden.

```
systemctl restart ctxmonitord
<!--NeedCopy-->
```

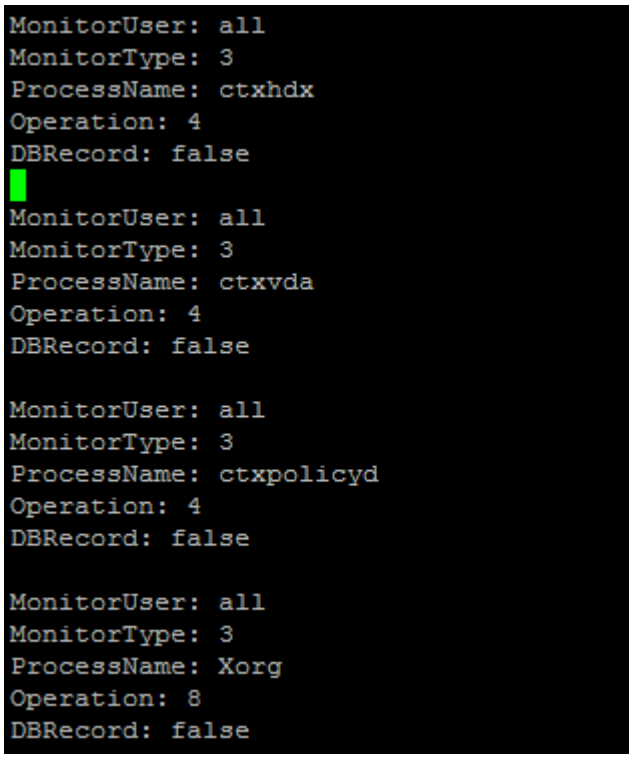
- **scanningpolicy.conf**

  Diese Konfigurationsdatei aktiviert oder deaktiviert den Monitor Service Daemon. Sie legt das Diensterkennungsintervall fest und gibt an, ob erkannte Ausnahmen repariert werden sollen.

  - MonitorEnable: true/false (Standardwert: true)
  - DetectTime: 20 (Einheit: Sekunden, Standardwert: 20, Mindestwert: 5)
  - AutoRepair: true/false (Standardwert: true)
  - MultBalance: false
  - ReportAlarm: false

- **rulesets.conf**

Diese Konfigurationsdatei legt fest, welche Dienste überwacht werden. Vier Dienste werden standardmäßig überwacht, wie in der folgenden Bildschirmaufnahme zu sehen ist.



Legen Sie die folgenden Felder fest, um die zu überwachenden Dienste zu konfigurieren.

- **MonitorUser**: all
- **MonitorType**: 3
- **ProcessName**: <> (Der Prozessname darf nicht leer sein und muss exakt übereinstimmen.)
- **Operation**: 1/2/4/8 (1 = Dienst bei erkannter Ausnahme anhalten. 2 = Dienst bei erkannter Ausnahme abbrechen. 4 = Dienst neu starten. 8 = Xorg-Prozess bereinigen.)
- **DBRecord**: false

- **whitelist.conf**

  Die in der Datei **rulesets.conf** angegebenen Zieldienste müssen auch in der Datei **whitelist.conf** konfiguriert werden. Die konfigurierte Positivliste agiert als zweiter Sicherheitsfilter.

  Zum Konfigurieren der Positivliste fügen Sie nur die Prozessnamen (die exakt übereinstimmen müssen) in die Datei **whitelist.conf** ein. Ein Beispiel sehen Sie im folgenden Screenshot.


```
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:**
>
> Führen Sie erst den Befehl **systemctl stop ctxmonitord** aus, um den Monitor Service Daemon zu stoppen, bevor Sie die Dienste **ctxvda**, **ctxhdx** und **ctxpolicyd** stoppen. Andernfalls startet der Monitor Service Daemon die angehaltenen Dienste neu.

Tools und Hilfsprogramme

January 8, 2024

Hilfsprogramm zur Abfrage von Sitzungsdaten

Wir bieten ein Hilfsprogramm (**ctxsdcutil**), mit dem Sie Sitzungsdaten für jeden Linux VDA abfragen können. Führen Sie den Befehl `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]` aus, um die folgenden Daten aller Sitzungen oder einer bestimmten Sitzung auf einem VDA abzufragen. Das Argument `[-c]` bedeutet, dass Daten im Sekundentakt abgefragt werden.

- **Eingabebandbreite für Sitzung**

- **Ausgabebandbreite für Sitzung**
- **Ausgabeübertragungsrate für Sitzung**
- **Latenz - zuletzt gemessen**
- **Roundtripzeit**
- **Ausgabebandbreite für Thinwire**
- **Ausgabebandbreite für Audio**
- **Ausgabebandbreite für Drucker**
- **Eingabebandbreite für Laufwerk**
- **Ausgabebandbreite für Laufwerk**

Das xdlcollect-Bashskript

Das **xdlcollect**-Bashskript zum Sammeln der Protokolle ist in die Linux VDA-Software integriert und unter **/opt/Citrix/VDA/bin** zu finden. Nach der Installation des Linux VDA können Sie den Befehl **bash /opt/Citrix/VDA/bin/xdlcollect.sh** ausführen, um Protokolle zu sammeln. Nach Abschluss der Protokollsammlung wird eine komprimierte Protokolldatei in dem Ordner mit dem Skript generiert. Das **xdlcollect**-Bashskript kann fragen, ob Sie die komprimierte Protokolldatei in Citrix Insight Services (CIS) hochladen möchten. Wenn Sie zustimmen, gibt **xdlcollect** nach Abschluss des Uploads eine upload_ID zurück. Die komprimierte Protokolldatei wird beim Upload nicht von Ihrem lokalen Computer entfernt. Andere Benutzer können mit der upload_ID auf die Protokolldatei in CIS zugreifen.

XDPing

Das Linux-**XDPing**-Tool ist eine Befehlszeilenanwendung. Sie können damit das Prüfen auf häufige Konfigurationsprobleme in einer Linux VDA-Umgebung automatisieren.

Linux XDPing Tool installieren

XDPing wird beim Ausführen von ctxsetup.sh nicht installiert. Führen Sie den Befehl `sudo /opt/Citrix/VDA/bin/xdping` aus, um **XDPing** zu installieren.
Der Befehl erstellt auch die für **XDPing** erforderliche virtuelle **Python3**-Umgebung. Wenn keine virtuelle **Python3**-Umgebung erstellt wird, erstellen Sie sie manuell gemäß der Anleitung unter Erstellen einer virtuellen **Python3**-Umgebung.

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
```

Mit XDPing ausführbare Aufgaben

XDPing enthält die einzelne ausführbare Datei **xdping**, die über die Befehlsshell ausgeführt wird.

In der folgenden Tabelle werden die Aufgaben beschrieben, die mit den entsprechenden **XDPing**-Befehlen ausgeführt werden können:

Aufgabe	**XDPing**-Befehl	Bemerkungen
Befehlszeilenoptionen anzeigen	**sudo /opt/Citrix/VDA/bin/xdping -h**	–
Gesamte Testreihe ausführen	**sudo /opt/Citrix/VDA/bin/xdping** (**XDPing** ohne Befehlszeilenoption ausführen)	Das Linux-Tool **XDPing** führt mehr als 150 Einzeltests im System durch. Weitere Informationen finden Sie weiter unten in diesem Artikel unter Einzelne Tests.
Statusprüfung der VDA-Registrierung ausführen	**sudo /opt/Citrix/VDA/bin/xdping -a**	Weitere Informationen finden Sie weiter unten in diesem Artikel unter Umfang der Prüfungen zum Registrierungsstatus.
Wichtigste VDA-Daten sichern	**sudo /opt/Citrix/VDA/bin/xdping -b**	Weitere Informationen finden Sie weiter unten in diesem Artikel unter Backup und Vergleich von VDA-Daten.
Letzte beiden Kopien der VDA-Backupdaten vergleichen	**sudo /opt/Citrix/VDA/bin/xdping -diff**	Weitere Informationen finden Sie weiter unten in diesem Artikel unter Backup und Vergleich von VDA-Daten.
Zwei spezifische Kopien von VDA-Backupdaten vergleichen	**sudo /opt/Citrix/VDA/bin/xdping -diff=:**	Weitere Informationen finden Sie weiter unten in diesem Artikel unter Backup und Vergleich von VDA-Daten.

Aufgabe	**XDPing**-Befehl	Bemerkungen
Überprüfen der Umgebung, bevor Sie das Linux VDA-Paket installieren	**sudo /opt/Citrix/VDA/bin/xdping –preflight**	–
Nur bestimmte Testkategorien ausführen, z. B. Zeit-, Kerberos- und Datenbanktests	**sudo /opt/Citrix/VDA/bin/xdping -T time,kerberos,database**	–
Bestimmten Delivery Controller testen	**sudo /opt/Citrix/VDA/bin/xdping -d **	–

Einzelne Tests Das Linux **XDPing**-Tool führt mehr als 150 Einzeltests im System durch, die wie folgt kategorisiert werden können:

- Überprüfen, ob die Systemanforderungen für Linux VDA erfüllt sind.
- Identifizieren und Anzeigen von Maschineninformationen einschließlich der Linux-Distributionen.
- Überprüfen der Linux-Kernel-Kompatibilität.
- Überprüfen, ob bekannte Probleme mit der Linux-Distribution vorliegen, die die Funktion des Linux VDA beeinträchtigen können.
- Überprüfen des Security-Enhanced Linux (SELinux)-Modus und der Kompatibilität.
- Identifizieren von Netzwerkschnittstellen und Überprüfen der Netzwerkeinstellungen.
- Überprüfen der Speicherpartitionierung und des verfügbaren Speicherplatzes.
- Überprüfen der Konfiguration von Maschinenhost und Domänenname.
- Überprüfen der DNS-Konfiguration und Durchführen von Suchtests.
- Identifizieren zugrunde liegender Hypervisoren und Überprüfen der Konfiguration virtueller Maschinen. Unterstützung für:
  - Citrix Hypervisor
  - Microsoft Hyper-V
  - VMware vSphere
- Überprüfen der Zeiteinstellungen und der Betriebsbereitschaft der Netzwerkzeitsynchronisierung.
- Überprüfen, ob der PostgreSQL-Dienst ordnungsgemäß konfiguriert und betriebsbereit ist.
- Überprüfen, ob SQLite ordnungsgemäß konfiguriert und betriebsbereit ist.
- Überprüfen, ob die Firewall aktiviert ist und die erforderlichen Ports offen sind.
- Überprüfen der Kerberos-Konfiguration und Durchführen von Authentifizierungstests.
- Überprüfen der LDAP-Suchumgebung für die Gruppenrichtlinienengine.

- Überprüfen, ob die Active Directory-Integration ordnungsgemäß eingerichtet und die aktuelle Maschine mit der Domäne verbunden ist. Unterstützung für:
  - Samba Winbind
  - Dell Quest Authentication Services
  - Centrify DirectControl
  - SSSD
- Überprüfen der Integrität des Linux-Computerobjekts in Active Directory.
- Überprüfen der PAM-Konfiguration (Pluggable Authentication Module).
- Überprüfen des Coredump-Musters.
- Überprüfen, ob alle vom Linux VDA benötigten Pakete installiert sind.
- Identifizieren des Linux VDA-Pakets und Überprüfen der Integrität der Installation.
- Überprüfen der Integrität der PostgreSQL-Registrierungsdatenbank.
- Überprüfen, ob die Linux VDA-Dienste ordnungsgemäß konfiguriert und betriebsbereit sind.
- Überprüfen der Integrität der VDA- und HDX-Konfiguration.
- Test jedes konfigurierten Delivery Controllers, um zu prüfen, ob der Brokerdienst erreichbar und betriebsbereit ist und reagiert.
- Überprüfen, ob die Maschine bei der Delivery Controller-Farm registriert ist.
- Überprüfen des Zustands jeder aktiven oder getrennten HDX-Sitzung.
- Scannen von Protokolldateien auf Linux VDA-bezogene Fehler und Warnungen.
- Prüfen der Eignung der Version von Xorg.
- Überprüfen, ob die erforderlichen Abhängigkeiten installiert sind.

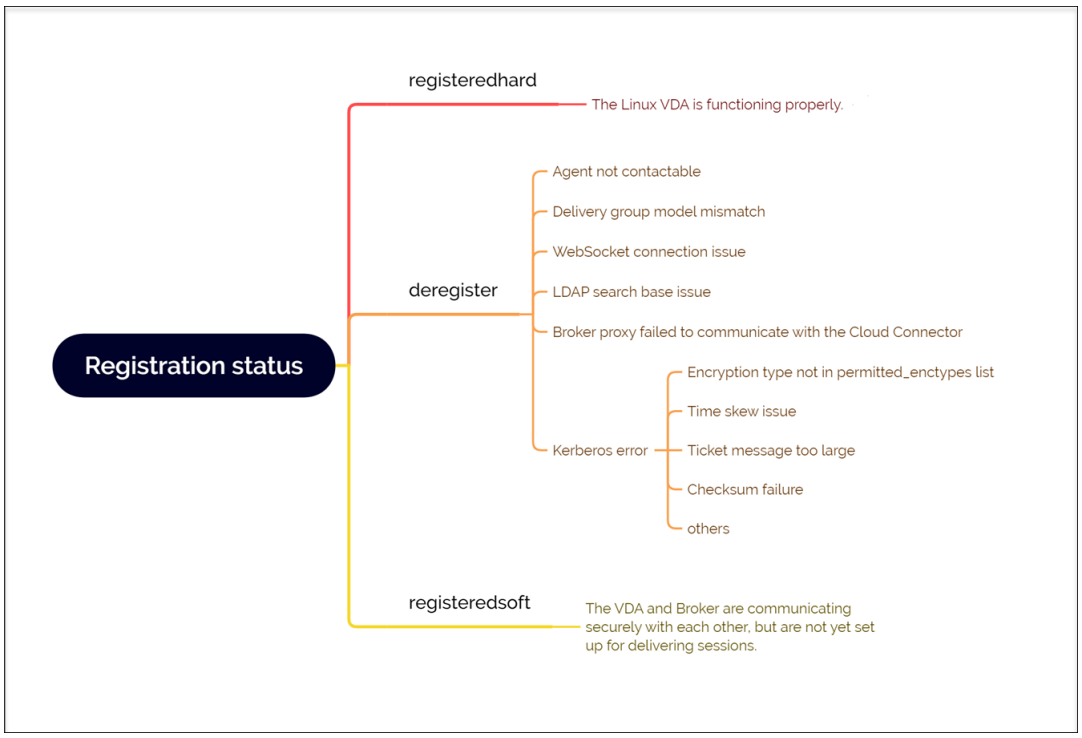
Beispielausgabe Dies ist die Beispielausgabe eines ausgeführten Kerberos-Tests:

```
sudo xdping -T kerberos

Root User ------------------------------------------------------------------
    User:         root
    EUID:         0
      Verify user is root                                                [Pass]

Kerberos -------------------------------------------------------------------
    Kerberos version: 5
      Verify Kerberos available                                          [Pass]
      Verify Kerberos version 5                                          [Pass]
    KRB5CCNAME:   [Not set]
                  Distro default FILE:/tmp/krb5cc_%{uid}
    KRB5CCNAME type: [Supported]
    KRB5CCNAME format: [Default]
      Verify KRB5CCNAME cache type                                       [Pass]
      Verify KRB5CCNAME format                                           [Pass]
    Configuration file: /etc/krb5.conf [Exists]
```



```
  Verify Kerberos configuration file found                          [Pass]
Keytab file:  /etc/krb5.keytab [Exists]
Default realm: XD2.LOCAL
Default realm KDCs: [NONE SPECIFIED]
Default realm domains: [NONE SPECIFIED]
DNS lookup realm: [Enabled]
DNS lookup KDC: [Enabled]
Weak crypto:  [Disabled]
Clock skew limit:  300 s
  Verify system keytab file exists                                  [Pass]
  Verify default realm set                                          [Pass]
  Verify default realm in upper-case                                [Pass]
  Verify default realm not EXAMPLE.COM                              [Pass]
  Verify default realm domain mappings                              [Pass]
  Verify default realm master KDC configured                        [Pass]
  Verify Kerberos weak crypto disabled                              [Pass]
  Verify Kerberos clock skew setting                                [Pass]
Default ccache: [Not set]
               Distro default FILE:/tmp/krb5cc_%{uid}
Default ccache type: [Supported]
Default ccache format: [Default]
  Verify default credential cache cache type                        [Pass]
  Verify default credential cache format                            [Pass]
UPN system key [MYVDA1$@          ]: [MISSING]
SPN system key [host/r                  l]: [Exists]
  Verify Kerberos system keys for UPN exist                        [ERROR]
  No system keys were found for the user principal name (UPN) of
  the machine account. For the Linux VDA to mutually authenticate
  with the Delivery Controller, the system keytab file must
  contain keys for both the UPN and host-based SPN of the machine
  account.

    Verify Kerberos system keys for SPN exist                        [Pass]
  Kerberos login: [FAILED AUTHENTICATION]
                  Keytab contains no suitable keys for MYVDA1$@
                  while getting initial credentials
    Verify KDC authentication                                       [ERROR]
    Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
    from the KDC authentication service for the machine account UPN
    MYVDA1$@          . Check that the Kerberos configuration is
    valid and the keys in the system keytab are current.


Summary ------------------------------------------------------------------
  The following tests did not pass:
    Verify Kerberos system keys for UPN exist                       [ERROR]
    Verify KDC authentication                                       [ERROR]
```

Umfang der Prüfungen zum Registrierungsstatus Das Linux-Tool **XDPing** bietet auch ein Analysemodul, mit dem Sie den VDA-Registrierungsstatus überprüfen und analysieren können. Der folgende Screenshot zeigt den Umfang der Prüfungen zum Registrierungsstatus an:



Backup und Vergleich von VDA-Daten Ab Linux VDA 2305 umfasst das Tool **XDPing** ein VDA-Backup-Modul. Mit diesem Modul können Sie die wichtigsten Daten eines VDAs, z. B. die Konfiguration, die Datenbank und die binären Berechtigungsdaten, jederzeit sichern. Sie können die wichtigsten Daten eines VDAs sichern, wenn dieser ordnungsgemäß ausgeführt wird. Falls der VDA später ausfällt, sichern Sie eine weitere Kopie der Daten und vergleichen Sie die beiden Datenkopien, um die Fehlerbehebung zu erleichtern. In der folgenden Tabelle werden VDA-Datenbackup und -Vergleich mit den **XDPing**-Befehlen beschrieben:

Aufgabe	**XDPing**-Befehl	Bemerkungen
Wichtigste VDA-Daten sichern	**sudo /opt/Citrix/VDA/bin/xdping -b**	Jedes Mal, wenn Sie den Befehl “backup”ausführen, wird eine Kopie der Backupdaten generiert und in einem Verzeichnis unter **/var/ctxbackup** gespeichert. Die Verzeichnisse mit den Backupdaten werden nach dem aktuellen Datum und der aktuellen Uhrzeit im Format **jjjj-mm-tt-hh_mm_ss** benannt, z. B. **2023-02-27-16_31_27**. Standardmäßig ist die maximale Anzahl von Backupdaten-Verzeichnissen 30 und das **XDPing**-Tool rotiert oder löscht alte Verzeichnisse, wenn die Anzahl überschritten wird. Führen Sie den folgenden Befehl aus, um die Nummer für die Verzeichnisrotation anzupassen: `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent\Backup"-t "REG_DWORD" -v " MaxDirRotationCount"-d "0x0000005"--force`
Letzte beiden Kopien der VDA-Backupdaten vergleichen	**sudo /opt/Citrix/VDA/bin/xdping -diff**	–
Zwei spezifische Kopien von VDA-Backupdaten vergleichen	**sudo /opt/Citrix/VDA/bin/xdping -diff=:**	–

Sonstige

February 9, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Unterstützung für die Citrix Workspace-App für HTML5
- Virtuelle **Python3**-Umgebung erstellen
- Integration von NIS in Active Directory
- **IPv6**
- LDAPS
- **Xauthority**

Unterstützung für die Citrix Workspace-App für HTML5

January 8, 2024

Sie können die Citrix Workspace-App für HTML5 verwenden, um in Linux auf virtuelle Apps und Desktops direkt zuzugreifen, ohne dass Ihr Client mit Citrix Gateway verbunden ist. Weitere Informationen über die Citrix Workspace-App für HTML5 finden Sie in der Citrix-Dokumentation.

Aktivieren des Features

Das Feature ist in der Standardeinstellung deaktiviert. Gehen Sie folgendermaßen vor, um es zu aktivieren:

1. Aktivieren Sie in Citrix StoreFront die Citrix Workspace-App für HTML5.

   Das ausführliche Verfahren finden Sie im Schritt 1 des Knowledge Center-Artikels CTX208163.

2. Aktivieren Sie WebSocket-Verbindungen.

   a) Legen Sie in Citrix Studio für die Richtlinie **WebSockets-Verbindungen** die Einstellung **Zugelassen** fest.

   Sie können auch die anderen WebSocket-Richtlinien festlegen. Eine vollständige Liste der WebSocket-Richtlinien finden Sie unter WebSockets-Richtlinieneinstellungen.

   b) Starten Sie auf dem VDA den `ctxvda`-Dienst und den `ctxhdx`-Dienst neu –in dieser Reihenfolge –damit die Einstellungen wirksam werden.

c) Führen Sie auf dem VDA den folgenden Befehl aus, um zu überprüfen, ob der WebSocket-Listener ausgeführt wird.

```
netstat -an | grep 8008
```

Wenn der WebSocket-Listener ausgeführt wird, ähnelt die Befehlsausgabe der folgenden:

```
tcp 0 0 :::8008 :::* LISTEN
```

Hinweis: Sie können auch die TLS-Verschlüsselung aktivieren, um WebSocket-Verbindungen zu sichern. Weitere Informationen zum Aktivieren der TLS-Verschlüsselung finden Sie unter Schützen von Benutzersitzungen mit TLS.

Virtuelle Python3-Umgebung erstellen

January 8, 2024

Beim Verbinden mit dem Netzwerk können Sie den Befehl `sudo /opt/Citrix/VDA/bin/xdping` oder `/opt/Citrix/VDA/sbin/enable_ldaps.sh` ausführen, um eine virtuelle **Python3**-Umgebung zu erstellen. Wird durch die Befehle keine virtuelle **Python3**-Umgebung erstellt, können Sie sie selbst ohne Netzwerkverbindung manuell erstellen. In diesem Artikel werden die Voraussetzungen und Schritte zum Erstellen einer virtuellen **Python3**-Umgebung ohne Netzwerkverbindung beschrieben.

Voraussetzungen

- Sie müssen über Administratorrechte verfügen, um auf das Verzeichnis `/opt/Citrix/VDA/sbin/ctxpython3` zugreifen zu können.
- Die WHL-Dateien von `Python3`-Paketen sind vorhanden. Sie finden die WHL-Dateien zum Download unter https://pypi.org/.

Virtuelle Python3-Umgebung erstellen

Führen Sie die folgenden Schritte aus, um eine virtuelle **Python3**-Umgebung zu erstellen:

1. Installieren Sie **Python3**-Abhängigkeiten.

   Amazon Linux 2:

   ```
   yum -y install python3 python3-devel krb5-devel gcc
   <!--NeedCopy-->
   ```


RHEL und Rocky Linux:

```
yum -y install python3-devel krb5-devel gcc
<!--NeedCopy-->
```

> **Hinweis:**
>
> Möglicherweise müssen Sie ein bestimmtes Repository aktivieren, um einige Abhängigkeiten zu installieren. Für RHEL 7 führen Sie den Befehl `subscription-manager repos --enable rhel-7-server-optional-rpms` aus. Für RHEL 8 führen Sie den Befehl `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms` aus.

Debian, Ubuntu:

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
<!--NeedCopy-->
```

SUSE:

```
zypper -n install lsb-release python3-devel python3-setuptools krb5-devel gcc libffi-devel libopenssl-devel
<!--NeedCopy-->
```

2. Erstellen Sie eine virtuelle **Python3**-Umgebung.

> **Hinweis:**
>
> Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des Pip-Tools auftreten können, sollten Sie die folgenden vertrauenswürdigen Hosts zur Datei /etc/pip.conf hinzufügen:
>
> ```
> [global]
> trusted-host =
> pypi.org
> files.pythonhosted.org
> ```

Amazon Linux 2, Debian, RHEL, Rocky Linux, Ubuntu:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

SUSE:

```
sudo ln -s /usr/lib/mit/bin/krb5-config /usr/bin/krb5-config

export PATH=$PATH:/usr/lib/mit/bin:/usr/lib/mit/sbin

```



```
sudo mkdir -p /usr/lib/mit/include/gssapi/

sudo ln -s /usr/include/gssapi/gssapi_ext.h/usr/lib/mit/include/
    gssapi/gssapi_ext.h

sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
<!--NeedCopy-->
```

3. Installieren Sie LDAPS-Abhängigkeiten.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
    upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
    cffi==1.15.0 cryptography==36.0.2 decorator==5.1.1 gssapi
    ==1.7.3 ldap3==2.9.1 pyasn1==0.4.8 pycparser==2.21 six==1.16.0
<!--NeedCopy-->
```

4. Installieren Sie **XDPing**-Abhängigkeiten.

```
sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install --
    upgrade pip==21.3.1

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install
    asn1crypto==1.5.1 cffi==1.15.0 cryptography==36.0.2 decorator
    ==5.1.1 gssapi==1.7.3 ldap3==2.9.1 netifaces==0.11.0 packaging
    ==21.3 pg8000==1.26.0 psutil==5.9.0 pyasn1==0.4.8 pycparser
    ==2.21 pyparsing==3.0.8 scramp==1.4.1 six==1.16.0 termcolor
    ==1.1.0

sudo /opt/Citrix/VDA/sbin/ctxpython3/bin/python3 -m pip install /
    opt/Citrix/VDA/sbin/ctxpython3/packages/xdping-*.whl
<!--NeedCopy-->
```

Integration von NIS in Active Directory

January 8, 2024

In diesem Artikel wird beschrieben, wie NIS in Windows Active Directory (AD) auf dem Linux VDA über SSSD integriert wird. Der Linux VDA ist eine Komponente von Citrix Virtual Apps and Desktops. Daher passt er eng in die Windows AD-Umgebung.

Zur Verwendung von NIS statt AD als UID- und GID-Anbieter müssen die Kontoinformationen (Benutzername-/Kennwortkombinationen) in AD und NIS identisch sein.

> **Hinweis:**
>
> Die Authentifizierung findet weiterhin auf dem Active Directory-Server statt. NIS+ wird nicht unterstützt. Wenn Sie NIS als UID- und GID-Anbieter verwenden, werden die POSIX-Attribute des Windows-Servers nicht mehr verwendet.
>
> **Tipp:**
>
> Diese Methode ist eine veraltete Methode zum Bereitstellen des Linux VDA und wird nur in besonderen Fällen verwendet Folgen Sie für eine RHEL/CentOS-Distribution den Anweisungen unter Linux VDA manuell auf Amazon Linux 2, CentOS, RHEL und Rocky Linux installieren. Folgen Sie für eine Ubuntu-Distribution den Anweisungen unter Linux VDA manuell auf Ubuntu installieren.

Was ist SSSD?

SSSD ist ein System-Daemon. Seine primäre Funktion ist die Bereitstellung des Zugriffs zur Identifizierung und Authentifizierung von Remoteressourcen über ein gemeinsames Framework, das Zwischenspeicherung und Offlineunterstützung für das System liefert. Es bietet PAM- und NSS-Module und soll künftig D-BUS-Schnittstellen für erweiterte Benutzerinformationen unterstützen. Es bietet zudem eine bessere Datenbank für lokale Benutzerkonten und erweiterte Benutzerdaten.

Integrieren von NIS in Active Directory

Führen Sie die folgenden Schritte aus, um NIS in AD zu integrieren:

Schritt 1: Hinzufügen von Linux VDA als NIS-Client

Konfigurieren Sie den NIS-Client:

```
yum –y install ypbind rpcbind oddjob-mkhomedir
<!--NeedCopy-->
```

Legen Sie die NIS-Domäne fest:

```
ypdomainname nis.domain
echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
<!--NeedCopy-->
```

Fügen Sie die IP-Adresse des NIS-Servers/-Clients zu **/etc/hosts** hinzu:

```
{ NIS server IP address }    server.nis.domain nis.domain
```

Konfigurieren Sie NIS über `authconfig`:

```
sudo authconfig --enablenis --nisdomain=nis.domain --nisserver=server.
    nis.domain --enablemkhomedir --update
<!--NeedCopy-->
```


nis.domain ist der Name der NIS-Serverdomäne. **server.nis.domain** ist der Hostname des NIS-Servers (bzw. dessen IP-Adresse).

Konfigurieren Sie die NIS-Dienste:

```
sudo systemctl start rpcbind ypbind

sudo systemctl enable rpcbind ypbind
<!--NeedCopy-->
```

Vergewissern Sie sich, dass die NIS-Konfiguration richtig ist:

```
ypwhich
<!--NeedCopy-->
```

Prüfen Sie, ob die Kontoinformationen über den NIS-Server zur Verfügung stehen:

```
getent passwd nisaccount
<!--NeedCopy-->
```

> **Hinweis:**
>
> **nisaccount**ist das tatsächliche NIS-Konto auf dem NIS-Server. Stellen Sie sicher, dass die UID, GID, das Homeverzeichnis und die Login-Shell ordnungsgemäß konfiguriert sind.

Schritt 2: Beitritt zur Domäne und Erstellen einer Hostschlüsseltabelle mit Samba

SSSD bietet keine AD-Clientfunktionen für den Domänenbeitritt und die Verwaltung der Systemschlüsseltabelle. Zum Ausführen dieser Funktionen gibt es mehrere Methoden:

- `adcli`
- `realmd`
- `Winbind`
- `Samba`

Die Informationen in diesem Abschnitt basieren auf der Verwendung von Samba. Informationen über `realmd` finden Sie in der Anbieterdokumentation zu RHEL oder CentOS. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

Treten Sie der Domäne bei und erstellen Sie eine Hostschlüsseltabelle mit Samba:

Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

- /etc/krb5.conf
- /etc/samba/smb.conf:

Konfigurieren Sie die Maschine für die Samba- und Kerberos-Authentifizierung:


```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=
    REALM --krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
<!--NeedCopy-->
```

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **domain** ist der NetBIOS-Name der Domäne.

Wenn eine DNS-basierte Suche nach dem KDC-Server und -Bereichsnamen erforderlich ist, fügen Sie dem vorherigen Befehl die folgenden beiden Optionen hinzu:

```
--enablekrb5kdcdns --enablekrb5realmdns
```

Öffnen Sie die Datei **/etc/samba/smb.conf** und fügen Sie im Abschnitt **[Global]** nach dem von dem Tool **authconfig** erstellten Abschnitt die folgenden Einträge hinzu:

```
kerberos method = secrets and keytab
winbind offline logon = no
```

Zum Beitritt zur Windows-Domäne muss der Domänencontroller erreichbar sein und Sie müssen ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zu der Domäne haben:

```
sudo net ads join REALM -U user
<!--NeedCopy-->
```

REALM ist der Kerberos-Bereichsname in Großbuchstaben und **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Domäne.

Schritt 3: Einrichten von SSSD

Die Einrichtung von SSSD umfasst die folgenden Schritte:

- Pakete **sssd-ad** und **sssd-proxy** auf der Linux-Clientmaschine installieren.
- Konfiguration verschiedener Dateien (z. B. von **sssd.conf**) ändern.
- Dienst **sssd** starten.

/etc/sssd/sssd.conf Muster einer **sssd.conf**-Konfiguration (weitere Optionen können bei Bedarf hinzugefügt werden):

```
[sssd]
config_file_version = 2
domains = EXAMPLE
services = nss, pam

[domain/EXAMPLE]
# Uncomment if you need offline logins
# cache_credentials = true
```



```
re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@
    (?P<domain>.+$))|(^(?P<name>[^@\\]+)$))
id_provider = proxy
proxy_lib_name = nis
auth_provider = ad
access_provider = ad

# Should be specified as the 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
<!--NeedCopy-->
```

Ersetzen Sie **ad.domain.com**, **server.ad.example.com** durch den jeweils gültigen Wert. Weitere Informationen finden Sie unter **sssd-ad**(5) - Linux man page.

Legen Sie Dateieigentümer und Berechtigungen für **sssd.conf** fest:

```
chown root:root /etc/sssd/sssd.conf
chmod 0600 /etc/sssd/sssd.conf
restorecon /etc/sssd/sssd.conf
```

Schritt 4: Konfigurieren von NSS/PAM

RHEL/CentOS:

Aktivieren Sie SSSD mit **authconfig**. Installieren Sie **oddjob-mkhomedir**, damit die Erstellung des Homeverzeichnisses mit SELinux kompatibel ist:

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update

sudo systemctl start sssd

sudo systemctl enable sssd
<!--NeedCopy-->
```


> **Tipp:**
>
> Berücksichtigen Sie bei der Konfiguration der Linux VDA-Einstellungen, dass es für SSSD keine besonderen Einstellungen für den Linux VDA-Client gibt. Verwenden Sie als weitere Lösung im Skript **ctxsetup.sh** den Standardwert.

Schritt 5: Überprüfen der Kerberos-Konfiguration

Um sicherzustellen, dass Kerberos zur Verwendung mit dem Linux VDA ordnungsgemäß konfiguriert ist, überprüfen Sie, ob die Systemdatei für die **Schlüsseltabelle** erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
<!--NeedCopy-->
```

Mit diesem Befehl wird die Liste der Schlüssel angezeigt, die für die verschiedenen Kombinationen aus Prinzipalnamen und Verschlüsselungssammlungen verfügbar sind. Führen Sie den Kerberos-Befehl **kinit** aus, um die Maschine mit dem Domänencontroller zu authentifizieren, die diese Schlüssel verwendet:

```
sudo kinit  – k MACHINE$@REALM
<!--NeedCopy-->
```

Maschinen- und Bereichsname müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss durch einen umgekehrten Schrägstrich (\) geschützt werden, um das Ersetzen in der Shell zu verhindern. In einigen Umgebungen sind DNS-Domänenname und Kerberos-Bereichsname unterschiedlich. Stellen Sie sicher, dass der Bereichsname verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Stellen Sie mit folgendem Befehl sicher, dass das TGT-Ticket für das Maschinenkonto zwischengespeichert wurde:

```
sudo klist -ke
<!--NeedCopy-->
```

Schritt 6: Überprüfen der Benutzerauthentifizierung

Prüfen Sie mit dem Befehl **getent**, ob das Anmeldeformat unterstützt wird und ob NSS funktioniert:

```
sudo getent passwd DOMAIN\username
<!--NeedCopy-->
```

Der Parameter **DOMAIN** ist die kurze Version des Domänennamens. Wenn ein anderes Anmeldeformat von erforderlich ist, überprüfen Sie dies zunächst mit dem Befehl **getent**.

Unterstützte Anmeldeformate:

- Down-Level-Anmeldename: `DOMAIN\username`
- UPN: `username@domain.com`
- NetBIOS-Suffix-Format: `username@DOMAIN`

Um sich zu vergewissern, dass das SSSD-PAM-Modul fehlerfrei konfiguriert wurde, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
sudo ssh localhost  – l DOMAIN\username

id -u
<!--NeedCopy-->
```

Stellen Sie sicher, dass eine entsprechende Cachedatei mit Kerberos-Anmeldeinformationen für die mit dem Befehl **uid** zurückgegebene UID erstellt wurde:

```
ls /tmp/krb5cc_{
 uid }

<!--NeedCopy-->
```

Stellen Sie sicher, dass die Tickets im Kerberos-Anmeldeinformationscache des Benutzers gültig und nicht abgelaufen sind:

```
klist
<!--NeedCopy-->
```

IPv6

January 8, 2024

Der Linux VDA unterstützt **IPv6** ebenso wie Citrix Virtual Apps and Desktops. Beachten Sie bei der Verwendung dieses Features Folgendes:

- Für Umgebungen mit dualem Stapel wird **IPv4** verwendet, es sei denn, **IPv6** wurde explizit aktiviert.
- Wenn **IPv6** in einer **IPv4**-Umgebung aktiviert ist, funktioniert der Linux VDA nicht.

> **Wichtig:**
>
> - Die gesamte Netzwerkumgebung muss **IPv6** sein, nicht nur der Linux VDA.
> - **Centrify** unterstützt reines **IPv6** nicht.

Bei der Installation des Linux VDA ist für **IPv6** keine spezielle Einrichtung erforderlich.

Konfigurieren von IPv6 für den Linux VDA

Bevor Sie die Konfiguration für den Linux VDA ändern, stellen Sie sicher, dass die virtuelle Linux-Maschine zuvor in einem **IPv6**-Netzwerk funktioniert hat. Für die **IPv6**-Konfiguration müssen zwei Registrierungsschlüssel festgelegt werden:

```
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
   OnlyUseIPv6ControllerRegistration"
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
   ControllerRegistrationIPv6Netmask"
<!--NeedCopy-->
```

OnlyUseIPv6ControllerRegistration muss auf 1 festgelegt werden, damit **IPv6** auf dem Linux VDA aktiviert ist:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Policies\
   Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "
   OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
<!--NeedCopy-->
```

Wenn der Linux VDA mehrere Netzwerkschnittstellen hat, kann mit **ControllerRegistrationIPv6Netmask** angegeben werden, 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
<!--NeedCopy-->
```

Ersetzen Sie **{IPv6 netmask}** mit der echten Netzwerkmaske (z. B. 2000::/64).

Weitere Informationen zur **IPv6**-Bereitstellung in Citrix Virtual Apps and Desktops finden Sie unter **IPv4/IPv6-Unterstützung**.

Problembehandlung

Überprüfen Sie die grundlegende **IPv6**-Netzwerkumgebung und prüfen Sie mit ping6, ob AD und Delivery Controller erreichbar sind.

LDAPS

January 8, 2024

LDAPS ist die sichere Version des Lightweight Directory Access Protocol (LDAP), wobei die LDAP-Kommunikation mit TLS/SSL verschlüsselt wird.

Standardmäßig wird die LDAP-Kommunikation zwischen Client- und Serveranwendungen nicht verschlüsselt. Mit LDAPS schützen Sie den Inhalt von LDAP-Abfragen zwischen Linux VDA- und LDAP-Server.

Die folgenden Linux VDA-Komponenten benötigen LDAPS:

- Brokeragent: Registrierung des Linux VDA bei einem Delivery Controller
- Richtliniendienst: Richtlinienbewertung

Die Konfiguration von LDAPS umfasst Folgendes:

- Aktivieren von LDAPS auf dem Active Directory (AD)-/LDAP-Server
- Exportieren der Stammzertifizierungsstelle für Clients
- Aktivieren/Deaktivieren von LDAPS auf dem Linux VDA
- Konfigurieren von LDAPS für Drittanbieter-Plattformen
- SSSD konfigurieren
- Konfigurieren von Winbind
- Konfigurieren von Centrify
- Konfigurieren von Quest

> **Hinweis:**
>
> Mit folgendem Befehl können Sie einen Überwachungszyklus für die LDAP-Server festlegen. Der Standardwert ist 15 Minuten. Stellen Sie den Wert auf mindestens 10 Minuten ein.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent" -v "ListOfLDAPServersMonitorPeroid" -t "
     REG_DWORD" -d "0x0000000f" --force
2 <!--NeedCopy-->
```

Aktivieren von LDAPS auf dem AD-/LDAP-Server

Sie können LDAP über SSL (LDAPS) aktivieren, indem Sie ein ordnungsgemäß formatiertes Zertifikat von einer Microsoft Zertifizierungsstelle (ZS) oder einer anderen Zertifizierungsstelle installieren.

> **Tipp:**
>
> LDAPS wird automatisch aktiviert, wenn Sie eine unternehmenseigene Stammzertifizierungsstelle auf einem Domänencontroller installieren.

Weitere Informationen zum Installieren des Zertifikats und Verifizieren der LDAPS-Verbindung finden Sie unter How to enable LDAP over SSL with a third-party certification authority.

Wenn Sie eine Zertifikatauthentifizierungshierachie mit mehreren Ebenen verwenden, besitzen Sie nicht automatisch das geeignete Zertifikat für die LDAPS-Authentifizierung auf dem Domänencontroller.

Informationen zum Aktivieren von LDAPS für Domänencontroller über eine Zertifikatauthentifizierungshierachie mit mehreren Ebenen finden Sie im Artikel LDAP over SSL (LDAPS) Certificate.

Aktivieren der Stammzertifizierungsstelle für Clients

Der Client muss ein Zertifikat einer Zertifizierungsstelle verwenden, dem der LDAP-Server vertraut. Importieren Sie das Stammzertifizierungsstellenzertifikat in einen vertrauenswürdigen Schlüsselspeicher, um die LDAPS-Authentifizierung für den Client zu aktivieren.

Weitere Informationen zum Exportieren der Stammzertifizierungsstelle finden Sie unter How to export Root Certification Authority Certificate auf der Supportwebsite von Microsoft.

Aktivieren oder Deaktivieren von LDAPS auf dem Linux VDA

Zum Aktivieren oder Deaktivieren von LDAPS auf dem Linux VDA führen Sie das folgende Skript aus (Sie müssen als Administrator angemeldet sein):

Die Syntax für diesen Befehl enthält Folgendes:

- Aktivieren von LDAP über SSL/TLS mit dem bereitgestellten Stammzertifizierungsstellenzertifikat:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
<!--NeedCopy-->
```

- Aktivieren von LDAP über SSL/TLS mit Kanalbindung:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das Stammzertifizierungsstellenzertifikat für die Kanalbindung muss im PEM-Format vorliegen. Wenn durch Aktivieren von LDAPS keine virtuelle **Python3**-Umgebung erstellt wird, erstellen Sie sie gemäß den Anweisungen unter Erstellen einer virtuellen **Python3**-Umgebung manuell.
>
> Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des Pip-Tools auftreten können, sollten Sie die folgenden vertrauenswürdigen Hosts zur Datei /etc/pip.conf hinzufügen:
> `[global]`


```
trusted-host =
pypi.org
files.pythonhosted.org
```

- Fallback auf LDAP ohne SSL/TLS

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
<!--NeedCopy-->
```

Der Java-Schlüsselspeicher für LDAPS ist in **/etc/xdl/.keystore**. Unter anderem sind folgende Registrierungsschlüssel betroffen:

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore

HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
<!--NeedCopy-->
```

Konfigurieren von LDAPS für Drittanbieter-Plattformen

Neben Linux VDA-Komponenten gibt es verschiedene Softwarekomponenten von Drittanbietern, die mit dem Linux VDA verbunden sind und ebenfalls sicheres LDAP erfordern, z. B. SSSD, Winbind, Centrify und Quest. In den folgenden Abschnitten wird beschrieben, wie Sie sicheres LDAP mit LDAPS, STARTTLS oder SASL Sign and Seal konfigurieren.

> **Tipp:**
>
> Nicht alle diese Softwarekomponenten nutzen den SSL-Port 636 für sicheres LDAP. Außerdem kann LDAPS (LDAP über SSL auf Port 636) meist nicht gemeinsam mit STARTTLS auf Port 389 verwendet werden.

SSSD

Konfigurieren Sie den sicheren LDAP-Datenverkehr mit SSSD auf Port 636 oder Port 389 entsprechend den Optionen. Weitere Informationen finden Sie hier: SSSD LDAP Linux man page.

Winbind

Die Winbind LDAP-Abfrage verwendet die ADS-Methode. Winbind unterstützt nur die StartTLS-Methode auf Port 389. Betroffene Konfigurationsdateien sind **/etc/samba/smb.conf** und **/etc/openl-**

dap/ldap.conf (für Amazon Linux 2, RHEL, Rocky Linux, CentOS und SUSE) oder **/etc/ldap/ldap.conf** (für Debian und Ubuntu). Nehmen Sie an den Dateien die folgenden Änderungen vor:

- smb.conf

  ```
  ldap ssl = start tls
  ldap ssl ads = yes
  client ldap sasl wrapping = plain
  ```

- ldap.conf

  ```
  TLS_REQCERT never
  ```

Alternativ können Sie sicheres LDAP mit SASL GSSAPI Sign and Seal konfigurieren; es kann jedoch nicht neben TLS/SSL existieren. Um SASL-Verschlüsselung zu verwenden, ändern Sie die Konfiguration für **smb.conf**:

```
ldap ssl = off
ldap ssl ads = no
client ldap sasl wrapping = seal
```

Centrify

Centrify unterstützt LDAPS auf Port 636 nicht. Es bietet jedoch sichere Verschlüsselung auf Port 389. Weitere Informationen finden Sie auf der Website von Centrify.

Quest

Quest Authentication Services unterstützt LDAPS auf Port 636 nicht, bietet jedoch mit einer anderen Methode sichere Verschlüsselung auf Port 389.

Problembehandlung

Folgende Probleme können bei der Verwendung dieses Features auftreten:

- **Verfügbarkeit des LDAPS-Diensts**

  Stellen Sie sicher, dass die LDAPS-Verbindung auf dem AD/LDAP-Server verfügbar ist. Der Port ist standardmäßig 636.

- **Registrierung des Linux VDA schlägt fehl, wenn LDAPS aktiviert ist**

  Überprüfen Sie, ob der LDAP-Server und die Ports richtig konfiguriert sind. Überprüfen Sie zuerst das Stammzertifizierungsstellenzertifikat und stellen Sie sicher, dass es mit dem AD/LDAP-Server übereinstimmt.

- **Versehentlich vorgenommene falsche Registrierungsänderung**

  Wenn Sie die LDAPS-bezogenen Schlüssel versehentlich ohne **enable_ldaps.sh** aktualisiert haben, wird u. U. die Abhängigkeit der LDAPS-Komponenten unterbrochen.

- **LDAP-Datenverkehr wird nicht durch SSL/TLS von Wireshark oder anderen Netzwerküberwachungs-Tools verschlüsselt.**

  LDAPS ist standardmäßig deaktiviert. Führen Sie **/opt/Citrix/VDA/sbin/enable_ldaps.sh** aus, um die Aktivierung zu erzwingen.

- **Kein LDAPS-Datenverkehr von Wireshark oder einem anderen Netzwerküberwachungstool**

  Bei der Linux VDA-Registrierung und Gruppenrichtlinienbewertung erfolgt LDAP/LDAPS-Datenverkehr.

- **LDAPS-Verfügbarkeit konnte durch Ausführen von "ldp connect"auf dem AD-Server nicht verifiziert werden**

  Verwenden Sie den AD FQDN statt der IP-Adresse.

- **Stammzertifizierungsstellenzertifikat konnte nicht durch Ausführen des Skripts /opt/Citrix/VDA/sbin/enable_ldaps.sh importiert werden**

  Geben Sie den vollständigen Pfad des Zertifizierungsstellenzertifikats an und prüfen Sie den Typ des Stammzertifizierungsstellenzertifikats. Er sollte mit den meisten unterstützten Java Keytool-Typen kompatibel sein. Wenn er nicht in der Liste der unterstützten Typen enthalten ist, können Sie ihn konvertieren. Wir empfehlen das mit base64 verschlüsselte PEM-Format, wenn ein Problem mit dem Zertifikatformat auftritt.

- **Stammzertifizierungsstellenzertifikat wird mit Keytool -list nicht angezeigt**

  Wenn Sie LDAPS durch Ausführen von `/opt/Citrix/VDA/sbin/enable_ldaps.sh` aktivieren, wird das Zertifikat nach "/etc/xdl/.keystore"importiert und ein Kennwort wird zum Schutz des Schlüsselspeichers eingerichtet. Wenn Sie das Kennwort vergessen, können Sie das Skript erneut ausführen und einen Schlüsselspeicher erstellen.

Xauthority

January 8, 2024

Der Linux VDA unterstützt Umgebungen, in denen X11-Anzeigefunktionalität (einschließlich `xterm` und `gvim`) für interaktives Remoting verwendet wird. Dieses Feature bietet einen Sicherheitsmechanismus für die sichere Kommunikation zwischen XClient und XServer.

Es gibt zwei Methoden zum Sicherstellen der Berechtigung für die sichere Kommunikation:

- **Xhost**. Standardmäßig erlaubt Xhost nur die Kommunikation zwischen dem XClient auf Localhost und XServer. Wenn Sie den Zugriff eines Remote-XClient auf XServer zulassen, muss mit dem Xhost-Befehl die Berechtigung für die spezifische Maschine gewährt werden. Alternativ dazu können Sie auch **xhost +** verwenden, um damit alle XClient-Instanzen eine Verbindung zu XServer herstellen können.
- **Xauthority**. Die `.Xauthority`-Datei befindet sich im Homeverzeichnis jedes Benutzers. Sie wird zum Speichern von Anmeldeinformationen in Cookies verwendet, die von xauth für die Authentifizierung von XServer verwendet werden. Wenn eine XServer-Instanz (Xorg) gestartet wird, werden Verbindungen mit dem Cookie bei der spezifischen Anzeige authentifiziert.

Funktionsweise

Wenn Xorg gestartet wird, wird eine `.Xauthority`-Datei an Xorg übergeben. Diese `.Xauthority` -Datei enthält folgende Elemente:

- Anzeigenummer
- Remoteanfrageprotokoll
- Cookienummer

Sie können diese Datei mit dem Befehl `xauth` durchsuchen. Beispiel:

```
# xauth -f ~/.Xauthority

# > list

# > us01msip06:107  MIT-MAGIC-COOKIE-1
     fb228d1b695729242616c5908f11624b
<!--NeedCopy-->
```

Wenn **XClient** eine Remoteverbindung mit Xorg herstellt, müssen zwei Voraussetzungen erfüllt sein:

- Die Umgebungsvariable **DISPLAY** muss auf den Remote-XServer festgelegt sein.
- Rufen Sie die `.Xauthority`-Datei ab, die eine der Cookienummern in Xorg enthält.

Xauthority konfigurieren

Um **Xauthority** im Linux VDA für X11-Remoteanzeige zu aktivieren, müssen Sie die zwei folgenden Registrierungsschlüssel erstellen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "
    XauthEnabled" -d "0x00000001" --force

```



```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v "ListenTCP"
     -d "0x00000001" --force
<!--NeedCopy-->
```

Übergeben Sie die `.Xauthority`-Datei nach dem Aktivieren von **Xauthority** manuell oder durch Bereitstellen eines freigegebenen Homeverzeichnisses an den **XClient**:

- Manuelle Übergabe der `.Xauthority`-Datei an den XClient

  Nach dem Start einer ICA-Sitzung generiert der Linux VDA die `.Xauthority`-Datei für den XClient und speichert die Datei im Homeverzeichnis des Anmeldebenutzers. Sie können die `.Xauthority`-Datei auf die remote XClient-Maschine kopieren und die Umgebungsvariablen **DISPLAY** und **XAUTHORITY** festlegen. `DISPLAY` ist die in der `.Xauthority`-Datei gespeicherte Anzeigenummer und `XAUTHORITY` ist der Dateipfad von **Xauthority**. Ein Beispiel ist der folgende Befehl:

  ```
  export DISPLAY={
  Display number stored in the Xauthority file }


  export XAUTHORITY={
  the file path of .Xauthority }

  <!--NeedCopy-->
  ```

  > **Hinweis:**
  >
  > Wenn die Umgebungsvariable **XAUTHORITY** nicht festgelegt ist, wird standardmäßig die Datei `~/.Xauthority` verwendet.

- Übergabe der `.Xauthority`-Datei an den XClient durch Bereitstellen eines freigegebenen Homeverzeichnisses

  Eine bequeme Methode ist das Bereitstellen eines freigegebenen Homeverzeichnisses für den Benutzer, der sich anmeldet. Wenn der Linux VDA eine ICA-Sitzung startet, wird die `.Xauthority`-Datei im Homeverzeichnis des Anmeldebenutzers erstellt. Wenn dieses Homeverzeichnis für den XClient freigegeben ist, muss der Benutzer diese `.Xauthority`-Datei nicht manuell an den XClient übergeben. Wenn die Umgebungsvariablen **DISPLAY** und **XAUTHORITY** richtig festgelegt sind, wird die GUI automatisch auf dem XServer-Desktop angezeigt.

Problembehandlung

Wenn **Xauthority** nicht funktioniert, folgen Sie diesen Anleitungen zur Problembehandlung:

1. Rufen Sie als Administrator mit Root-Privilegien alle Xorg-Cookies ab:

   ```
   ps aux | grep -i xorg
   <!--NeedCopy-->
   ```

   Mit diesem Befehl wird der Xorg-Prozess angezeigt sowie die Parameter, die beim Starten an Xorg übergeben wurden. Ein weiterer Parameter zeigt an, welche `.Xauthority`-Datei verwendet wurde. Beispiel:

   ```
   /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

   Zeigen Sie Cookies mit dem Befehl **Xauth** an:

   ```
   Xauth -f /var/xdl/xauth/.Xauthority110
   <!--NeedCopy-->
   ```

2. Zeigen Sie mit dem Befehl `Xauth` die in `~/.Xauthority` enthaltenen Cookies an. Für eine bestimmte Anzeigenummer müssen die angezeigten Cookies in den `.Xauthority`-Dateien von Xorg und XClient dieselben sein.

3. Wenn die Cookies dieselben sind, überprüfen Sie den Zugriff auf den Remoteanzeigeport mit der IP-Adresse des Linux VDA und der Anzeigenummer des veröffentlichten Desktops.

   Führen Sie zum Beispiel den folgenden Befehl auf der XClient-Maschine aus:

   ```
   telnet 10.158.11.11 6160
   <!--NeedCopy-->
   ```

   Die Portnummer ist die Summe von 6000 + <display number>.

   Wenn dieser Telnet-Vorgang fehlschlägt, wird die Anfrage möglicherweise von der Firewall blockiert.

Authentifizierung

January 8, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Authentifizierung mit Azure Active Directory
- Single-Sign-On-Authentifizierung per Double-Hop
- Verbundauthentifizierungsdienst
- Authentifizierung ohne Single Sign-On

- Smartcards
- Zugriff durch nicht authentifizierte (anonyme) Benutzer

Authentifizierung mit Azure Active Directory

February 9, 2024

> **Hinweis:**
>
> Dieses Feature ist nur für von Azure gehostete VDAs verfügbar.

Je nach Bedarf können Sie zwei Arten von Linux-VDAs in Azure bereitstellen:

- Mit Azure AD DS verbundene VMs. Die VMs sind mit einer verwalteten Domäne von Azure Active Directory (AAD) Domain Services (DS) verbunden. Benutzer melden sich mit ihren Domänenanmeldeinformationen bei den VMs an.
- Nicht-domänengebundene VDAs. Die VMs werden in den AAD-Identitätsdienst integriert, um die Benutzerauthentifizierung bereitzustellen. Benutzer melden sich mit ihren AAD-Anmeldeinformationen bei den VMs an.

Weitere Informationen zu AAD DS und AAD finden Sie in diesem Microsoft-Artikel.

In diesem Artikel erfahren Sie, wie Sie den AAD-Identitätsdienst auf nicht in Domänen eingebundenen VDAs aktivieren und konfigurieren.

Unterstützte Distributionen

- Ubuntu 22.04, 20.04
- RHEL 8.8, 8.6, 7.9
- SUSE 15.4

Weitere Informationen finden Sie in diesem Microsoft-Artikel.

Bekannte Probleme und Workarounds

Unter RHEL 7.9 kann das PAM (Pluggable Authentication Module) `pam_loginuid.so` nach der AAD-Benutzerauthentifizierung `loginuid` nicht festlegen. Dieses Problem hindert AAD-Benutzer am Zugriff auf VDA-Sitzungen.

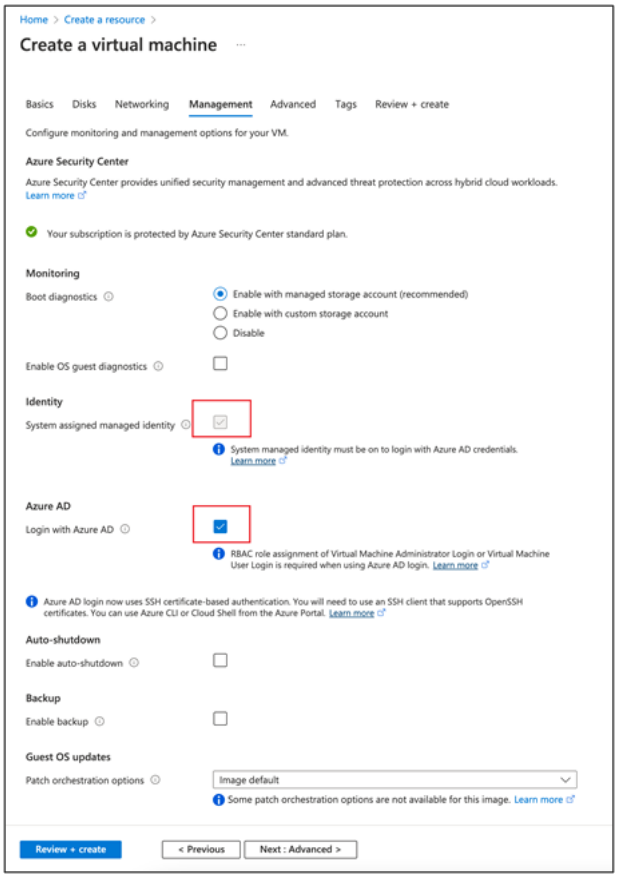
Kommentieren Sie in `/etc/pam.d/remote` die Zeile `Session required pam_loginuid.so` aus, um das Problem zu umgehen. Der folgende Screenshot enthält ein Beispiel.


```
#%PAM-1.0
auth       substack     password-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
#session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    include      postlogin
```

Schritt 1: Erstellen einer Vorlagen-VM im Azure-Portal

Erstellen Sie eine Vorlagen-VM und installieren Sie die Azure-Befehlszeilenschnittstelle auf der VM.

1. Erstellen Sie im Azure-Portal eine Vorlagen-VM. Aktivieren Sie auf der Registerkarte **Management** die Option **Login with Azure AD**, bevor Sie auf **Review + create** klicken.



2. Installieren Sie die Azure-Befehlszeilenschnittstelle auf der Vorlagen-VM.
   Weitere Informationen finden Sie in diesem Microsoft-Artikel.

Schritt 2: Vorbereiten eines Masterimages auf der Vorlagenmaschine

Um ein Masterimage zu erstellen, folgen Sie **Schritt 3: Masterimage vorbereiten** unter Linux VDAs über die Maschinenerstellungsdienste (MCS) erstellen.

Schritt 3: Festlegen der Vorlagen-VM als nicht-domänengebunden

Nachdem Sie ein Masterimage erstellt haben, führen Sie die folgenden Schritte aus, um die VM als nicht-domänengebunden zu definieren:

1. Führen Sie das folgende Skript an der Eingabeaufforderung aus.

```
Modify /var/xdl/mcs/mcs_util.sh
<!--NeedCopy-->
```

2. Suchen Sie nach `function read_non_domain_joined_info()`, und ändern Sie den Wert für `NonDomainJoined` in 2. Der folgende Codeblock ist ein Beispiel.

```
function read_non_domain_joined_info()
{

log "Debug: Enter read_non_domain_joined_info"
# check if websocket enabled
TrustIdentity=`cat ${
 id_disk_mnt_point }
 ${
 ad_info_file_path }
  | grep '[TrustIdentity]' | sed 's/\s//g'`
if [ "$TrustIdentity" == "[TrustIdentity]" ]; then
NonDomainJoined=2
fi
...
 }

<!--NeedCopy-->
```

3. Speichern Sie die Änderung.
4. Fahren Sie die Vorlagen-VM herunter.

Schritt 4: Erstellen der Linux-VMs aus der Vorlagen-VM

Nach dem Vorbereiten der nicht-domänengebundenen Vorlagen-VM führen Sie die folgenden Schritte aus, um VMs zu erstellen:

1. Melden Sie sich bei Citrix Cloud an.

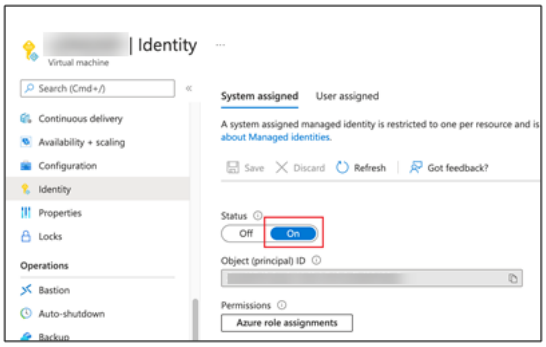
2. Doppelklicken Sie auf Citrix DaaS, und greifen Sie auf die Verwaltungskonsole "Vollständige Konfiguration"zu.
3. Wählen Sie unter **Maschinenkataloge** die Verwendung von MCS (Maschinenerstellungsdiensten) zum Erstellen der Linux-VMs aus der Vorlagen-VM aus. Weitere Informationen finden Sie unter Nicht in Domänen eingebundene VDAs im Citrix DaaS-Dokument.

Schritt 5: Zuweisen von AAD-Benutzerkonten zu den Linux-VMs

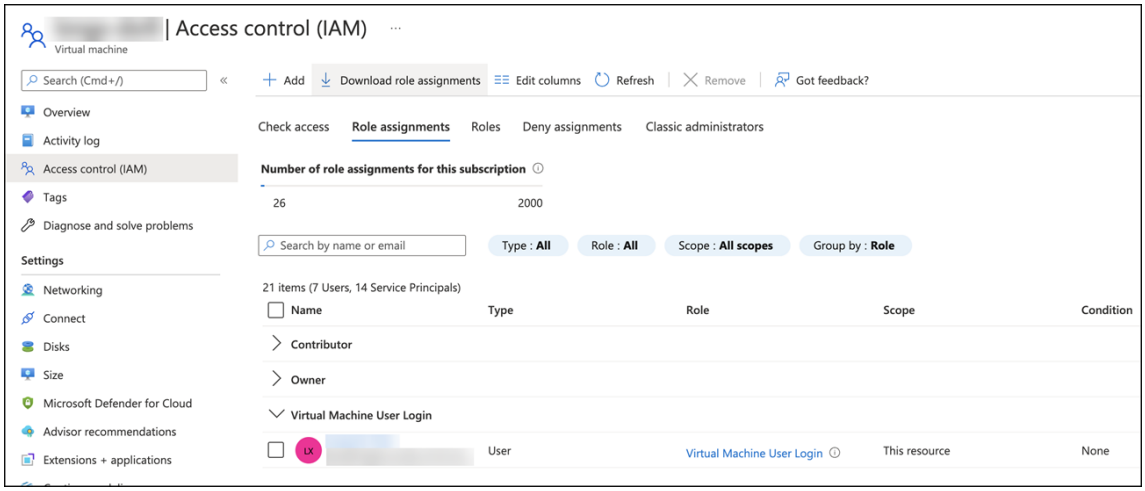
Nachdem Sie die nicht in Domänen eingebundenen VMs erstellt haben, weisen Sie ihnen AAD-Benutzerkonten zu.

Gehen Sie folgendermaßen vor, um einer VM AAD-Benutzerkonten zuzuweisen:

1. Greifen Sie mit einem Administratorkonto auf die VM zu.
2. Aktivieren Sie auf der Registerkarte **Identify > System assigned** die Option **System Identity**.



3. Suchen Sie auf der **Registerkarte Access control (IAM) > Role assignments** den Bereich **Virtual Machine User Login** und fügen Sie die AAD-Benutzerkonten nach Bedarf hinzu.



Anmeldung bei nicht-domänengebundenen VDAs

Endbenutzer in Ihrer Organisation haben zwei Möglichkeiten, sich bei einem nicht-domänengebundenen VDA anzumelden. Verfahren:

1. Starten Sie die Workspace-App und melden Sie sich am Workspace an, indem Sie den AAD-Benutzernamen und das zugehörige Kennwort eingeben. Die Workspace-Seite wird angezeigt.
2. Doppelklicken Sie auf einen nicht-domänengebundenen Desktop. Die Anmeldeseite von AAD wird angezeigt.

   Die Seite variiert je nach festgelegtem Anmeldemodus auf dem VDA: “Device Code”oder “AAD account/password”. Standardmäßig erfolgt die Authentifizierung von AAD-Benutzern auf Linux-VDAs über den Anmeldemodus “Device Code”. Als Administrator können Sie den Anmeldemodus bei Bedarf in “AAD account/password”ändern. Die dafür erforderliche Schrittfolge ist im folgenden Abschnitt beschrieben.

3. Melden Sie sich je nach Anweisung auf dem Bildschirm mit einem der folgenden Verfahren an der Desktopsitzung an:

   - Scannen Sie den QR-Code und geben Sie den Code ein.
   - Geben Sie den AAD-Benutzernamen und das zughörige Kennwort ein.

Ändern des Anmeldemodus in “AAD account/password”

Standardmäßig werden AAD-Benutzer auf Linux-VDAs mit Gerätecodes authentifiziert. Weitere Informationen finden Sie in diesem Microsoft-Artikel. Führen Sie folgende Schritte aus, um den Anmeldemodus in *AAD account/password* zu ändern:

Führen Sie folgenden Befehl auf dem VDA aus, suchen Sie den Schlüssel `AADAcctPwdAuthEnable`, und ändern Sie den Wert in `0x00000001`.

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Services\CitrixBrokerAgent\WebSocket" -t "REG_DWORD" -v "
   AADAcctPwdAuthEnable" -d "0x00000001" --force

<!--NeedCopy-->
```

> **Hinweis:**

> Dieser Ansatz funktioniert nicht für Microsoft-Konten oder Konten mit aktivierter zweistufiger Authentifizierung.

Single-Sign-On-Authentifizierung per Double-Hop

January 8, 2024

Die Benutzerdaten für den Zugriff auf einen StoreFront-Store können in das AuthManager-Modul der Citrix Workspace-App für Linux und Citrix Receiver für Linux 13.10 eingefügt werden. Sie können nach der Injektion den Client verwenden, um auf virtuelle Desktops und Anwendungen innerhalb einer Sitzung mit einem virtuellen Linux-Desktop zuzugreifen, ohne ein zweites Mal Benutzeranmeldeinformationen einzugeben.

> **Hinweis:**
>
> Dieses Feature wird von der Citrix Workspace-App für Linux und Citrix Receiver für Linux 13.10 unterstützt.

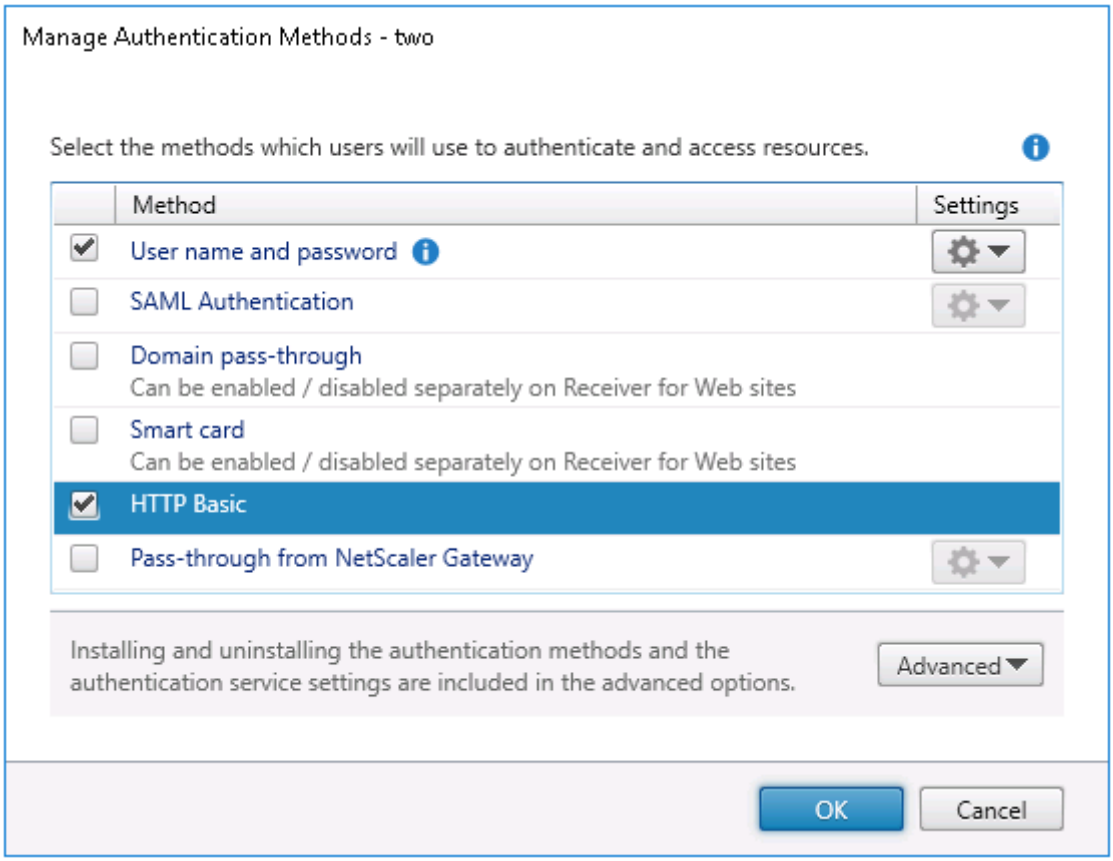
Aktivieren des Features:

1. Installieren Sie auf dem Linux VDA die Citrix Workspace-App für Linux oder Citrix Receiver für Linux 13.10.

   Laden Sie die App von der Citrix Downloadseite für Citrix Workspace oder für Citrix Receiver herunter.

   Der Standardinstallationspfad ist /opt/Citrix/ICAClient/. Wenn Sie die App an einem anderen Pfad installieren, legen Sie die Umgebungsvariable ICAROOT fest, sodass sie auf den tatsächlichen Installationspfad verweist.

2. Fügen Sie in der Citrix StoreFront-Verwaltungskonsole die **HTTP Basic**-Authentifizierungsmethode für den Zielstore hinzu.



3. Fügen Sie der AuthManager-Konfigurationsdatei ($ICAROOT/config/AuthManConfig.xml) den folgenden Schlüssel hinzu, um die HTTP Basic-Authentifizierung zuzulassen:

```
<Protocols>
     <HTTPBasic>
         <Enabled>True</Enabled>
    </HTTPBasic>
</Protocols>
<!--NeedCopy-->
```

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/
<!--NeedCopy-->
```

5. Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

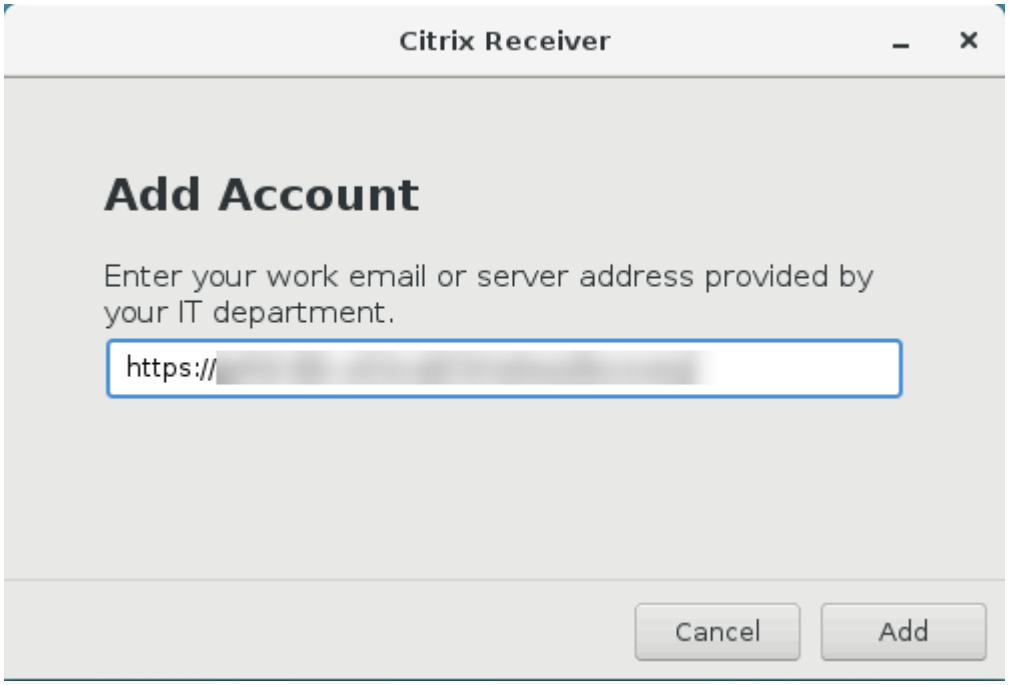
```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d "0
   x00000001"
<!--NeedCopy-->
```

6. Starten Sie eine virtuelle Linux-Desktopsitzung und starten Sie die Citrix Workspace-App für

Linux oder Citrix Receiver für Linux 13.10 innerhalb dieser Sitzung.

Beim ersten Start der Citrix Workspace-App werden Sie aufgefordert, ein Store-Konto anzugeben. Später werden Sie automatisch bei dem zuvor angegebenen Store angemeldet.

> **Hinweis:**
>
> Geben Sie eine HTTPS-URL als Storekonto an.



Verbundauthentifizierungsdienst

February 9, 2024

Mit dem Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) können Sie Benutzer authentifizieren, die sich bei einem Linux VDA anmelden. Der Linux VDA verwendet dieselbe Windows-Umgebung wie der Windows VDA für das FAS-Anmeldefeature. Informationen zur Konfiguration der Windows-Umgebung für FAS finden Sie unter Verbundauthentifizierungsdienst. Dieser Artikel enthält zusätzliche Informationen speziell für den Linux VDA.

> **Hinweis:**
>
> - Der Linux VDA bietet keine Unterstützung für die Richtlinie **In-session Behavior**.
> - Der Linux VDA verwendet kurze Verbindungen, um Daten an FAS-Server zu übertragen.

> • Ab Release 2206 können Sie den FAS-Port auf dem Linux VDA über CTX_XDL_FAS_LIST in der Datei ctxsetup.sh anpassen. Weitere Informationen finden Sie im Linux VDA-Installationsartikel zur Ihrer Distribution.

Unterstützte Distributionen

FAS unterstützt einige Linux-Distributionen und Methoden zum Domänenbeitritt. Siehe folgende Tabelle:

	Winbind	SSSD	Centrify	PBIS
Amazon Linux 2	Ja	Ja	Ja	Ja
Debian 11.3	Ja	Ja	Ja	Ja
RHEL 9.2/9.0	Ja	Ja	Nein	Nein
RHEL 8.8/8.6	Ja	Ja	Ja	Ja
RHEL 7.9, CentOS 7.9	Ja	Ja	Ja	Ja
Rocky Linux 9.2/9.0	Ja	Ja	Nein	Nein
Rocky Linux 8.8/8.6	Ja	Ja	Nein	Nein
SUSE 15.4	Ja	Ja	Ja	Nein
Ubuntu 22.04/20.04	Ja	Ja	Ja	Ja

Konfigurieren des FAS auf dem Linux VDA

FAS-Unterstützung unter RHEL 8.x/9.x und Rocky Linux 8.x/9.x

FAS ist abhängig von dem Modul pam_krb5, das unter RHEL 8.x und Rocky Linux 8.x veraltet ist. Die folgenden Schritte sind erforderlich, wenn Sie FAS auf RHEL 8.x- und Rocky Linux 8.x-Maschinen verwenden möchten, die im Multisitzungs-OS-Modus bereitgestellt werden. Für FAS auf RHEL 8.x- und Rocky Linux 8.x-Maschinen, die im Einzelsitzungs-OS-Modus (VDI-Modus) bereitgestellt werden, können Sie die folgenden Schritte überspringen.

1. Laden Sie den Quellcode pam_krb5-2.4.8-6 von der folgenden Website herunter:

   https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html.

2. Erstellen und installieren Sie das Modul pam_krb5 unter RHEL 8.x und Rocky Linux 8.x.


```
yum install make gcc krb5-devel pam-devel autoconf libtool

rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div

tar xvzf pam_krb5-2.4.8.tar.gz

cd pam_krb5-2.4.8

./configure --prefix=/usr

make

make install
<!--NeedCopy-->
```

3. Überprüfen Sie, ob pam_krb5.so unter /usr/lib64/security/ vorliegt.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

Einrichten von FAS-Servern

Um FAS bei einer Neuinstallation von Linux VDA zu verwenden, geben Sie den FQDN jedes FAS-Servers ein, wenn Sie ctxinstall.sh oder ctxsetup.sh ausführen.

> **Hinweis:**
>
> Die FAS-Server werden über die AD-Gruppenrichtlinie konfiguriert. Informationen zur Einstellung der FAS-Richtlinie im Domänen-Gruppenrichtlinienobjekt finden Sie unter Gruppenrichtlinie konfigurieren.
>
> Da der Linux VDA die AD-Gruppenrichtlinie nicht unterstützt, geben Sie stattdessen eine durch Semikolons getrennte Liste mit FAS-Servern an. Beachten Sie Folgendes:
>
> - Die Reihenfolge der Liste muss mit der Reihenfolge in der AD-Gruppenrichtlinie übereinstimmen.
> - Wenn eine Serveradresse entfernt wird, füllen Sie die leere Stelle mit der Textzeichenfolge **<none>** auf und behalten den Index der Serveradressen unverändert bei.

Zum Aktualisieren einer vorhandenen Linux VDA-Installation können Sie `ctxsetup.sh` erneut ausführen, um die FAS-Server einzurichten. Sie können die FAS-Server auch über die folgenden Befehle einrichten. Starten Sie anschließend den `ctxvda`-Dienst neu, um die Einstellung zu übernehmen.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
    VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
    " -v "Addresses" -d "<Your-FAS-Server-List>" --force

```



```
3 service ctxjproxy restart
4
5 service ctxvda restart
6 <!--NeedCopy-->
```

Um die FAS-Server über `ctxreg` zu aktualisieren, führen Sie die folgenden Befehle aus:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\
     VirtualDesktopAgent\Authentication\UserCredentialService" -v "
     Addresses" -d "<Your-FAS-Server-List>"
2
3 service ctxjproxy restart
4
5 service ctxvda restart
6 <!--NeedCopy-->
```

Installieren von Zertifikaten

Für die Überprüfung von Benutzerzertifikaten installieren Sie das Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate auf dem VDA. Beispiel: Zum Installieren des Stammzertifizierungsstellenzertifikats rufen Sie das AD-Stammzertifikat aus dem vorherigen Schritt **Abrufen des ZS-Zertifikats von der Microsoft-Zertifizierungsstelle (in AD)** ab oder laden Sie es im DER-Format vom Stammzertifizierungsstellenserver `http://CA-SERVER/certsrv` herunter.

> **Hinweis:**
>
> Die folgenden Befehle gelten auch für die Konfiguration eines Zwischenzertifikats.

Mit diesem oder einem ähnlichen Befehl können Sie eine DER-Datei (.crt, .cer, .der) in PEM konvertieren.

```
1 sudo openssl x509 -inform der -in root.cer -out root.pem
2 <!--NeedCopy-->
```

Anschließend installieren Sie mit diesem oder einem ähnlichen Befehl das Stammzertifizierungsstellenzertifikat im Verzeichnis `openssl`:

```
1 sudo cp root.pem /etc/pki/CA/certs/
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Speichern Sie das Stammzertifizierungsstellenzertifikat nicht im Verzeichnis **/root**. Andernfalls besitzt FAS keine Leseberechtigung für das Stammzertifizierungsstellenzertifikat.

Ausführen von ctxfascfg.sh

Führen Sie das Skript ctxfascfg.sh aus, um FAS zu konfigurieren:

```
sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
<!--NeedCopy-->
```

Es werden Umgebungsvariablen hinzugefügt, damit `ctxfascfg.sh` im stillen Modus ausgeführt werden kann:

- **CTX_FAS_ADINTEGRATIONWAY=winbind | sssd | centrify | pbis**: Die Active Directory-Integrationsmethode; das entspricht `CTX_EASYINSTALL_ADINTEGRATIONWAY`, wenn `CTX_EASYINSTALL_ADINTEGRATIONWAY` angegeben wurde. Wenn `CTX_EASYINSTALL_ADINTEGRA` nicht angegeben ist, verwendet `CTX_FAS_ADINTEGRATIONWAY` die eigene Werteinstellung.
- **CTX_FAS_CERT_PATH =<certificate path>**: Gibt den vollständigen Pfad an, in dem Stammzertifikate und alle Zwischenzertifikate gespeichert werden.
- **CTX_FAS_KDC_HOSTNAME**: Gibt den Hostnamen des Schlüsselverteilungscenters (KDC) an, wenn Sie PBIS auswählen.
- **CTX_FAS_PKINIT_KDC_HOSTNAME**: Gibt den Hostnamen des PKINIT KDC an, der CTX_FAS_KDC_HOSTNAM ist, sofern nicht anders angegeben. Wenn Sie mehrere Delivery Controller haben, fügen Sie die Hostnamen aller KDCs der Domäne zu pkinit_kdc_hostname in der Datei **/etc/krb5.conf** hinzu. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX322129.

Wählen Sie die korrekte Active Directory-Integrationsmethode aus und geben Sie den korrekten Pfad zu den Zertifikaten ein (z. B. `/etc/pki/CA/certs/`).

Das Skript installiert die Pakete krb5-pkinit und pam_krb5 und legt die relevanten Konfigurationsdateien fest.

FAS deaktivieren

Um FAS auf dem Linux VDA zu deaktivieren, entfernen Sie alle FAS-Server aus ConfDB mit den folgenden Befehlen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent\Authentication\UserCredentialService" -t "REG_SZ
   " -v "Addresses" -d "" --force

service ctxjproxy restart

service ctxvda restart
<!--NeedCopy-->
```


Einschränkung

- FAS unterstützt den Sperrbildschirm noch nicht. Wenn Sie in einer Sitzung auf die Sperrschaltfläche klicken, können Sie sich mit FAS nicht erneut bei der Sitzung anmelden.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen, die in dieser Version unterstützt werden. Das **Einbinden über Azure AD mit Windows 10** ist nicht möglich.

Problembehandlung

Stellen Sie vor einer Problembehandlung des Verbundauthentifizierungsdiensts (FAS) sicher, dass der Linux VDA ordnungsgemäß installiert und konfiguriert ist und dass Sitzungen ohne FAS-Server erfolgreich im gemeinsamen Store per Kennwortauthentifizierung gestartet werden können.

Wenn Sitzungen ohne FAS-Server fehlerfrei ausgeführt werden, setzen Sie die HDX-Protokollebene der **Login**-Klasse auf VERBOSE und die VDA-Protokollebene auf TRACE. Informationen zum Aktivieren von Protokollen zur Ablaufverfolgung (Tracing) für Linux VDA finden Sie im Knowledge Center-Artikel CTX220130.

Sie können Ihre Linux VDA-Umgebung auch mit dem Linux **XDPing**-Tool auf mögliche Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter **XDPing**.

Fehler bei der FAS-Serverkonfiguration

Der Start einer Sitzung über den FAS-Store schlägt fehl.

Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie ein Fehlerprotokoll folgender Art:

```
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
```



```
12
13 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user:
      failed to validate fas credential
14
15 2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate:
      failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER
16
17 <!--NeedCopy-->
```

Lösung Stellen Sie mit folgendem Befehl sicher, dass der Citrix Registrierungswert "HKEY_LOCAL_MACHINE\SOF
auf <Your-FAS-Server-List> festgelegt ist.

```
1 sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
2 <!--NeedCopy-->
```

Wenn die Einstellung falsch ist, legen Sie sie erneut fest, wie weiter oben im Schritt Einrichten von FAS-Servern beschrieben.

Falsche Konfiguration des Zertifizierungsstellenzertifikats

Der Start einer Sitzung über den FAS-Store schlägt fehl. Ein graues Fenster wird für einige Sekunden angezeigt.

Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie ein Fehlerprotokoll folgender Art:

```
1 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
      get_logon_certificate: entry
2
3 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller:
      current process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]
4
5 2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
      get_public_certificate: entry
6
7 2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
       for response...
8
```



```
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
<!--NeedCopy-->
```

Lösung Stellen Sie sicher, dass Sie den vollständigen Pfad, in dem das Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate gespeichert werden, korrekt in `/etc/krb5.conf` festgelegt haben. Der vollständige Pfad ist dem folgenden ähnlich:

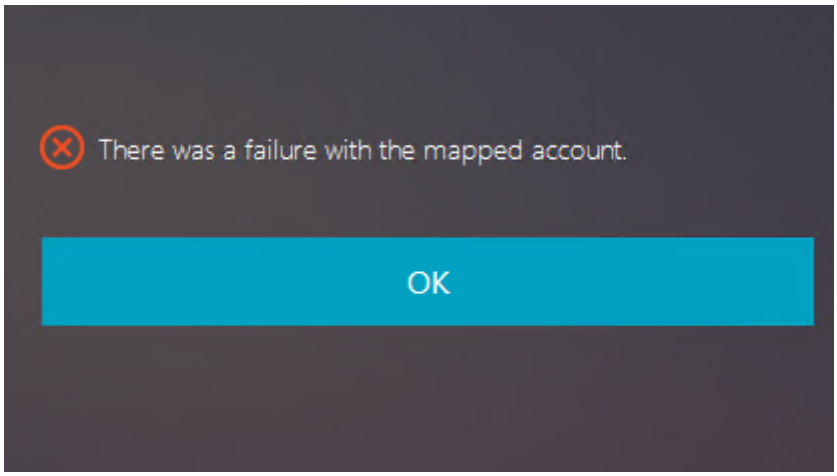
```
 [realms]

EXAMPLE.COM = {


    ......

    pkinit_anchors = DIR:/etc/pki/CA/certs/

    ......

 }

<!--NeedCopy-->
```

Wenn die vorhandene Einstellung falsch ist, legen Sie sie erneut fest, wie weiter oben im Schritt Installieren von Zertifikaten beschrieben.

Überprüfen Sie auch, ob das Stammzertifizierungsstellenzertifikat gültig ist.

Kontozuordnungsfehler bei Spiegelung

FAS ist für die SAML-Authentifizierung konfiguriert. Der folgende Fehler kann auftreten, wenn ein Benutzer der Active Directory-Verbunddienste (AD FS) den Benutzernamen und das Kennwort auf der AD FS-Anmeldeseite eingibt.

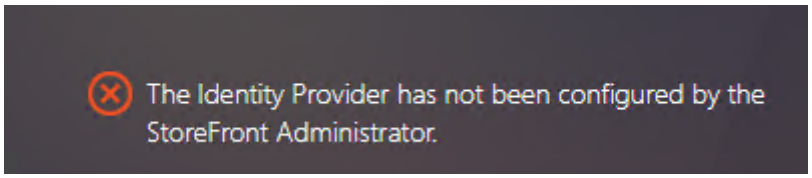


Die Fehlermeldung zeigt an, dass der Benutzer zwar erfolgreich in AD FS verifiziert wurde, aber kein gespiegeltes Konto für den Benutzer in AD konfiguriert ist.

Lösung Richten Sie das gespiegelte Konto in AD ein.

AD FS nicht konfiguriert

Bei einem Anmeldeversuch beim FAS-Store tritt folgender Fehler auf:



Das Problem tritt auf, wenn der FAS-Speicher für die SAML-Authentifizierung konfiguriert ist, aber die ADFS-Bereitstellung fehlt.

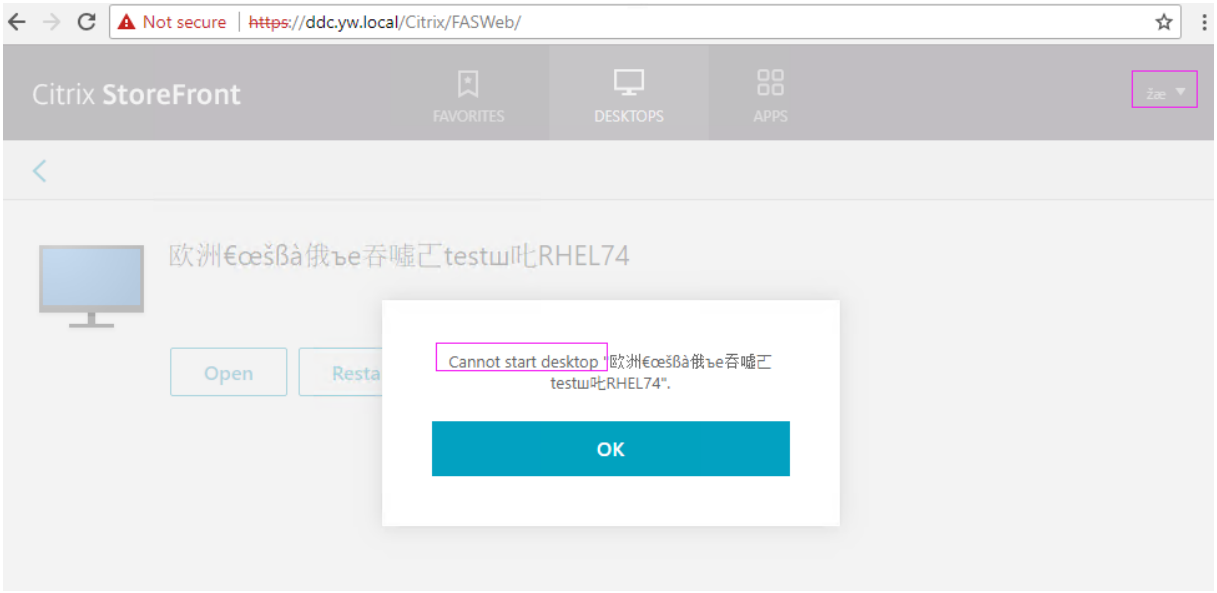
Lösung Stellen Sie den AD FS-Identitätsanbieter für den Verbundauthentifizierungsdienst (FAS) bereit. Weitere Informationen finden Sie unter AD FS-Bereitstellung des Verbundauthentifizierungsdiensts.

Verwandte Informationen

- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Artikel mit Anleitungen finden Sie unter Erweiterte Konfiguration des Verbundauthentifizierungsdiensts.

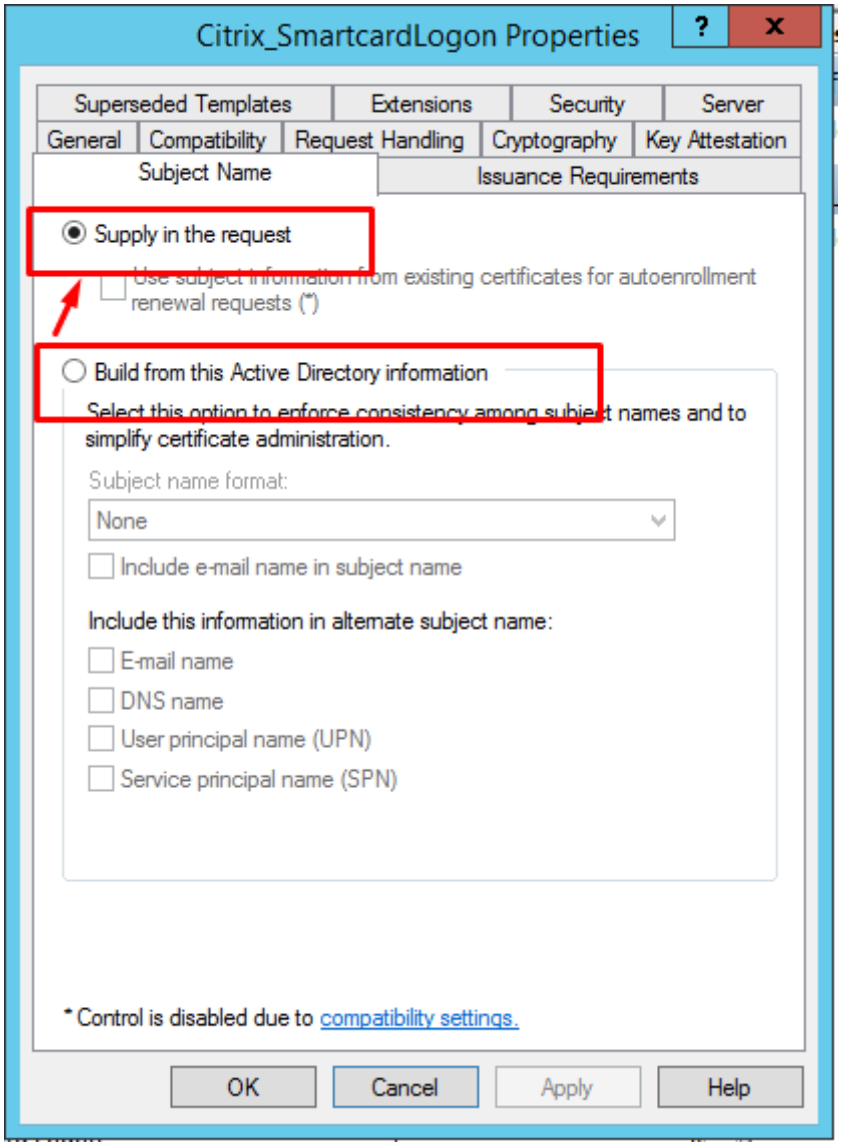
Bekannte Probleme

Beim Einsatz von FAS kann der Start einer veröffentlichten Desktop- oder App-Sitzung mit nicht-englischen Zeichen fehlschlagen.



Workaround

Klicken Sie im ZS-Tool mit der rechten Maustaste auf **Vorlagen verwalten** und ändern Sie die Vorlage für **Citrix_SmartcardLogon** von **Aus diesen Informationen in Active Directory erstellen** in **Informationen werden in der Anforderung angegeben**:



FIDO2 (Preview)

January 8, 2024

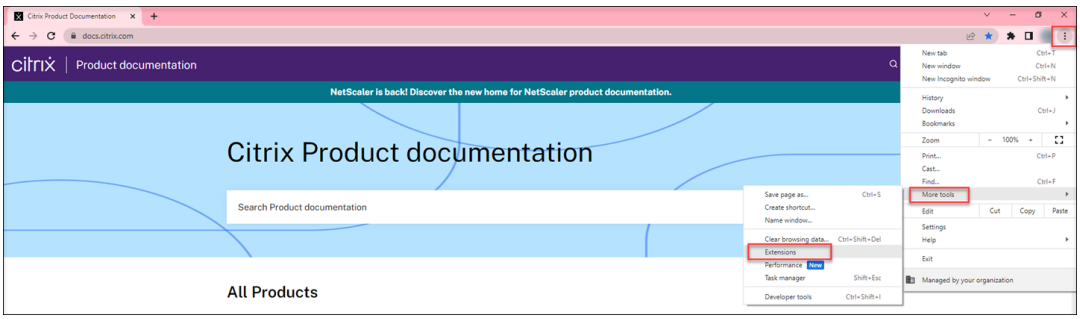
Sie können die FIDO2-Authentifizierung einrichten, um mithilfe von Google Chrome auf dem Linux VDA gehostet auf Websites zuzugreifen.

> **Hinweis:**
>
> Dieses Feature ist als Preview verfügbar. Als Preview verfügbare Features sind möglicherweise nicht vollständig lokalisiert und werden für die Verwendung in Nicht-Produktionsumgebungen

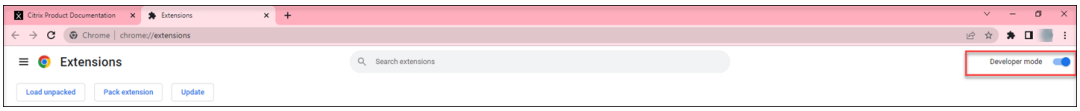
> empfohlen. Der technische Support von Citrix bietet keine Unterstützung bei Problemen mit als Preview verfügbaren Features.
>
> Der Linux VDA unterstützt nur die Kombination von FIDO2 und Google Chrome.

Gehen Sie wie folgt vor, um die FIDO2-Authentifizierung einzurichten:

1. Laden Sie das Citrix FIDO2-Erweiterungspaket herunter.
   a) Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
   b) Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
   c) Klicken Sie auf **Komponenten**, um den Linux VDA zu finden.
   d) Klicken Sie auf den Linux VDA, um die Downloadseite zu öffnen.
   e) Laden Sie das Quellpaket herunter.
   f) Entpacken Sie das Quellpaket, um **FIDO2-JavaScript-Extensions.zip** zu finden.
   g) Entpacken Sie das FIDO2-Erweiterungspaket. Das FIDO2-Erweiterungs-Verzeichnis ist unter **extensions > chrome > fido2**.
2. Fügen Sie die Citrix FIDO2-Erweiterung in Google Chrome hinzu:
   a) Öffnen Sie Google Chrome auf dem Linux VDA.
   b) Klicken Sie auf das Dreipunktmenü rechts neben der Adressleiste und wählen Sie **Weitere Tools > Erweiterungen**.



   c) Schalten Sie den **Entwicklermodus** ein.



   d) Klicken Sie auf **Entpackte Erweiterung laden** und wählen Sie das Erweiterungen-Verzeichnis unter **extensions > chrome > fido2** aus.
3. Registrieren Sie auf der Website, für die Sie die FIDO2-Authentifizierung verwenden möchten, einen FIDO2-Sicherheitsschlüssel.
   a) Fügen Sie einen FIDO2-Sicherheitsschlüssel am Client ein, auf dem die Citrix Workspace-App installiert ist.

b) Aktivieren Sie die Multifaktorauthentifizierung und fügen Sie FIDO2 als Authentifizierungsmethode hinzu.

Wenn die FIDO2-Authentifizierung eingerichtet ist, werden Sie aufgefordert, den Sicherheitsschlüssel zu berühren, um auf die Website zuzugreifen.

Authentifizierung ohne Single Sign-On

January 8, 2024

Dieser Artikel enthält eine Anleitung zum Aktivieren der Authentifizierung ohne Single Sign-On auf dem Linux VDA.

Übersicht

Standardmäßig ist auf dem Linux VDA Single Sign-On (SSO) aktiviert. Die Benutzer melden sich bei der Citrix Workspace-App und bei VDA-Sitzungen mit einem Satz Anmeldeinformationen an.

Sollen sich Benutzer bei VDA-Sitzungen mit einem anderen Satz Anmeldeinformationen anmelden, deaktivieren Sie SSO auf dem Linux VDA. In der folgenden Tabelle sind Kombinationen von Benutzerauthentifizierungsmethoden aufgeführt, die in Szenarien ohne SSO unterstützt werden.

Citrix Workspace-App	VDA-Sitzung
Benutzername	Benutzername
Smartcard	Benutzername
Benutzername	Smartcard
FAS	Benutzername
FAS	Smartcard

Deaktivieren von SSO

Führen Sie den folgenden Befehl auf dem Linux VDA aus:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\WinStations\tcp" -t "REG_DWORD" -v "
     fPromptForDifferentUser" -d "0x00000001" --force
2 <!--NeedCopy-->
```


Smartcards

April 18, 2024

Sie können eine mit dem Clientgerät verbundene Smartcard zur Anmeldung an einer virtuellen Linux-Desktopsitzung verwenden. Dieses Feature wurde in Form der Smartcardumleitung über den virtuellen ICA-Smartcardkanal implementiert. Sie können die Smartcard auch innerhalb der Sitzung verwenden. Anwendungsfälle:

- Digitale Signatur zu einem Dokument hinzufügen
- E-Mails verschlüsseln oder entschlüsseln
- Authentifizierung bei einer Website

Auf dem Linux VDA wird hierfür die gleiche Konfiguration wie auf dem Windows VDA verwendet. Weitere Informationen finden Sie unter Konfigurieren der Smartcardumgebung in diesem Artikel.

> **Hinweis:**
>
> Die Verwendung einer zugeordneten Smartcard in einer Linux VDA-Sitzung zur Anmeldung bei Citrix Gateway wird nicht unterstützt.

Voraussetzungen

Die Passthrough-Authentifizierung mit Smartcard erfordert die Erfüllung folgender Voraussetzungen:

- Der Linux VDA ist unter einer der folgenden Distributionen installiert:
  - RHEL 9.2/9.0
  - RHEL 8.8/8.6
  - RHEL 7, CentOS 7
  - Rocky Linux 9.2/9.0
  - Rocky Linux 8.8/8.6
  - Ubuntu 22.04
  - Ubuntu 20.04
  - Debian 11.3

  Stellen Sie nach Abschluss der VDA-Installation sicher, dass sich der VDA beim Delivery Controller registrieren kann und Sie die veröffentlichten Linux-Desktopsitzungen mit Windows-Anmeldeinformationen öffnen können.
- Es werden von OpenSC unterstützte Smartcards verwendet. Weitere Informationen finden Sie unter Überprüfen der Kompatibilität der verwendeten Smartcards mit OpenSC.

- Citrix Workspace-App für Windows wird verwendet.

Überprüfen der Kompatibilität der verwendeten Smartcards mit OpenSC

OpenSC ist ein gebräuchlicher Treiber für Smartcards unter RHEL 7.4+. Als voll kompatibler Ersatz von CoolKey unterstützt OpenSC viele Arten von Smartcards (siehe Smart Card Support in Red Hat Enterprise Linux).

In diesem Artikel dient die YubiKey-Smartcard als Beispiel zur Veranschaulichung der Konfiguration. YubiKey ist ein im Handel erhältliches und PIV-konformes USB-Gerät mit CCID-Funktion. YubiKey wird vom OpenSC-Treiber unterstützt.

Wenn in Ihrer Organisation eine anspruchsvollere Smartcard benötigt wird, stellen Sie eine physische Maschine mit einer unterstützten Linux-Distribution und installiertem OpenSC-Paket bereit. Informationen zur Installation von OpenSC finden Sie unter Installieren des Smartcardtreibers. Führen Sie die Smartcard ein und prüfen Sie mit folgendem Befehl, ob OpenSC Ihre Smartcard unterstützt:

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
<!--NeedCopy-->
```

Konfiguration

Vorbereiten eines Stammzertifikats

Ein Stammzertifikat wird zur Überprüfung des Zertifikats auf der Smartcard verwendet. Führen Sie die folgenden Schritte aus, um ein Stammzertifikat herunterzuladen und zu installieren:

1. Rufen Sie (normalerweise von einem Zertifizierungsstellenserver) ein Stammzertifikat im PEM-Format ab.

   Sie können eine DER-Datei (*.crt, *.cer, *.der) mithilfe des folgenden Befehls in PEM konvertieren. In dem Beispiel heißt die DER-Datei **certnew.cer**.

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   <!--NeedCopy-->
   ```

2. Installieren Sie das Stammzertifikat im Verzeichnis `openssl`. Die Datei **certnew.pem** gilt hier als Beispiel.

   ```
   cp certnew.pem <path where you install the root certificate>
   <!--NeedCopy-->
   ```

   Um einen Pfad für die Installation des Stammzertifikats zu erstellen, führen Sie `sudo mdkir -p <path where you install the root certificate>` aus.

Erstellen Sie das Modul pam_krb5 unter RHEL 8.x/9.x und Rocky Linux 8.x/9.x

Die Smartcardauthentifizierung ist abhängig vom Modul pam_krb5, das unter RHEL 8.x und Rocky Linux 8.x veraltet ist. Die folgenden Schritte sind erforderlich, wenn Sie die Smartcardauthentifizierung auf RHEL 8.x- und Rocky Linux 8.x-Maschinen verwenden möchten, die im Multisitzungs-OS-Modus bereitgestellt werden. Für die Smartcardauthentifizierung auf RHEL 8.x- und Rocky Linux 8.x-Maschinen, die im Einzelsitzungs-OS-Modus (VDI-Modus) bereitgestellt werden, können Sie die folgenden Schritte überspringen.

1. Laden Sie den pam_krb5-2.4.8-6-Quellcode von https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html herunter.
2. Erstellen und installieren Sie das Modul pam_krb5 unter RHEL 8.x und Rocky Linux 8.x.

```
yum install -y opensc pcsc-lite pcsc-lite-libs pcsc-lite-ccid nss-tools
yum install gcc krb5-devel pam-devel autoconf libtool
rpm2cpio pam_krb5-2.4.8-6.el7.src.rpm | cpio -div
tar xvzf pam_krb5-2.4.8.tar.gz
cd pam_krb5-2.4.8
./configure --prefix=/usr
make
make install
<!--NeedCopy-->
```

3. Überprüfen Sie, ob pam_krb5.so unter /usr/lib64/security/ vorliegt.

```
ls -l /usr/lib64/security | grep pam_krb5
<!--NeedCopy-->
```

Konfigurieren der Smartcardumgebung

Sie können die Smartcardumgebung mit dem Skript ctxsmartlogon.sh oder auch manuell konfigurieren.

(Option 1) Konfigurieren der Smartcardumgebung mit dem Skript ctxsmartlogon.sh

> **Hinweis:**
>
> Das Skript ctxsmartlogon.sh fügt PKINIT-Informationen zum Standardbereich hinzu. Sie können diese Einstellung über die Konfigurationsdatei **/etc/krb5.conf** ändern.

Vor der ersten Verwendung von Smartcards konfigurieren Sie die Smartcardumgebung mit dem Skript ctxsmartlogon.sh.

> **Tipp:**
>
> Wenn Sie SSSD zum Domänenbeitritt verwendet haben, starten Sie den SSSD-Dienst nach dem Ausführen von ctxsmartlogon.sh neu.

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
<!--NeedCopy-->
```

Die Ergebnisse ähneln der folgenden Anzeige:

```
#*********************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*********************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
  Please select which Active Directory integration method to use:
     1: Winbind
     2: SSSD
     3: Centrify
  Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
  Installing, please wait...
    [krb5-pkinit][pam_krb5] already installed.
    [pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
  Packages installed. [Success]
Step 4:Configure krb5.conf.
  Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
  /etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
  Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
  /etc/pam.d/ctxfsc configure successfully.
  /etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

Sie können Smartcards auch deaktivieren, indem Sie das Skript ctxsmartlogon.sh ausführen:

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
<!--NeedCopy-->
```

Die Ergebnisse ähneln der folgenden Anzeige:

```
#*********************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#*********************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.
```

(Option 2) Manuelles Konfigurieren der Smartcardumgebung Auf dem Linux VDA wird dieselbe Smartcardumgebung verwendet wie auf dem Windows VDA. In der Umgebung müssen mehrere Kom-

ponenten konfiguriert werden: Domänencontroller, Microsoft-Zertifizierungsstelle, Internetinformationsdienste (IIS), Citrix StoreFront und Citrix Workspace-App. Informationen zur Konfiguration am Beispiel der YubiKey-Smartcard finden Sie im Knowledge Center-Artikel CTX206156.

Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie Folgendes sicher:

- Sie haben alle Komponenten ordnungsgemäß konfiguriert.
- Sie haben den privaten Schlüssel und das Benutzerzertifikat auf die Smartcard heruntergeladen.
- Sie können sich mit der Smartcard erfolgreich am VDA anmelden.

Installieren der PC/SC Lite-Pakete PC/SC Lite ist eine Implementierung der PC/SC-Spezifikation (Personal Computer/Smartcard) unter Linux. Sie bietet eine Windows-Smartcardschnittstelle zur Kommunikation mit Smartcards und Lesegeräten. Die Smartcardumleitung des Linux VDAs ist auf PC/SC-Ebene implementiert.

Führen Sie den folgenden Befehl aus, um die PC/SC Lite-Pakete zu installieren:

RHEL 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x, RHEL 7/CentOS 7:

```
yum install pcsc-lite pcsc-lite-ccid pcsc-lite-libs
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04, Debian 11.3:

```
apt-get install -y libpcsclite1 libccid
<!--NeedCopy-->
```

Installieren des Smartcardtreibers OpenSC ist ein gebräuchlicher Treiber für Smartcards. Wenn OpenSC nicht installiert ist, führen Sie den folgenden Befehl aus, um es zu installieren:

RHEL 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x, RHEL 7/CentOS 7:

```
yum install opensc
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04, Debian 11.3:

```
apt-get install -y opensc
<!--NeedCopy-->
```

Installieren der PAM-Module für die Authentifizierung per Smartcard Führen Sie den folgenden Befehl aus, um die Module pam_krb5 und krb5-pkinit zu installieren:

RHEL 7/CentOS 7:


```
yum install pam_krb5 krb5-pkinit
<!--NeedCopy-->
```

RHEL 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x:

```
yum install krb5-pkinit
<!--NeedCopy-->
```

Ubuntu 22.04, Ubuntu 20.04:

```
apt-get install libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

Debian 11.3:

```
apt-get install -y libpam-krb5 krb5-pkinit
<!--NeedCopy-->
```

pam_krb5 ist ein austauschbares Authentifizierungsmodul. Damit können PAM-fähige Anwendungen mit pam_krb5 Kennwörter prüfen und Ticket Granting Tickets vom Schlüsselverteilungscenter (KDC) abrufen. krb5-pkinit enthält das PKINIT-Plug-In, mit dem Clients mit einem privaten Schlüssel und einem Zertifikat Anfangsanmeldeinformationen vom KDC abrufen können.

Konfigurieren des pam_krb5-Moduls Das pam_krb5-Modul interagiert mit dem KDC zum Abrufen von Kerberos-Tickets über Zertifikate auf Smartcards. Führen Sie den folgenden Befehl aus, um die pam_krb5-Authentifizierung in PAM zu aktivieren:

```
authconfig --enablekrb5 --update
<!--NeedCopy-->
```

Fügen Sie der Konfigurationsdatei **/etc/krb5.conf** PKINIT-Informationen entsprechend dem tatsächlichen Bereich hinzu:

> **Hinweis:**
>
> Die Option **pkinit_cert_match** gibt Übereinstimmungsregeln an, die das Clientzertifikat erfüllen muss, damit es zum Versuch der PKINIT-Authentifizierung verwendet wird. Die Syntax der Übereinstimmungsregeln ist:
>
> **[relation-operator] component-rule**…
>
> , wobei **relation-operator** entweder **&&** (alle Komponentenregeln müssen erfüllt werden) sein kann oder **||** (nur eine Komponentenregel muss erfüllt werden).

Beispiel für eine generische krb5.conf-Datei:

```
EXAMPLE.COM = {

```



```
3
4       kdc = KDC.EXAMPLE.COM
5
6       auth_to_local = RULE:[1:$1@$0]
7
8       pkinit_anchors = FILE:<path where you install the root certificate
            >/certnew.pem
9
10      pkinit_kdc_hostname = KDC.EXAMPLE.COM
11
12      pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
13
14      pkinit_eku_checking = kpServerAuth
15
16    }
17
18  <!--NeedCopy-->
```

Die Konfigurationsdatei sieht in etwa folgendermaßen aus, nachdem Sie die PKINIT-Informationen hinzugefügt haben:

```
CTXDEV.LOCAL = {
    kdc = ctx-ad.ctxdev.local
    auth_to_local = RULE:[1:$1@$0]
    pkinit_kdc_hostname = ctx-ad.ctxdev.local
    pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
    pkinit_eku_checking = kpServerAuth
    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
}
```

Konfigurieren der PAM-Authentifizierung PAM-Konfigurationsdateien bestimmen, welche Module für die PAM-Authentifizierung verwendet werden. Um pam_krb5 als Authentifizierungsmodul hinzuzufügen, fügen Sie der Datei **/etc/pam.d/smartcard-auth** folgende Zeile hinzu :

```
auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options
=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.
so
```

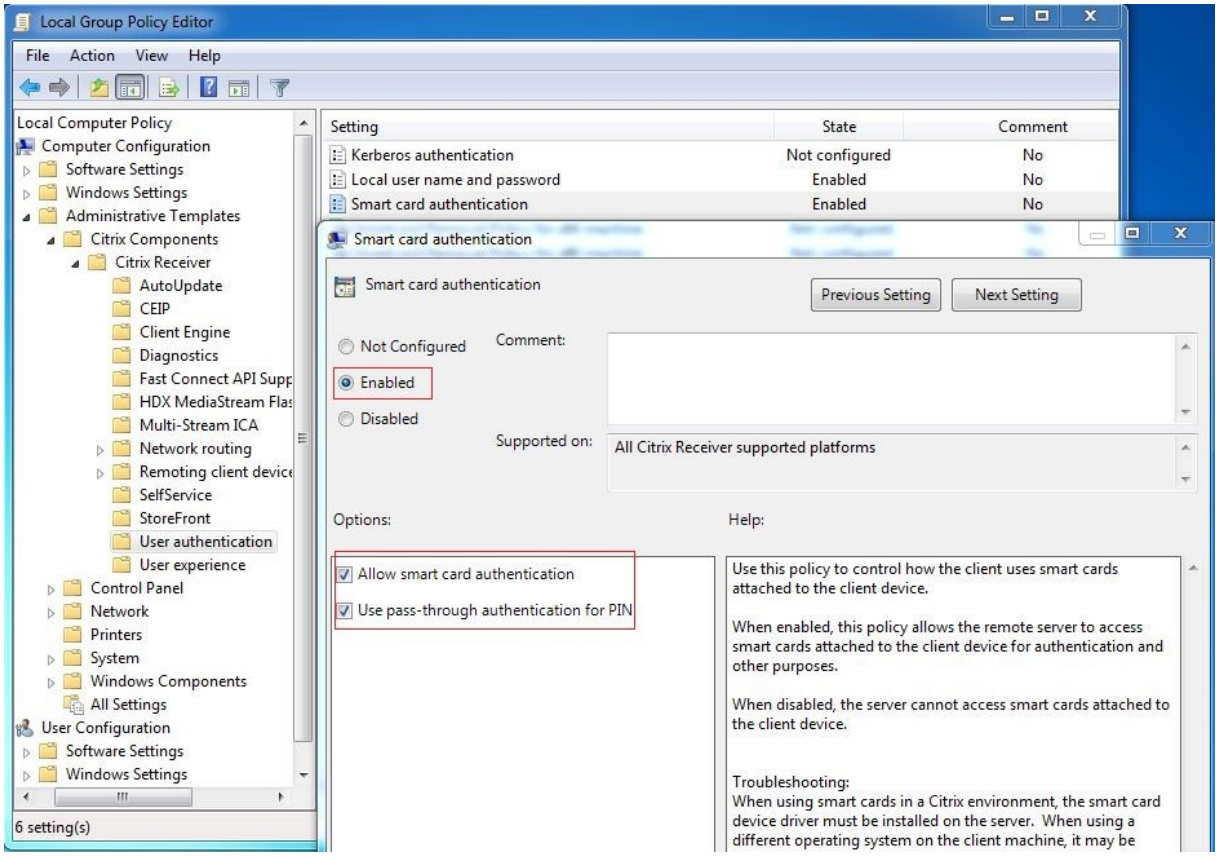
Die Konfigurationsdatei sieht in etwa folgendermaßen aus, nachdem Sie sie geändert haben, wenn SSSD verwendet wird:


```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die]  pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
account     required      pam_permit.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
#session     optional      pam_oddjob_mkhomedir.so umask=0077
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
session     optional      pam_krb5.so
```

Optional: Single Sign-On per Smartcard

Single Sign-On ist ein Citrix Feature, mit dem die Passthrough-Authentifizierung in Starts von virtuellen Desktops und Anwendungen implementiert wird. Dadurch müssen Benutzer ihre PIN seltener eingeben. Konfigurieren Sie die Citrix Workspace-App, um SSO mit dem Linux VDA zu verwenden. Die Konfiguration ist die gleiche wie für den Windows-VDA. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX133982.

Aktivieren Sie die Smartcardauthentifizierung wie nachfolgend beschrieben, wenn Sie die Gruppenrichtlinie in der Citrix Workspace-App konfigurieren.



Anmeldung mit Schneller Smartcard

Das Schnelle-Smartcard-Feature ist eine Verbesserung gegenüber der alten HDX PC/SC-basierten Smartcardumleitung. Das Feature verbessert die Leistung, wenn Smartcards in WANs mit hoher Latenz verwendet werden. Weitere Informationen finden Sie unter Smartcards.

Der Linux VDA unterstützt Schnelle Smartcards auf folgenden Versionen der Citrix Workspace-App:

- Citrix Receiver für Windows 4.12
- Citrix Workspace-App 1808 für Windows und höher

Aktivieren der Anmeldung mit Schneller Smartcard auf dem Client Die Anmeldung mit Schneller Smartcard ist standardmäßig auf dem VDA aktiviert und auf dem Client deaktiviert. Zum Aktivieren des Features auf dem Client fügen Sie folgenden Parameter in die Datei default.ica der zugehörigen StoreFront-Site ein:

```
1 [WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

Deaktivieren der Anmeldung mit Schneller Smartcard auf dem Client Um die Anmeldung mit Schneller Smartcard auf dem Client zu deaktivieren, entfernen Sie den Parameter **SmartCardCryptographicRedirection** aus der Datei default.ica der zugehörigen StoreFront-Website.

XDPing ausführen

Nachdem Sie die vorherigen Schritte ausgeführt haben, können Sie Ihre Linux VDA-Umgebung mit dem Linux **XDPing**-Tool auf mögliche Konfigurationsprobleme überprüfen. Weitere Informationen finden Sie unter XDPing.

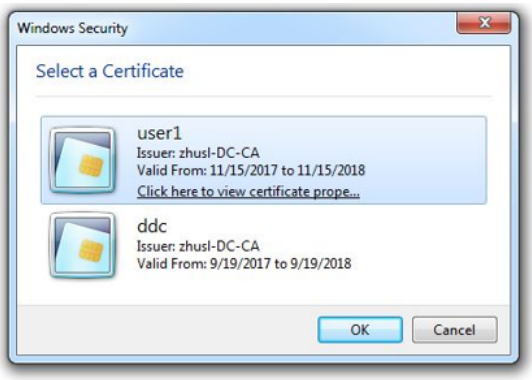
Verwendung

Anmelden am Linux VDA mit einer Smartcard

Sie können sich per Smartcard am Linux VDA in Szenarien mit und ohne Single Sign-On anmelden.

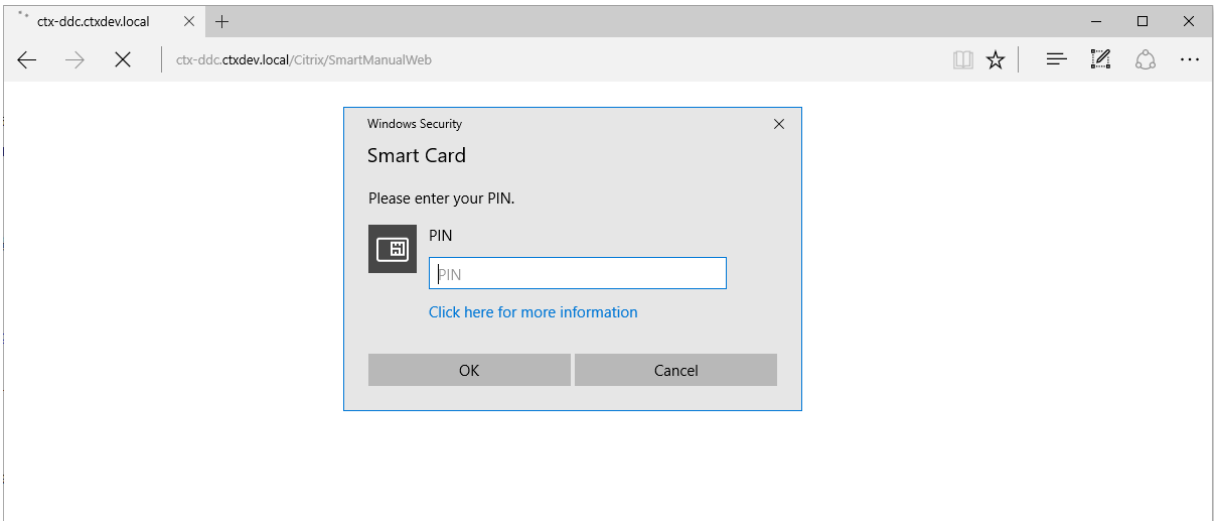
- Bei Verwendung von Single Sign-On werden Sie automatisch mit dem zwischengespeicherten Smartcardzertifikat und der PIN bei StoreFront angemeldet. Wenn Sie eine virtuelle Linux-Desktopsitzung in StoreFront starten, wird die PIN an den Linux VDA zur Smartcardauthentifizierung weitergeleitet.

- Wird kein Single Sign-On verwendet, werden Sie aufgefordert, ein Zertifikat auszuwählen und eine PIN einzugeben, um sich bei StoreFront anzumelden.



Wenn Sie eine Sitzung mit virtuellem Linux-Desktop in StoreFront starten, wird auf dem Linux VDA das nachfolgende Anmeldedialogfeld angezeigt. Der Benutzername wird aus dem Zertifikat auf der Smartcard extrahiert und Sie müssen die PIN zur Anmeldeauthentifizierung erneut eingeben.

Dieses Verhalten ist mit dem des Windows VDA identisch.



Wiederherstellen der Verbindung mit einer Sitzung per Smartcard

Stellen Sie sicher, dass die Smartcard mit dem Clientgerät verbunden ist, um die Verbindung zu einer Sitzung wiederherzustellen. Andernfalls wird nur kurz ein graues Caching-Fenster auf dem Linux VDA angezeigt, da die erneute Authentifizierung ohne Smartcard fehlschlägt. In diesem Fall wird keine weitere Aufforderung angezeigt, um Sie daran zu erinnern, die Smartcard anzuschließen.

In StoreFront wird beim Wiederherstellen einer Verbindung zu einer Sitzung ohne Smartcard eventuell eine Warnmeldung in folgender Form ausgegeben:

Einschränkung

Unterstützung für eingeschränkte Linux-Distributionen und AD-Integrationsmethoden

- Die Smartcard-Passthrough-Authentifizierung unterstützt eingeschränkte Linux-Distributionen und AD-Integrationsmethoden. Siehe folgende Tabelle:

	Winbind	SSSD	Centrify
Debian 11.3	Ja	Ja	Ja
RHEL 9.2/9.0	Ja	Ja	Nein
RHEL 8.8/8.6	Ja	Ja	Ja
RHEL 7.9, CentOS 7.9	Ja	Ja	Ja
Rocky Linux 9.2/9.0	Ja	Ja	Nein
Rocky Linux 8.8/8.6	Ja	Ja	Nein
Ubuntu 22.04/20.04	Ja	Ja	Ja

Richtlinie zum Entfernen der Smartcard

Auf dem Linux VDA wird nur das Standardverhalten für das Entfernen von Smartcards verwendet. Wenn Sie die Smartcard nach der Anmeldung beim Linux VDA entfernen, bleibt die Sitzung weiterhin verbunden und der Sitzungsbildschirm wird nicht gesperrt.

Unterstützung für andere Smartcards und die PKCS#11-Bibliothek

Citrix bietet eine generische Umleitungslösung für Smartcards. Obwohl nur die OpenSC-Smartcard in unserer Supportliste aufgeführt ist, können Sie versuchen, andere Smartcards und die PKCS#11-Bibliothek zu verwenden. Wechseln Sie zu Ihrer speziellen Smartcard oder der PKCS #11-Bibliothek:

1. Ersetzen Sie alle Instanzen von “opensc-pkcs11.so”durch Ihre PKCS#11-Bibliothek.
2. Führen Sie den folgenden Befehl aus, um den Pfad Ihrer PKCS#11-Bibliothek in der Registrierung festzulegen:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
     CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v "
     PKCS11LibPath" -d "PATH"
2 <!--NeedCopy-->
```

   Wobei **PATH** auf Ihre PKCS#11-Bibliothek verweist, z. B. /usr/lib64/pkcs11/opensc-pkcs11.so
3. Deaktivieren Sie die Anmeldung mit Schneller Smartcard auf dem Client.

Zugriff durch nicht authentifizierte (anonyme) Benutzer

April 18, 2024

Sie können Benutzern Zugriff auf Anwendungen und Desktops gewähren, ohne dass die Benutzer Anmeldeinformationen in StoreFront oder der Citrix Workspace-App eingeben müssen. Um nicht authentifizierten Benutzern Zugriff zu gewähren, benötigen Sie einen StoreFront-Store ohne Authentifizierung und müssen den Zugriff für nicht authentifizierte Benutzer in einer Bereitstellungsgruppe aktivieren.

> **Hinweis:**
>
> Der Zugriff durch nicht authentifizierte Benutzer wird nur für domänengebundene VDAs unterstützt.
>
> Der Sitzungsvorabstart wird für nicht authentifizierte Benutzer nicht unterstützt. Der Sitzungsvorabstart wird außerdem nicht von der Citrix Workspace-App für Android unterstützt.

StoreFront-Store ohne Authentifizierung erstellen

1. Wählen Sie im linken Bereich der Citrix StoreFront-Verwaltungskonsole den Knoten **Stores** und klicken Sie im **Aktionsbereich** auf **Store erstellen**.
2. Geben Sie auf der Seite **Storename** einen Namen für den Store ein, klicken Sie auf **Nur nicht authentifizierte (anonyme) Benutzer dürfen auf diesen Store zugreifen** und klicken Sie auf **Weiter**.

Weitere Informationen finden Sie unter Erstellen eines Stores ohne Authentifizierung.

Zugriff nicht authentifizierter Benutzer in einer Bereitstellungsgruppe aktivieren

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Wenn Sie angeben, wer die Anwendungen und Desktops in einer Bereitstellungsgruppe verwenden kann, können Sie nicht authentifizierten Benutzern Zugriff gewähren. Weitere Informationen finden Sie unter
Bereitstellungsgruppen erstellen.

Leerlauf-Timeout für Sitzungen nicht authentifizierter Benutzer festlegen

Für Benutzersitzungen ohne Authentifizierung gilt ein Standardleerlauftimeout von 10 Minuten. Beim Trennen der Verbindung mit dem Client erfolgt automatisch die Abmeldung. Sie können ein benutzerdefiniertes Leerlauf-Timeout über die Registrierungseinstellung **AnonymousUserIdleTime** konfigurieren. Um beispielsweise ein Leerlauf-Timeout von fünf Minuten festzulegen, führen Sie den folgenden Befehl aus:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k  "HKLM\System\
     CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime  -d 0
     x00000005
2 <!--NeedCopy-->
```

Festlegen der maximalen Anzahl nicht authentifizierter Benutzer

Zum Festlegen der maximalen Anzahl nicht authentifizierter Benutzer verwenden Sie den Registrierungsschlüssel **MaxAnonymousUserNumber**. Mit dieser Einstellung wird die Anzahl gleichzeitiger Sitzungen nicht authentifizierter Benutzer auf einem Linux VDA beschränkt. Verwenden Sie das Tool **ctxreg**, um diese Registrierungseinstellung zu konfigurieren. Um den Wert beispielsweise auf 32 festzulegen, führen Sie den folgenden Befehl aus:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg update -k  "HKLM\System\
     CurrentControlSet\Control\Citrix"  -v MaxAnonymousUserNumber  -d  0
     x00000020
2 <!--NeedCopy-->
```

> **Wichtig:**
>
> Begrenzen Sie die Anzahl der Sitzungen nicht authentifizierter Benutzer. Wenn zu viele Sitzungen gleichzeitig gestartet werden, können Probleme auf dem VDA (z. B. Arbeitsspeichermangel) auftreten.

Problembehandlung

Berücksichtigen Sie beim Konfigurieren von Sitzungen nicht authentifizierter Benutzer Folgendes:

- **Fehler beim Anmelden bei einer Sitzung mit nicht authentifiziertem Benutzer.**

Prüfen Sie, ob die Registrierung mit folgendem Parameter (Einstellung auf 0) aktualisiert wurde:

```
sudo /opt/Citrix/VDA/bin/ctxreg read -k "HKLM\System\CurrentControlSet\Control\Citrix" -v MaxAnonymousUserNumber
<!--NeedCopy-->
```

Prüfen Sie, ob der Dienst **ncsd** ausgeführt wird und die Kennwortzwischenspeicherung **passwd** zulässt:

```
ps uax | grep nscd
cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
<!--NeedCopy-->
```

Legen Sie die Cachevariable **passwd** auf **no** fest, wenn diese aktiviert ist, und starten Sie den Dienst **ncsd** neu. Nach dem Ändern dieser Konfiguration müssen Sie möglicherweise den Linux VDA neu installieren.

- **Die Schaltfläche zum Sperren des Bildschirms wird in Sitzungen nicht authentifizierter Benutzer bei KDE angezeigt.**

Die Schaltfläche und das Menü zum Sperren des Bildschirms sind in Sitzungen nicht authentifizierter Benutzer standardmäßig deaktiviert. Sie werden jedoch ggf. weiterhin in KDE angezeigt. Zum Deaktivieren der Schaltfläche und des Menüs zum Sperren des Bildschirms in KDE für einen bestimmten Benutzer fügen Sie der Konfigurationsdatei **$Home/.kde/share/config/kdeglobals** die nachfolgend aufgeführten Zeilen hinzu. Beispiel:

```
[KDE Action Restrictions]
action/lock_screen=false
<!--NeedCopy-->
```

Wenn der Parameter `KDE Action Restrictions` jedoch in einer globalen `kdeglobals` -Datei wie `/usr/share/kde-settings/kde-profile/default/share/config/kdeglobals` als unveränderlich konfiguriert ist, hat die Benutzerkonfiguration keine Auswirkung.

Zum Beheben dieses Problems entfernen Sie entweder das Tag `[$i]` aus dem Abschnitt `[KDE Action Restrictions]` der `kdeglobals`-Datei oder deaktivieren Sie die Schaltfläche und das Menü zum Sperren des Bildschirms direkt über die systemweite Konfiguration. Weitere Informationen zur KDE-Konfiguration finden Sie auf der Seite KDE System Administration/Kiosk/Keys.

Datei

January 8, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Dateien kopieren und einfügen
- Dateiübertragung

Dateien kopieren und einfügen

January 8, 2024

Über Kontextmenü oder mit Tastenkombinationen können Benutzer Dateien zwischen einer Sitzung und einem lokalen Client kopieren und einfügen. Für dieses Feature ist Citrix Virtual Apps and Desktops 2006 oder höher und Citrix Workspace-App 1903 oder höher für Windows erforderlich.

Zum Kopieren und Einfügen von Dateien muss Folgendes sichergestellt werden:

- Die Anzahl von Dateien darf 20 nicht überschreiten.
- Die Dateigröße darf 200 MB nicht überschreiten.
- Der Nautilus-Dateimanager ist auf der Maschine verfügbar, auf dem Sie den Linux VDA installiert haben.

Unterstützte Linux-Distributionen

Das **Feature zum Kopieren und Einfügen von Dateien** ist für alle Linux-Distributionen verfügbar, die der Linux VDA unterstützt.

Relevante Richtlinien

Die folgenden Zwischenablagenrichtlinien sind für die Konfiguration des Features relevant. Weitere Informationen zu den Zwischenablagenrichtlinien finden Sie in der Liste der unterstützten Richtlinien.

- Clientzwischenablagenumleitung
- Aktualisierungsmodus für die Zwischenablageauswahl
- Aktualisierungsmodus für die Primärauswahl

> **Hinweis:**
>
> Um die Funktion zum Kopieren und Einfügen von Dateien zu deaktivieren, legen Sie die Richtlinie zur **Clientzwischenablagenumleitung** in Citrix Studio auf **Nicht zugelassen** fest.

Einschränkungen

- Ausschneiden wird nicht unterstützt. Versuche des Ausschneidens einer Datei werden als Kopiervorgang behandelt.
- Drag & Drop wird nicht unterstützt.
- Das Kopieren von Verzeichnissen wird nicht unterstützt.
- Das Kopieren und Einfügen von Dateien muss einzeln ausgeführt werden. Erst wenn eine Datei kopiert und eingefügt wurde, kann die nächste Datei kopiert werden.

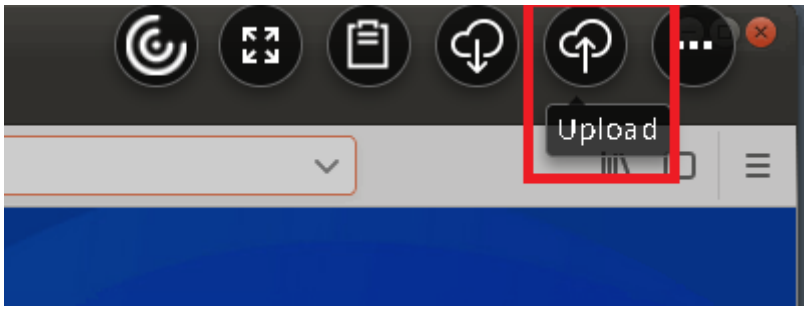
Dateiübertragung

January 8, 2024

Dateiübertragungen zwischen dem Linux VDA und dem Clientgerät werden unterstützt. Diese Funktion ist verfügbar, wenn auf dem Clientgerät ein Webbrowser ausgeführt wird, der das HTML5-Sandbox-Attribut unterstützt. Das HTML5-Sandbox-Attribut ermöglicht Benutzern den Zugriff auf virtuelle Desktops und Apps mit der Citrix Workspace-App für HTML5 und für Chrome.

> **Hinweis:**
>
> Dateiübertragung ist für die Citrix Workspace-App für HTML5 und Chrome verfügbar.

Innerhalb von Sitzungen mit veröffentlichten Apps bzw. Desktops ermöglicht die Dateiübertragung das Hoch- und Herunterladen von Dateien zwischen Linux VDA und Clientgerät. Um Dateien vom Clientgerät auf den Linux VDA hochzuladen, klicken Sie auf der Symbolleiste der Citrix Workspace-App auf das Symbol **Hochladen** und wählen Sie die gewünschte Datei aus. Um Dateien vom Linux VDA auf das Clientgerät herunterzuladen, klicken Sie auf das Symbol **Herunterladen**. Sie können während des Uploads und Downloads Dateien hinzufügen. Sie können bis zu 100 Dateien gleichzeitig übertragen.



> **Hinweis:**
>
> Zum Hochladen und Herunterladen von Dateien zwischen Linux VDA und Clientgerät müssen Sie

> die Symbolleiste der Citrix Workspace-App aktivieren.
> Sie können eine Version der Citrix Workspace-App verwenden, mit der Sie Dateien per Drag & Drop verschieben können.

Der automatische Download ist eine Erweiterung der Dateiübertragung. Dateien, die Sie in das Verzeichnis **Auf eigenem Gerät speichern** auf dem VDA herunterladen oder verschieben, werden automatisch an das Clientgerät übertragen.

> **Hinweis:**
>
> Für den automatischen Download müssen die Richtlinien **Dateiübertragungen zwischen Desktop und Client zulassen** und **Dateien vom Desktop herunterladen** auf **Zulässig** festgelegt sein.

Beispiele von Anwendungsfällen für den automatischen Download:

- Download von Dateien in **Auf eigenem Gerät speichern**

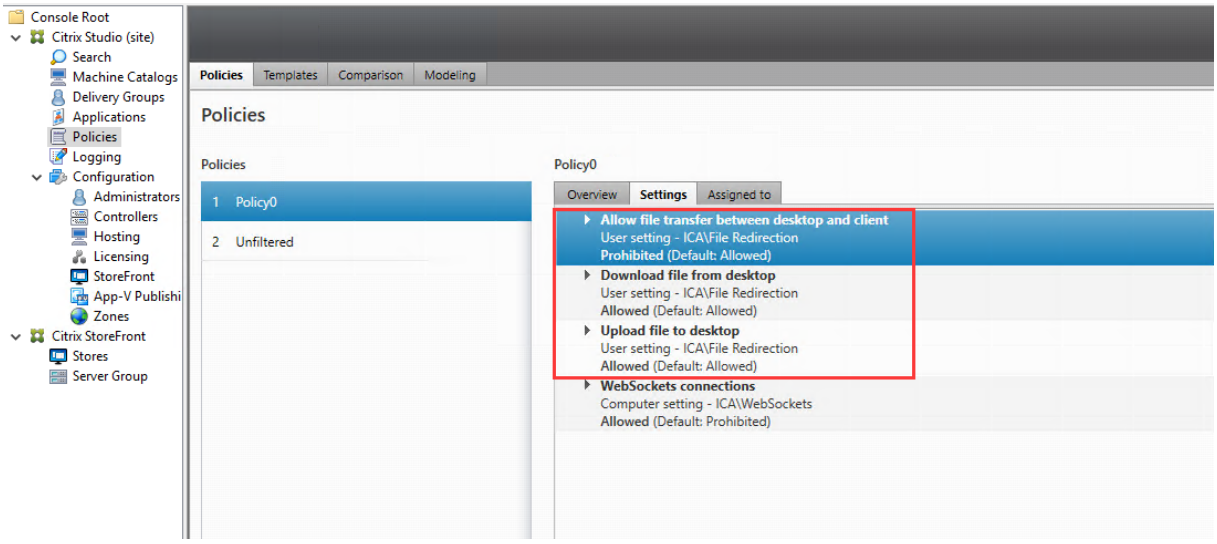
  In Sitzungen mit veröffentlichten Desktops und Webbrowser-Apps können Sie von Websites heruntergeladene Dateien zur automatischen Übertragung auf das Clientgerät im Verzeichnis **Auf eigenem Gerät speichern** auf dem VDA speichern. Damit der automatische Download funktioniert, legen Sie das Standard-Downloadverzeichnis des Sitzungs-Webbrowsers auf **Auf eigenem Gerät speichern** und in dem Webbrowser, in dem die Citrix Workspace-App für HTML5 oder Chrome ausgeführt wird, ein lokales Downloadverzeichnis fest.

- Verschieben oder Kopieren von Dateien in **Auf eigenem Gerät speichern**

  Wählen Sie in Sitzungen mit veröffentlichten Desktops die Zieldateien aus und verschieben oder kopieren Sie diese in das Verzeichnis **Auf eigenem Gerät speichern**, damit sie auf dem Clientgerät verfügbar sind.

Dateiübertragungsrichtlinien

Sie können Citrix Studio verwenden, um die Dateiübertragungsrichtlinien festzulegen. In der Standardeinstellung ist die Dateiübertragung aktiviert.



Richtlinienbeschreibungen:

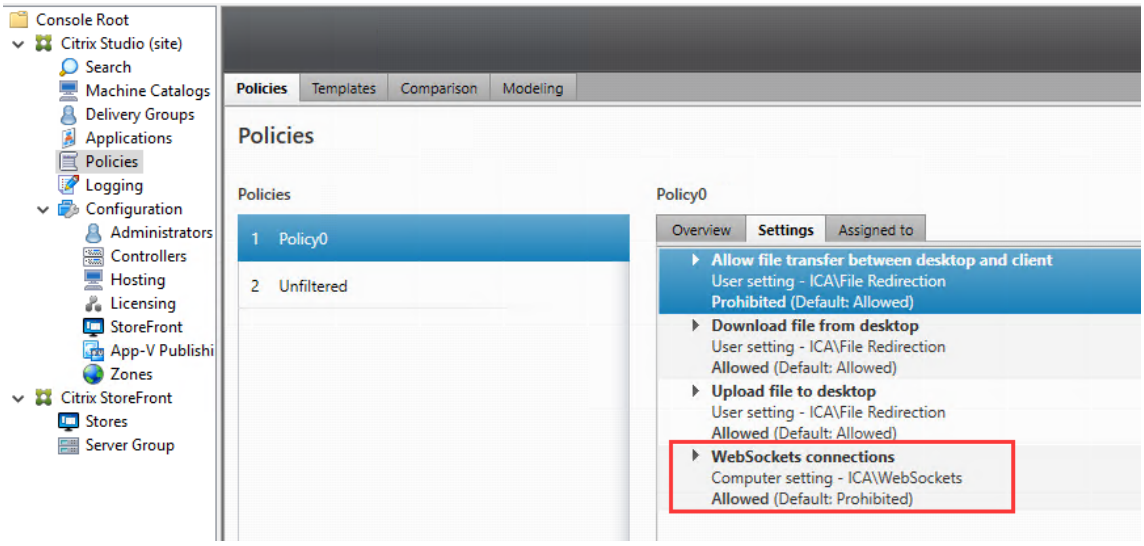
- **Dateiübertragungen zwischen Desktop und Client zulassen:** Die Option ermöglicht oder verhindert Dateiübertragungen zwischen den Citrix Virtual Apps and Desktops-Sitzungen und den Clientgeräten.
- **Dateien von Desktop herunterladen:** Die Option ermöglicht oder verhindert das Herunterladen von Dateien aus den Citrix Virtual Apps and Desktops-Sitzungen auf die Clientgeräte.
- **Dateien auf Desktop hochladen:** Die Option ermöglicht oder verhindert das Herunterladen von Dateien von den Clientgeräten in die Citrix Virtual Apps and Desktops-Sitzungen.

> **Hinweis:**
>
> Um sicherzustellen, dass die Richtlinien **Dateien von Desktop herunterladen** und **Dateien auf Desktop hochladen** angewendet werden, setzen Sie die Richtlinie **Dateiübertragungen zwischen Desktop und Client zulassen** auf **Zulässig**.

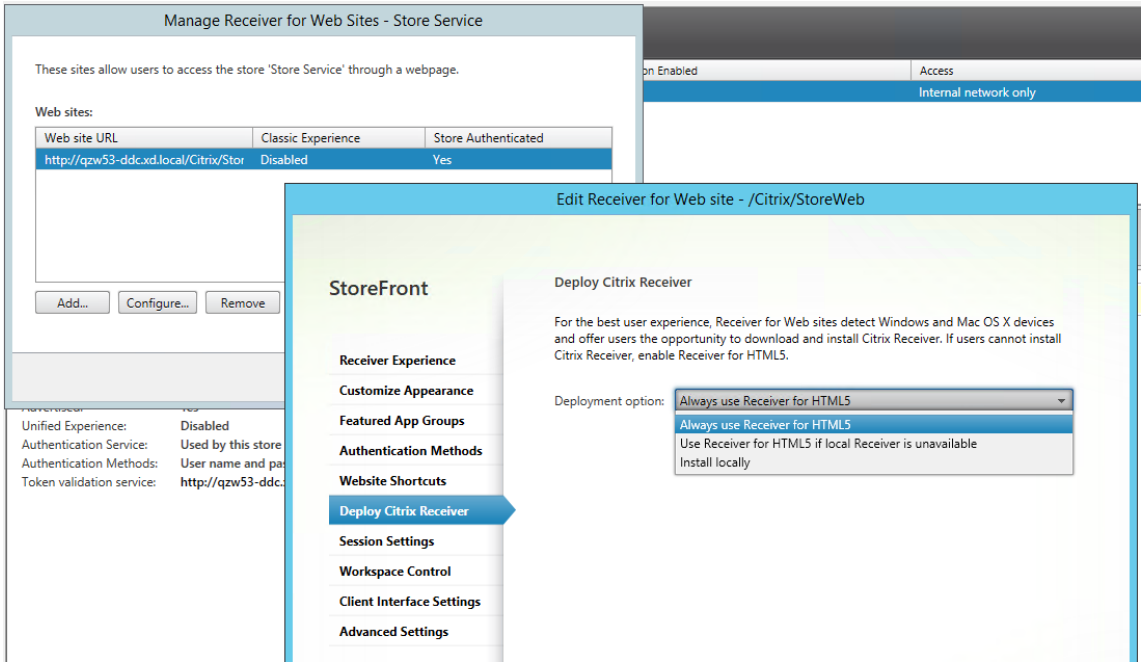
Verwendung

Um das Dateiübertragungsfeature über die Citrix Workspace-App für HTML5 zu verwenden:

1. Legen Sie in Citrix Studio für die Richtlinie **WebSockets-Verbindungen** die Einstellung **Zugelassen** fest.



2. Aktivieren Sie in Citrix Studio die Dateiübertragung über die oben beschriebenen Dateiübertragungsrichtlinien.
3. Klicken Sie in der Citrix StoreFront-Verwaltungskonsole auf **Stores**, wählen Sie den Knoten **Receiver für Web-Sites verwalten** und aktivieren Sie Citrix Receiver für HTML5, indem Sie die Option **Immer Receiver für HTML5 verwenden** wählen.



4. Starten Sie eine virtuelle Desktop- oder Webbrowser-App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux VDA und dem Clientgerät durch.

Um das Dateiübertragungsfeature über die Citrix Workspace-App für Chrome zu verwenden:

1. Aktivieren Sie die Dateiübertragung über die oben beschriebenen Dateiübertragungsrichtlin-

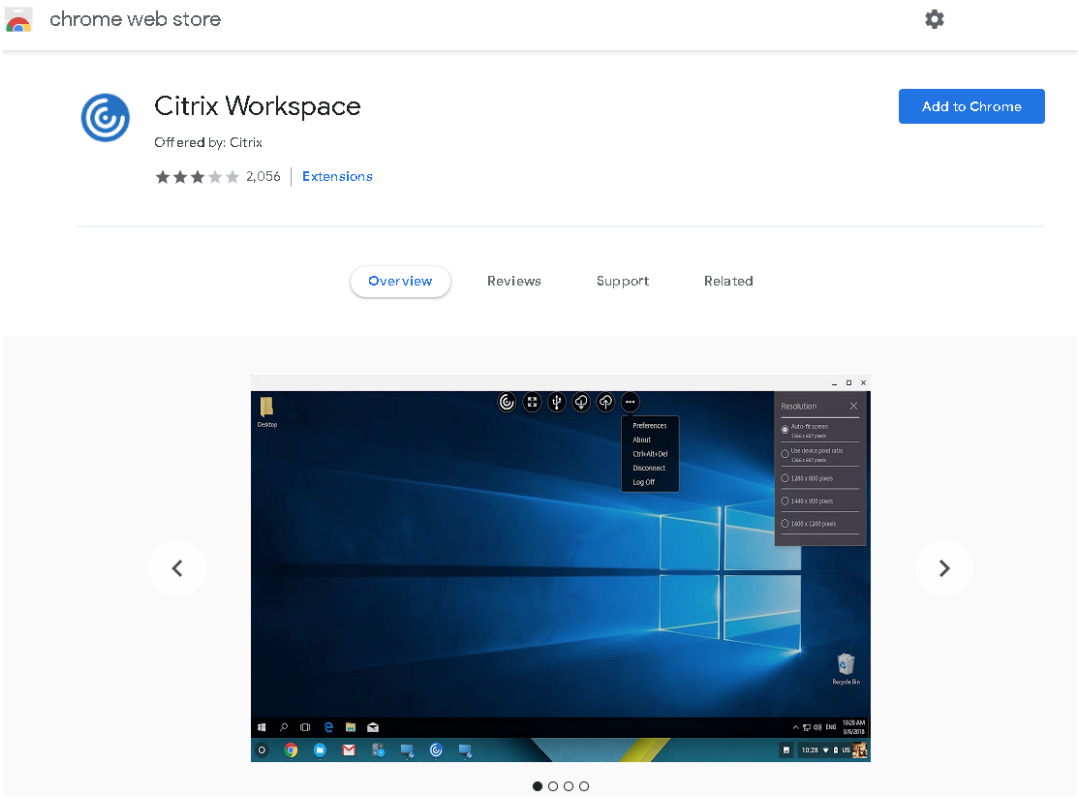
ien.

2. Rufen Sie Citrix Workspace-App aus dem Chrome Web Store ab.

   Überspringen Sie diesen Schritt, wenn Sie bereits Citrix Workspace-App für Chrome der Seite “Chrome-Apps”hinzugefügt haben.

   a) Geben Sie **Citrix Workspace für Chrome** in das Suchfeld von Google Chrome ein. Klicken Sie auf das Suchsymbol.

   b) Klicken Sie unter den Suchergebnissen auf die URL zum Chrome Web Store, in dem die Citrix Workspace-App verfügbar ist.



   c) Klicken Sie auf **Zu Chrome hinzufügen**, um die Citrix Workspace-App zu Google Chrome hinzuzufügen.

3. Klicken Sie auf der Seite “Chrome Apps”auf “Citrix Workspace-App für Chrome”.
4. Geben Sie die URL des StoreFront-Stores ein, zu dem eine Verbindung hergestellt werden soll.

   Überspringen Sie diesen Schritt, wenn Sie die URL bereits vorher eingegeben haben.

5. Starten Sie eine virtuelle Desktop- oder App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux VDA und dem Clientgerät durch.

Grafik

January 8, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Automatische DPI-Skalierung
- Clientakkustatusanzeige
- Grafikkonfiguration und -feineinstellung
- HDX-Bildschirmfreigabe
- Nicht virtualisierte GPUs
- Sitzungswasserzeichen
- Progressive Anzeige für Thinwire

Automatische DPI-Skalierung

April 18, 2024

Der Linux VDA unterstützt die automatische DPI-Skalierung. Wenn ein Benutzer eine Sitzung mit virtuellem Desktop oder virtueller Anwendung öffnet, wird der DPI-Wert in der Sitzung automatisch an die DPI-Einstellung auf dem Client angepasst.

Beachten Sie folgende Überlegungen zu diesem Feature:

- Für das Feature müssen Sie die DPI-Anpassung für Citrix Workspace aktivieren. Bei Verwendung der Citrix Workspace-App für Windows muss die Option **Nein, native Auflösung verwenden** ausgewählt sein. Weitere Informationen zum Konfigurieren der DPI-Skalierung für die Citrix Workspace-App für Windows finden Sie unter DPI-Skalierung.
- In Szenarien mit mehreren verwendeten Bildschirmen muss auf jedem Bildschirm dieselbe DPI-Einstellung konfiguriert sein. Szenarien mit unterschiedlichen DPI-Einstellungen werden nicht unterstützt. Wenn unterschiedliche DPI-Einstellungen vorliegen, wendet der Linux VDA auf alle Bildschirme den kleinsten DPI-Wert an.
- Das Feature ist für MATE, GNOME, GNOME Classic und KDE aktiviert. Beachten Sie mit KDE oder MATE Folgendes:
  - Für virtuelle Linux-Desktops in einer KDE-Desktopumgebung:
    - Wir empfehlen die Verwendung von KDE Plasma 5 oder höher.

        * Wenn Sie die DPI-Einstellungen auf dem Client ändern, während Sitzungen ausgeführt werden, müssen Benutzer sich ab- und erneut anmelden.
    - Für virtuelle Linux-Desktops in einer MATE-Desktopumgebung:
        * Es werden nur die Skalierungsfaktoren 1 und 2 unterstützt.
        * Wenn Sie die DPI-Einstellungen auf dem Client ändern, während Sitzungen ausgeführt werden, müssen Benutzer sich ab- und erneut anmelden.

- Der DPI-Wert in der virtuellen Sitzung wird automatisch an die DPI-Einstellung auf dem Client angepasst. Derzeit unterstützt das Feature nur ganzzahlige Skalierungsfaktoren, z. B. 100 % und 200 %. Wenn auf dem Client ein Skalierungsfaktor vom Typ "Bruchzahl"konfiguriert ist, wird der DPI-Wert der virtuellen Sitzung gemäß der folgenden Tabelle in einen ganzzahligen Skalierungsfaktor geändert. Beispiel: Bei einem Skalierungsfaktor von 125 % ändert sich der DPI-Wert in 100 %.

Skalierungsfaktor auf dem Client	DPI der Remotesitzung
Weniger als oder gleich 174 %	96 (1 x 96)
175 %–274 %	192 (2 x 96)
275 %–399 %	288 (3 x 96)
Größer als oder gleich 400 %	384 (4 x 96)

Clientakkustatusanzeige

January 8, 2024

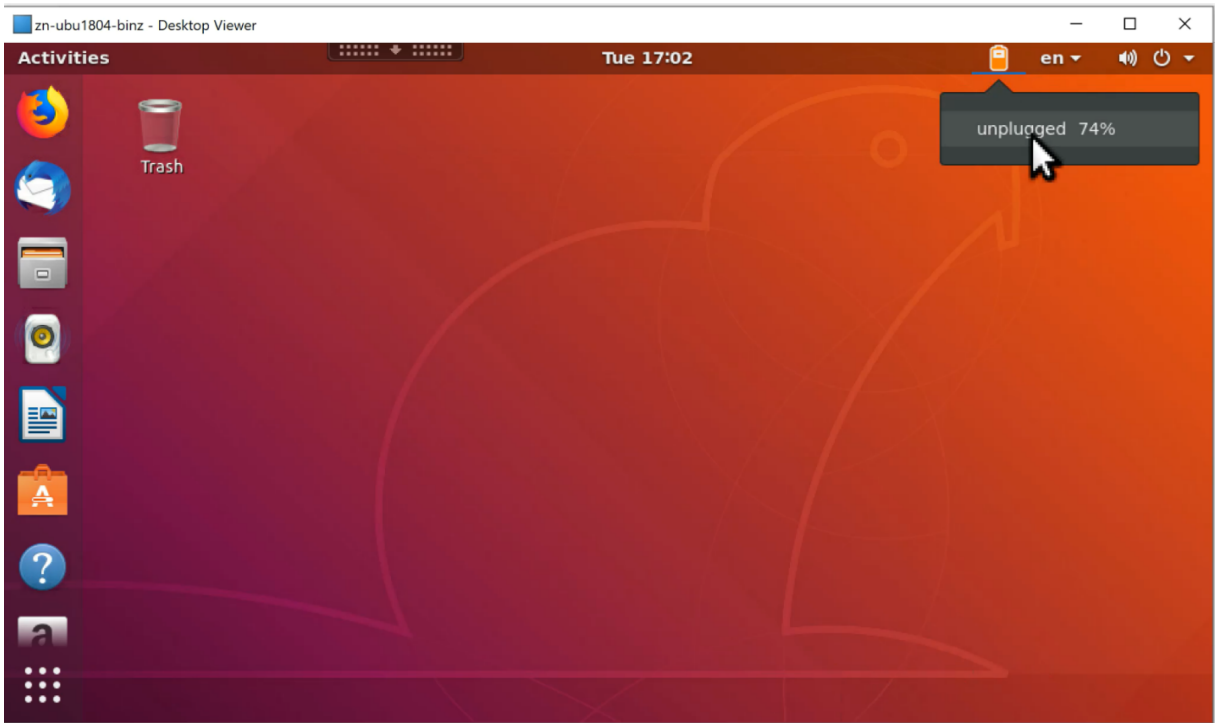
Der Linux VDA kann den Akkustatus von Clientgeräten zu virtuellen Desktops umleiten und dort anzeigen. Dieses Feature ist standardmäßig aktiviert und für folgende Versionen der Citrix Workspace-App verfügbar:

- Citrix Workspace-App für iOS
- Citrix Workspace-App für Linux
- Citrix Workspace-App für Mac (Version 2204.1 wird nicht unterstützt)
- Citrix Workspace-App für Windows (Version 2204.1 wird nicht unterstützt)

Übersicht

Wenn Benutzer einen virtuellen Desktop öffnen, wird im Linux-Infobereich ein Akkusymbol angezeigt. Dieses Symbol zeigt den Akkustatus ihrer Clientgeräte an. Klicken Sie auf das Akkusymbol, um die

verbleibende Akkulaufzeit (in Prozent) zu überprüfen. Ein Beispiel sehen Sie im folgenden Screenshot:



Je nach Akkustatus werden unterschiedliche Symbole angezeigt. Eine Übersicht finden Sie in der folgenden Tabelle:

Akkusymbol	Ladezustand	Akkustand	Verbleibende Akkulaufzeit in Prozent
	Akku wird geladen (“+” -Symbol)	Hoch (grüner Akku)	=80 %
	Akku wird geladen (“+” -Symbol)	Mittel (orangefarbener Akku)	= 20 % und < 80 %
	Akku wird geladen (“+” -Symbol)	Niedrig (roter Akku)	< 20 %
	Akku wird nicht geladen (“-“-Symbol)	Hoch (grüner Akku)	=80 %

Akkusymbol	Ladezustand	Akkustand	Verbleibende Akkulaufzeit in Prozent
	Akku wird nicht geladen (“-“-Symbol)	Mittel (orangefarbener Akku)	= 20 % und < 80 %
	Akku wird nicht geladen (“-“-Symbol)	Niedrig (roter Akku)	< 20 %
	Unbekannt	Unbekannt	Unbekannt

Konfiguration

Die Client-Akkustatusanzeige ist standardmäßig aktiviert.

Führen Sie folgenden Befehl aus, um das Feature zu deaktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
   Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000000"
<!--NeedCopy-->
```

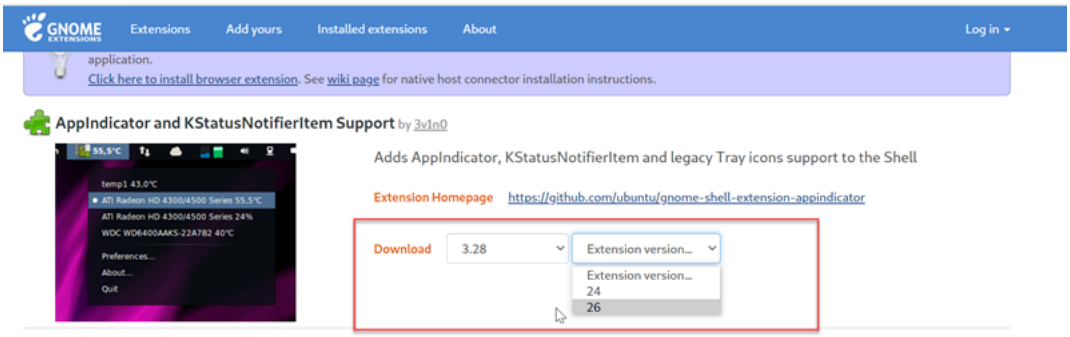
Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
   Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000001"
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die oben genannten Befehle wirken sich auf das Bildschirmtastatur-Feature aus, das Mobile Receiver Virtual Channel (MRVC) mit der Client-Akkustatusanzeige verwendet.

Führen Sie je nach vorliegender Distribution folgende zusätzlichen Schritte aus:

1. Bei Verwendung von mit GNOME installiertem RHEL 8.x oder SUSE 15.x installieren Sie eine kompatible Erweiterung für die GNOME-Shell, um die AppIndicator-Unterstützung zu aktivieren:
   a) Führen Sie den Befehl `gnome-shell --version` aus, um Ihre GNOME-Shellversion zu überprüfen.
   b) Laden Sie eine kompatible Erweiterung für die GNOME-Shell von https://extensions.gnome.org/extension/615/appindicator-support herunter. Wenn Ihre Shellversion beispielsweise 3.28 ist, können Sie 24 oder 26 als Erweiterungsversion auswählen.



c) Entpacken Sie das heruntergeladene TAR-Paket. Stellen Sie sicher, dass der Wert **"uuid"** in der Datei **metadata.json** im Paket auf **appindicatorsupport@rgcjonas.gmail.com** gesetzt ist.

d) Führen Sie den Befehl `mv` aus, um das Verzeichnis **appindicatorsupport@rgcjonas.gmail.com** unter `/usr/share/gnome-shell/extensions/` zu speichern.

e) Führen Sie den Befehl `chmod a+r metadata.json` aus, um die Datei **metadata.json** für andere Benutzer lesbar zu machen.

> **Tipp:**
>
> Die Datei **metadata.json** im Verzeichnis **appindicatorsupport@rgcjonas.gmail.com** kann standardmäßig nur vom Root-Benutzer gelesen werden. Um die Bildschirmfreigabe zu unterstützen, machen Sie die Datei **metadata.json** auch für andere Benutzer lesbar.

f) Installieren Sie GNOME Tweaks.

g) Laden Sie in der Desktopumgebung Ihre GNOME-Shell neu, indem Sie nacheinander die Tasten `Alt+F2`, `r` und `Enter` drücken oder aber den Befehl `killall -SIGQUIT gnome-shell` ausführen.

h) Führen Sie in der Desktopumgebung GNOME Tweaks aus und aktivieren Sie **KStatusNotifierItem/AppIndicator Support** im Tweaks-Tool.

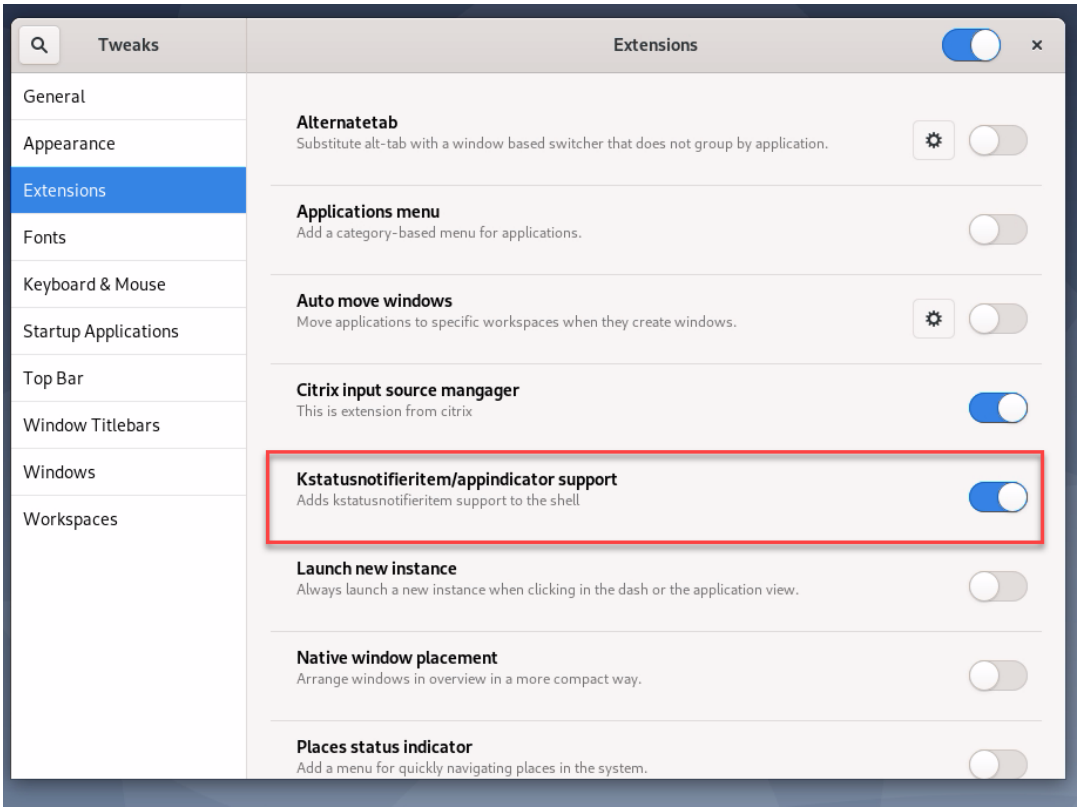
2. Bei Verwendung von mit GNOME installiertem Debian 11.3 führen Sie die folgenden Schritte aus, um GNOME-Taskleistensymbole zu installieren und zu aktivieren:

a) Führen Sie den Befehl `sudo apt install gnome-shell-extension-appindicator` aus. Sie müssen sich möglicherweise abmelden und erneut anmelden, damit die Erweiterung von GNOME erkannt wird.

b) Suchen Sie im Bildschirm **Activities** nach Tweaks.

c) Wählen Sie im Tweaks-Tool **Extensions**.

d) Aktivieren Sie **Kstatusnotifieritem/appindicator support**.



Grafikkonfiguration und -feineinstellung

January 8, 2024

Dieser Artikel erläutert die Grafikkonfiguration und -optimierung für den Linux VDA.

Weitere Informationen finden Sie unter Systemanforderungen und Installationsübersicht.

Konfiguration

Optimierung für 3D-Grafikworkload

Mit dieser Einstellung werden die am besten für grafikintensive Workloads geeigneten Standardwerte konfiguriert. Aktivieren Sie diese Einstellung für Benutzer die vorwiegend mit grafikintensiven Anwendungen arbeiten. Wenden Sie diese Richtlinie nur an, wenn eine GPU für die Sitzung verfügbar ist. Alle anderen Einstellungen, die die von dieser Richtlinie festgelegten Standardeinstellungen explizit außer Kraft setzen, haben Vorrang.

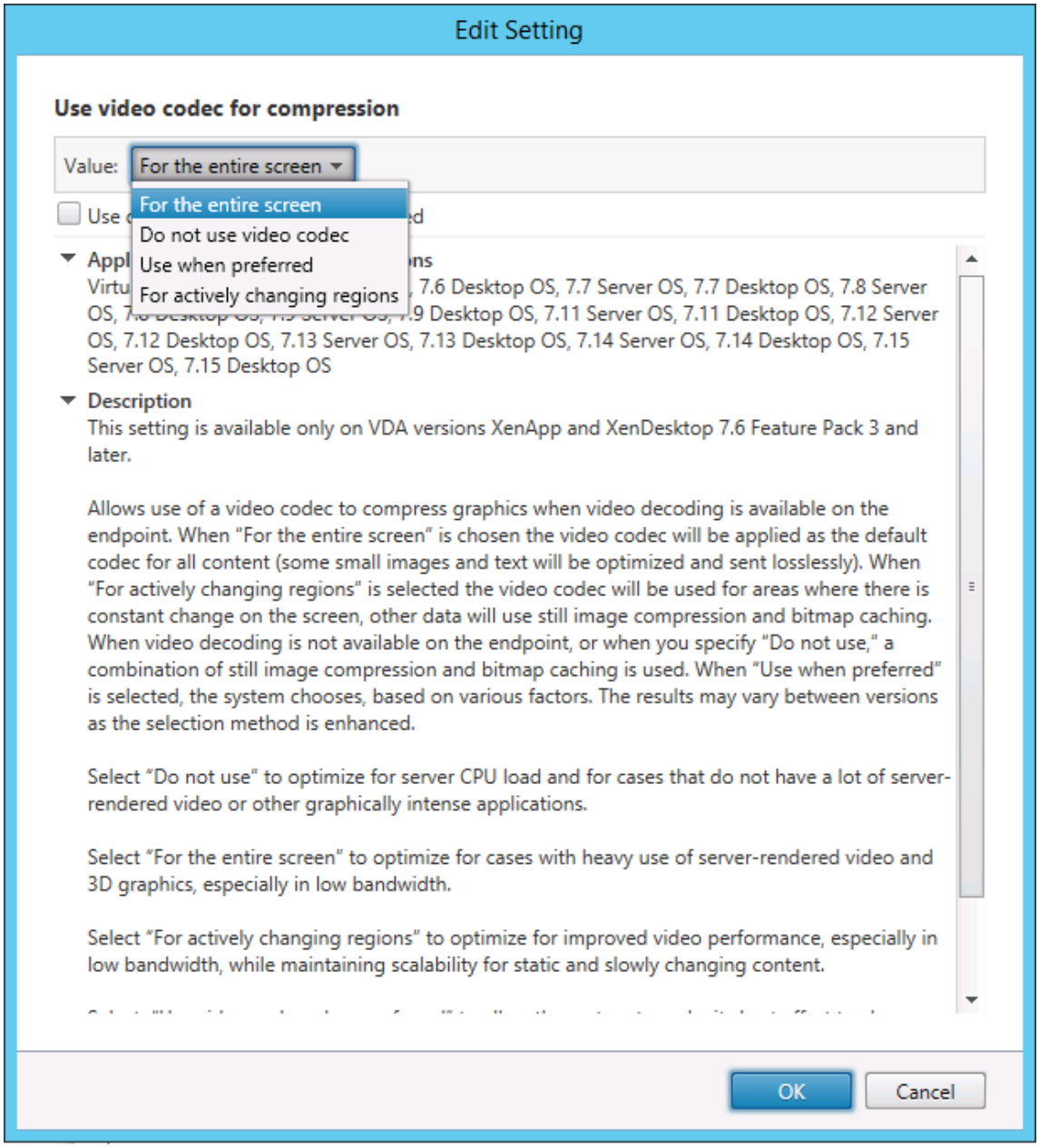
Standardmäßig ist die **Optimierung für 3D-Grafik-Workloads** deaktiviert.

Videocodec für die Komprimierung

Thinwire ist die bei Linux VDAs verwendete Technologie für das Anzeigeremoting. Durch sie können auf einer Maschine erzeugte Grafiken auf eine andere Maschine für die Anzeige übertragen werden (normalerweise über ein Netzwerk).

Die Richtlinie **Videocodec für Komprimierung verwenden** bestimmt den Standardgrafikmodus und bietet folgende Optionen für verschiedene Anwendungsfälle:

- **Verwenden, wenn bevorzugt**. Dies ist die Standardeinstellung. Eine zusätzliche Konfiguration ist nicht erforderlich. Dies stellt sicher, dass Thinwire für alle Citrix Verbindungen ausgewählt und für Skalierbarkeit, Bandbreite und bessere Bildqualität bei typischen Desktoparbeitslasten optimiert wird.
- **Für den gesamten Bildschirm**. Thinwire wird mit Vollbild-H.264 oder -H.265 zur Optimierung der Benutzererfahrung und Bandbreite, insbesondere bei intensiver 3D-Grafiknutzung, verwendet. Sitzungswasserzeichen wird unterstützt, wenn **Für den gesamten Bildschirm** ausgewählt ist, oder wenn **Verwenden, wenn bevorzugt** ausgewählt und Optimierung für 3D-Grafikworkload aktiviert ist.
- **Für aktive Änderungsbereiche**. Die Technologie für adaptive Anzeige von Thinwire identifiziert Bewegtbilder (Video, 3D In Motion). H.264 oder H.265 wird nur in dem Bildschirmbereich verwendet, in dem das Bild sich bewegt. Mit der selektiven Verwendung des H.264- oder H.265-Videocodecs können Bildschirmsegmente, die häufig mit dem H.264- oder H.265-Videocodec aktualisiert werden, von HDX Thinwire erkannt und codiert werden. Für den übrigen Bildschirm (einschließlich Text und Fotos) werden weiterhin die Standbildkomprimierung (JPEG, RLE) und das Bitmapcaching verwendet. Dies verbraucht weniger Bandbreite und führt zu einer verbesserten Anzeige von Videoinhalten, verbunden mit verlustfreiem Text und hoher Bildqualität. Die selektive Verwendung von H.265 wird nicht unterstützt, wenn die Richtlinie **Bildqualität** auf **Immer verlustfrei** oder **Zu verlustfrei verbessern** festgelegt ist.



Einige weitere Richtlinieneinstellungen, einschließlich der nachfolgend aufgeführten Einstellungen der Richtlinie "Visuelle Anzeige", können zur Optimierung der Anzeigeremoting-Leistung verwendet werden:

- **Bevorzugte Farbtiefe für einfache Grafiken**
- **Frameratesollwert**
- **Bildqualität**

H.265-/H.264-Hardwarekodierung

Die Richtlinie **Hardwarecodierung für Videocodec verwenden** ermöglicht das Komprimieren von Bildschirmelementen mit dem Videocodec mithilfe der GPU-Hardwarebeschleunigung (falls verfügbar). Die GPU-Hardwarebeschleunigung optimiert die Ressourcenauslastung der Hardware und verbessert die FPS-Leistung (Frames pro Sekunde).

Die GPU-Hardwarebeschleunigung umfasst alle Grafikmodi, die in der Richtlinie Videocodec zur Komprimierung verwenden festgelegt sind:

- **Verwenden, wenn bevorzugt**
- **Für den gesamten Bildschirm**
- **Für aktive Änderungsbereiche**

Gehen Sie wie folgt vor, um die Hardwarevideokomprimierung zu aktivieren:

1. Legen Sie die Richtlinie **Hardwarecodierung für Videocodec verwenden** auf **Aktiviert** fest.
2. Legen Sie **Videocodec zur Komprimierung verwenden** auf **Verwenden, wenn bevorzugt**, **Für den gesamten Bildschirm** oder **Für aktive Änderungsbereiche** fest. Vergewissern Sie sich, dass die Option nicht auf **Videocodec nicht verwenden** festgelegt ist.

Der H.265-Videocodec muss auf dem VDA und in der Citrix Workspace-App unterstützt und aktiviert sein. Wenn der H.265-Videocodec weder vom Linux VDA noch von der Citrix Workspace-App unterstützt wird, wird die Richtlinieneinstellung **H.265-Decodierung für Grafiken** ignoriert und Sitzungen greifen auf den H.264-Videocodec zurück. Wenn GPU-Hardware nicht verfügbar ist, wird die CPU-basierte Codierung mit dem Software-Videocodec verwendet.

Informationen zum Aktivieren der H.265-Hardwarecodierung auf dem Client finden Sie unter H.265-Videocodierung.

Der Linux VDA unterstützt H.265 für die Hardwarebeschleunigung von Grafiken und Videos auf den folgenden Clients:

- Citrix Receiver für Windows 4.10 bis 4.12
- Citrix Workspace-App 1808 für Windows und höher

Verlustfreie H.265-/H.264-Komprimierung

Die verlustfreie H.265-/H.264-Komprimierung ist für die HDX 3D PRO-Hardwarebeschleunigung mit NVIDIA-GPUs verfügbar. Für die verlustfreie H.265-Komprimierung ist die Citrix Workspace-App 2305 für Windows und höher erforderlich. Für die verlustfreie H.264-Komprimierung sind die folgenden Clients erforderlich:

- Citrix Workspace-App 2303 für Windows und höher

- Citrix Workspace-App 2301 für Mac und höher mit dem Apple M1-Chip

Gehen Sie wie folgt vor, um die verlustfreie H.265-/H.264-Komprimierung zu aktivieren:

1. Legen Sie die Richtlinie **Hardwarecodierung für Videocodec verwenden** auf **Aktiviert** fest.
2. Legen Sie die Richtlinie **Videocodec zur Komprimierung verwenden** auf **Für den gesamten Bildschirm** fest.
3. Legen Sie die Richtlinie **Bildqualität** auf **Immer verlustfrei** oder **Zu verlustfrei verbessern** fest.

Visuell verlustfreie Komprimierung zulassen

Mit der Richtlinie **Visuell verlustfreie Komprimierung zulassen** wird für Grafiken **visuell** verlustfreie Komprimierung statt echter verlustfreier Komprimierung verwendet. Visuell verlustfreie Komprimierung steigert im Vergleich zu echter verlustfreier Komprimierung die Leistung, hat jedoch geringe Verluste, die für das Auge nicht erkennbar sind. Durch diese Einstellung ändert sich, wie die Einstellungswerte für die **Bildqualität** verwendet werden.

Die Richtlinie **Visuell verlustfreie Komprimierung zulassen** ist standardmäßig deaktiviert. Um die **visuell** verlustfreie Komprimierung zu aktivieren, setzen Sie **Visuell verlustfreie Komprimierung zulassen** auf **Aktiviert** und die Richtlinie für **visuelle Qualität** auf **Zu verlustfrei verbessern**.

Wenn die Richtlinie **Videocodec für Komprimierung verwenden** auf **Videocodec nicht verwenden** festgelegt ist, wird die **visuell** verlustfreie Komprimierung auf die statische Bildcodierung angewendet. Wenn die Richtlinie **Videocodec für Komprimierung verwenden** auf einen anderen Grafikmodus als **Videocodec nicht verwenden** festgelegt ist, wird die **visuell** verlustfreie Komprimierung auf die H.264-Codierung angewendet.

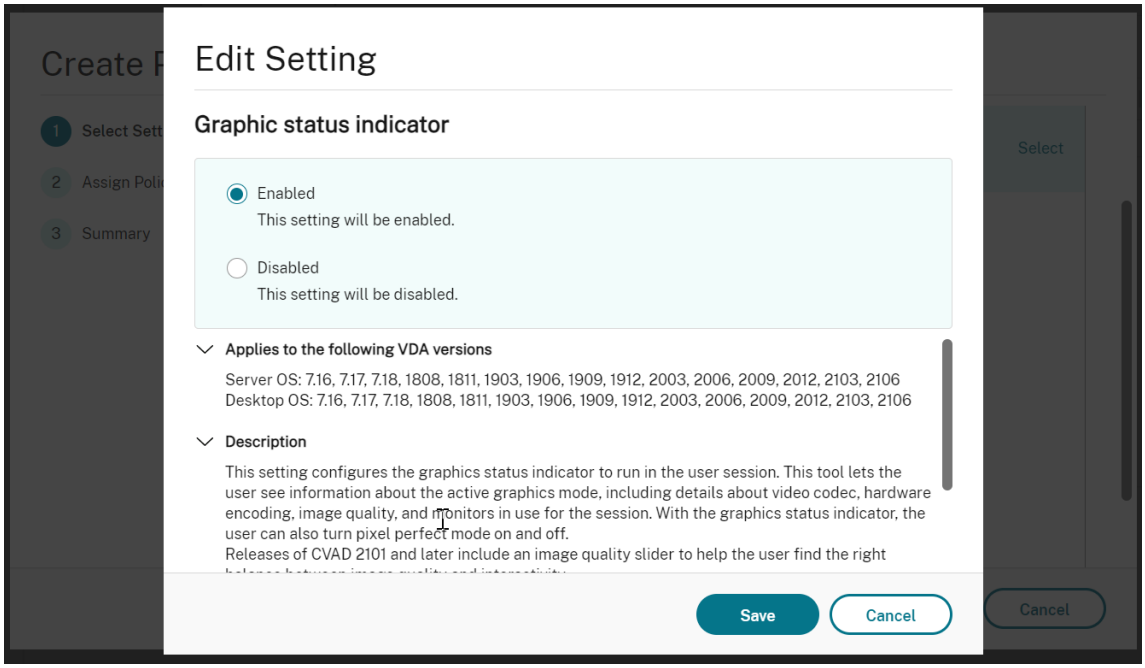
Weitere Informationen zu den Richtlinieneinstellungen für **Bildqualität** und **Videocodec zur Komprimierung verwenden** finden Sie unter Einstellungen der Richtlinie "Visuelle Anzeige" und Einstellungen der Richtlinie "Grafiken".

Schieberegler für Grafikqualität

In der in virtuellen Linux-Sitzungen ausgeführten Grafikstatusanzeige gibt es jetzt einen Schieberegler für Grafikqualität. Mit dem Schieberegler finden Sie das richtige Gleichgewicht zwischen Bildqualität und Interaktivität.

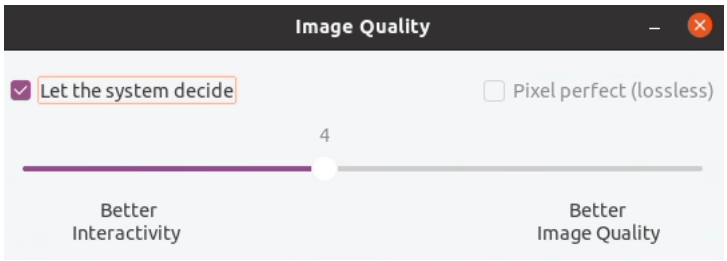
Führen Sie die folgenden Schritte aus, um den Schieberegler zu verwenden:

1. Aktivieren Sie die Richtlinie **Grafikstatusanzeige** in Citrix Studio.



2. Öffnen Sie das Terminal und führen Sie den Befehl `ctxslider` aus. Der Schieberegler wird angezeigt.

> **Hinweis:**
>
> - Wenn Sie die Richtlinie **Bildqualität** auf **Immer verlustfrei** oder **Zu verlustfrei verbessern** festgelegt haben, wird der Schieberegler nicht angezeigt.
> - Sie können den Schieberegler vom Terminal und vom Infobereich aus starten.



Die folgenden Optionen sind jetzt verfügbar:

- Um die Bildqualität zu ändern, verschieben Sie den Schieberegler. Der Schieberegler hat einen Bereich von 0 bis 9.
- Um systemdefinierte Einstellungen zu verwenden, wählen Sie **System entscheiden lassen**.
- Um in den verlustfreien Modus zu wechseln, wählen Sie **Pixelgenau**.

Anpassen der durchschnittlichen Bitraten basierend auf Bandbreitenschätzungen

Citrix verbessert die HDX 3D Pro-Hardwarecodierung durch Anpassung der durchschnittlichen Bitraten basierend auf Bandbreitenschätzungen.

Wenn die HDX 3D Pro-Hardwarecodierung verwendet wird, kann der VDA sporadisch die Bandbreite des Netzwerks schätzen und die Bitraten von codierten Frames entsprechend anpassen. Dieses neue Feature bietet einen Mechanismus, um zwischen Schärfe und Fluss auszugleichen.

Dieses Feature ist standardmäßig aktiviert. Führen Sie folgenden Befehl aus, um es zu deaktivieren:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    DisableReconfigureEncoder" -d "0x00000001" --force
<!--NeedCopy-->
```

Zusätzlich zu diesem Feature können Sie auch die folgenden Befehle ausführen, um zwischen Schärfe und Fluss anzupassen. Die Parameter **AverageBitRatePercent** und **MaxBitRatePercent** legen den Prozentsatz der Bandbreitenauslastung fest. Je höhere Werte Sie festlegen, desto schärfer sind Grafiken und weniger glatt fließen sie. Der empfohlene Bereich für diese Einstellung ist 50 bis 100.

```
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
<!--NeedCopy-->
```

Wenn mit der durchschnittlichen Bitratenanpassung der Bildschirm angehalten wird, erscheint der letzte Frame mit niedriger Qualität, weil keine neuen Frames gesendet werden. Die Schärfungsunterstützung kann dieses Problem beheben, indem neu konfiguriert und sofort der neueste Frame in höchster Qualität sofort gesendet wird.

Eine vollständige Liste der von Linux VDA Thinwire unterstützten Richtlinien finden Sie unter Liste der unterstützten Richtlinien.

Informationen zur Konfiguration der Multi-Monitor-Unterstützung für den Linux VDA finden Sie unter CTX220128.

Parallele Verarbeitung

Thinwire kann die Anzahl der Frames pro Sekunde (FPS) durch Parallelisierung bestimmter Aufgaben verbessern, was einen insgesamt etwas höheren CPU-Verbrauch verursacht. Das Feature ist in der Standardeinstellung deaktiviert. Führen Sie den folgenden Befehl auf Ihrem VDA aus, um das Feature zu aktivieren:


```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ParallelProcessing" -d "0x00000001" --force
<!--NeedCopy-->
```

Problembehandlung

Verwendeten Grafikmodus ermitteln

Führen Sie folgenden Befehl aus, um den verwendeten Grafikmodus zu ermitteln (**0** ist TW+, **1** ist Vollbildvideocodec):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
<!--NeedCopy-->
```

Das Ergebnis sieht in etwa wie folgt aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force
```

Verifizieren, dass H.264 verwendet wird

Führen Sie folgenden Befehl aus, um zu ermitteln, ob H.264 verwendet wird (**0** = nicht verwendet, **1** = verwendet):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
<!--NeedCopy-->
```

Das Ergebnis kann zum Beispiel wie folgt aussehen:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000000"--force
```

Verifizieren, dass H.265 verwendet wird

Führen Sie folgenden Befehl aus, um zu ermitteln, ob Vollbild-H.265 verwendet wird (**0** = nicht verwendet, **1** = verwendet):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
<!--NeedCopy-->
```

Das Ergebnis kann zum Beispiel wie folgt aussehen:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H265"-d "0x00000000"--force
```


Ermitteln des verwendeten YUV-Codierungsschemas

Führen Sie den folgenden Befehl aus, um zu überprüfen, welches YUV-Codierungsschema verwendet wird (**0** bedeutet YUV420. **1** bedeutet YUV422. **2** bedeutet YUV444):

> **Hinweis:**
>
> Der Wert von **YUVFormat** ist nur dann sinnvoll, wenn ein Videocodec verwendet wird.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
<!--NeedCopy-->
```

Das Ergebnis kann zum Beispiel wie folgt aussehen:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000000"--force
```

Verifizieren, dass die YUV444-Softwarekodierung verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die YUV444-Softwarekodierung verwendet wird:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep Graphics
<!--NeedCopy-->
```

Wenn YUV444 verwendet wird, ähnelt das Ergebnis:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000001"--force

create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "H264"-d "0x00000001"--force

create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000000"--force

create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "YUVFormat"-d "0x00000002"--force
```

Verifizieren, dass HDX 3D Pro aktiviert ist

Führen Sie die folgenden Befehle aus, um zu überprüfen, ob HDX 3D Pro aktiviert ist:

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep ProductEdition

sudo /opt/Citrix/VDA/bin/ctxreg dump | grep StackSessionMode

```



```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep 3DPro
<!--NeedCopy-->
```

Wenn HDX 3D Pro aktiviert ist, sieht das Ergebnis wie folgt aus:

```
create -k "HKLM\Software\Citrix\VirtualDesktopAgent\State"-t "REG_SZ"
-v "ProductEdition"-d "<PLT or ENT>"--force

create -k "HKLM\System\CurrentControlSet\Control\Citrix\WinStations\
tcp"-t "REG_DWORD"-v "StackSessionMode"-d "0x00000000"--force

create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD
"-v "3DPro"-d "0x00000000"--force
```

Um zu überprüfen, ob die erforderlichen NVIDIA-Bibliotheken für HDX 3D Pro geladen sind, führen Sie den Befehl **nvidia-smi** auf dem Linux VDA aus. Das Ergebnis sieht in etwa wie folgt aus:

```
Tue Apr 12 10:42:03 2016
+-----------------------------------------------------+
| NVIDIA-SMI 361.28     Driver Version: 361.28        |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  GRID K1             Off  | 0000:00:05.0     Off |
                     N/A |
| N/A   42C    P0    14W /  31W |    207MiB /  4095MiB |      8%
   Default |
+-------------------------------+----------------------+----------------------+


+-----------------------------------------------------------------------------+

| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|

|    0      2164  C+G   /usr/local/bin/ctxgfx
   106MiB |
|    0      2187    G   Xorg
    85MiB |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```


Verifizieren, dass die Hardwarekodierung für 3D Pro verwendet wird

Führen Sie folgenden Befehl aus (**0** = nicht verwendet, **1** = verwendet):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
<!--NeedCopy-->
```

Wenn 3D Pro verwendet wird, sieht das Ergebnis wie folgt aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\1\Graphics"-t "REG_DWORD"
-v "HardwareEncoding"-d "0x00000001"--force
```

Prüfung auf fehlerfreie Installation des NVIDIA GRID-Grafiktreibers

Um die korrekte Installation des NVIDIA GRID-Grafiktreibers zu überprüfen, führen Sie **nvidia-smi** aus. Das Ergebnis sieht in etwa wie folgt aus:

```
+-----------------------------------------------------+
| NVIDIA-SMI 352.70     Driver Version: 352.70        |
|-------------------------------+----------------------+----------------------+

| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
   Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
   Compute M. |
|===============================+======================+======================|

|   0  Tesla M60           Off  | 0000:00:05.0     Off |
                     Off |
| N/A   20C    P0    37W / 150W |     19MiB /  8191MiB |      0%
   Default |
+-------------------------------+----------------------+----------------------+


+-----------------------------------------------------------------------------+

| Processes:                                                       GPU
   Memory |
|  GPU       PID  Type  Process name
   Usage      |
|=============================================================================|

|  No running processes found
                                 |
+-----------------------------------------------------------------------------+

<!--NeedCopy-->
```

Legen Sie die richtige Konfiguration für die Karte fest:

```
etc/X11/ctx-nvidia.sh
```


HDX 3D Pro - Probleme bei der Darstellungsaktualisierung bei mehreren Monitoren

Wenn beim Verwenden mehrerer Monitore Probleme bei der Darstellungsaktualisierung auf den sekundären Monitoren auftreten, prüfen Sie, ob die NVIDIA GRID-Lizenz verfügbar ist.

Überprüfen der Xorg-Fehlerprotokolle

Die Xorg-Protokolldatei heißt **Xorg.{DISPLAY}.log** (oder ähnlich) und ist im Ordner **/var/log/**.

Bekannte Probleme und Einschränkungen

Für vGPU wird auf der lokalen Citrix Hypervisor-Konsole der Bildschirm der ICA-Desktopsitzung angezeigt

Workaround: Deaktivieren Sie die lokale VGA-Konsole der VM, indem Sie folgende Befehle ausführen:

Citrix Hypervisor 8.1 und höher:

```
[root@xenserver ~]# xe vgpu-param-set uuid=vgpu-uuid extra_args=
   disable_vnc=1
<!--NeedCopy-->
```

Citrix Hypervisor vor Version 8.1:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
<!--NeedCopy-->
```

Gnome 3-Desktoppopups bei Anmeldung langsam

Dies ist eine Einschränkung im Gnome 3-Desktopsitzungsstart.

Einige OpenGL/WebGL-Anwendungen werden nach dem Ändern der Fenstergröße der Citrix Workspace-App nicht einwandfrei gerendert

Beim Ändern der Fenstergröße für die Citrix Workspace-App wird die Bildschirmauflösung geändert. Damit ändern sich einige interne Zustände des proprietären NVIDIA-Treibers, wodurch Anwendungen möglicherweise entsprechend reagieren müssen. Das WebGL-Bibliothekselement **lightgl.js** kann beispielsweise die Fehlermeldung **Rendering to this texture is not supported (incomplete frame buffer)** auslösen.

HDX-Bildschirmfreigabe

January 8, 2024

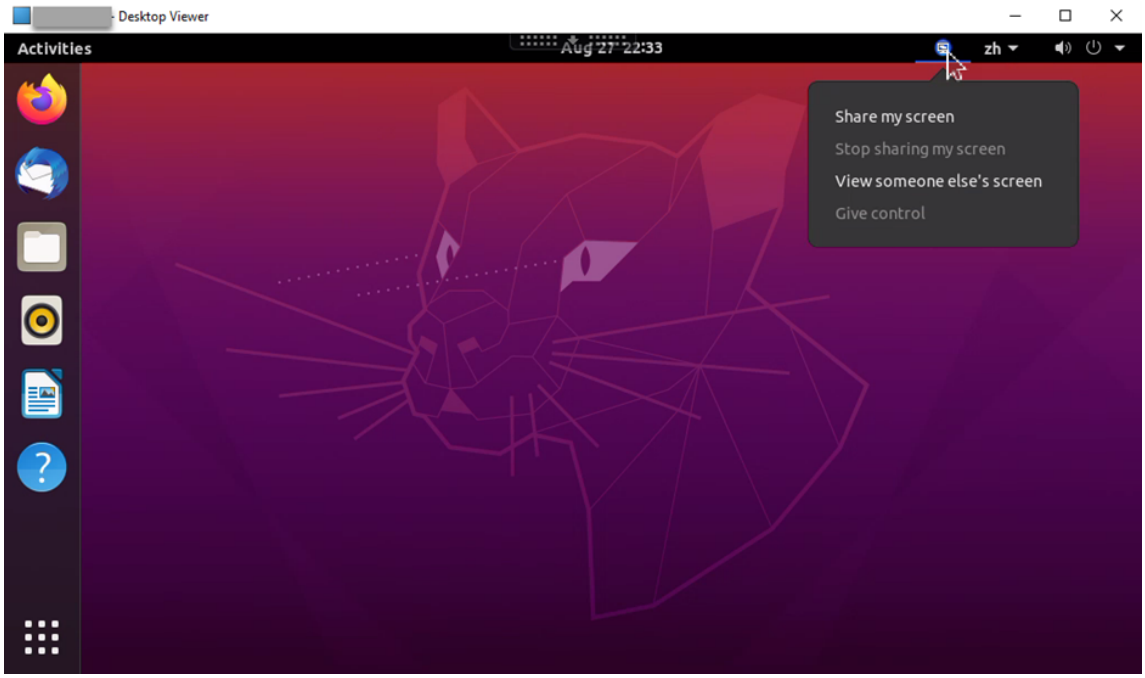
Übersicht

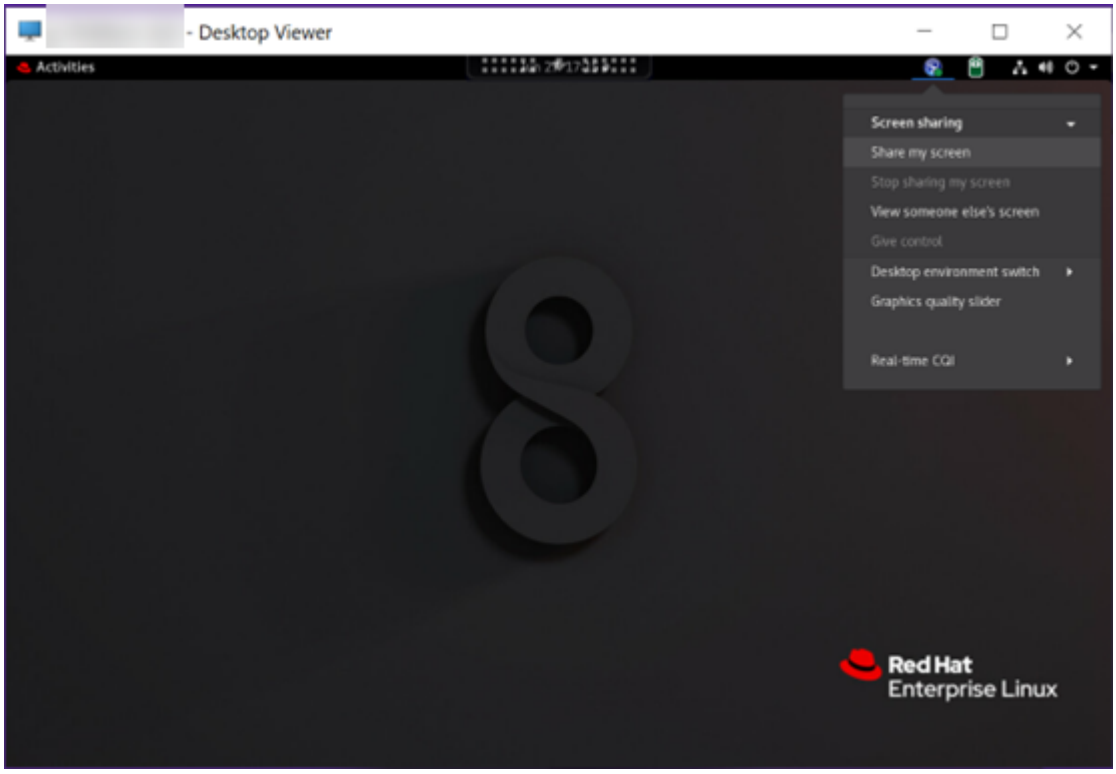
Mit dem Linux VDA können Sie den Bildschirm Ihres virtuellen Desktops für Sitzungsbenutzer auf anderen virtuellen Desktops freigeben.

Das folgende Beispiel erläutert die Schritte zur Freigabe eines Bildschirms und zur Anzeige des Bildschirms anderer Benutzer.

Freigeben des eigenen Bildschirms:

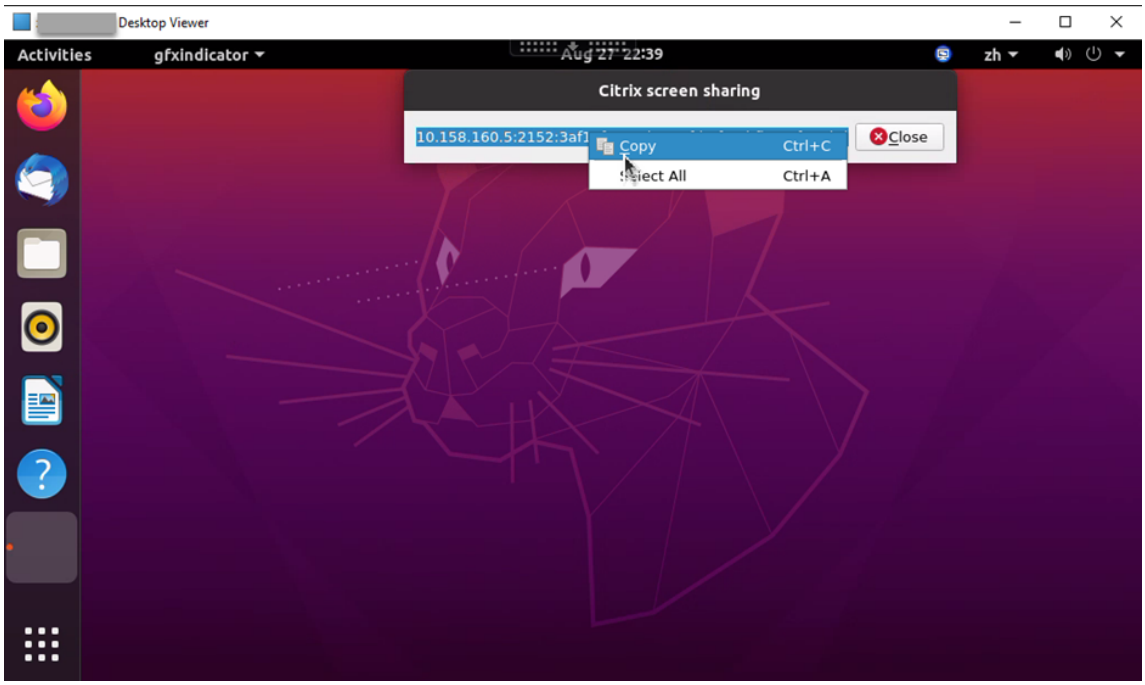
1. Klicken Sie im Benachrichtigungsfeld des virtuellen Desktops auf das folgende Symbol im Infobereich und wählen Sie **Bildschirmfreigabe > Meinen Bildschirm freigeben**.





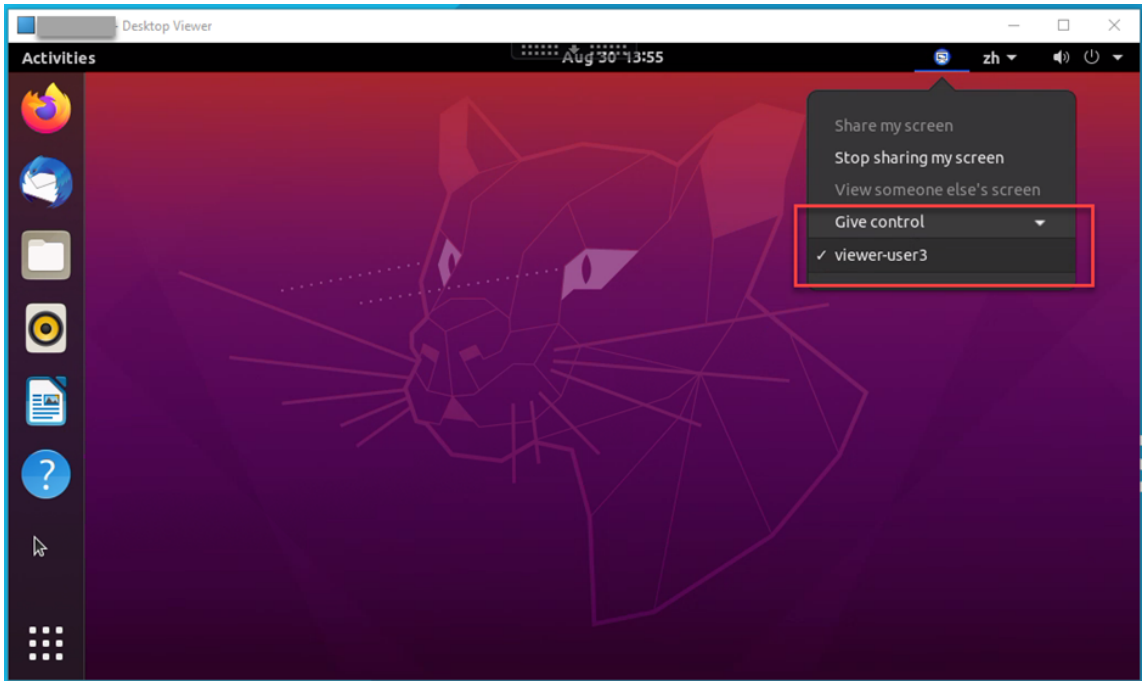
2. Klicken Sie auf **Kopieren und schließen**.

   Der aktuelle Code für die Bildschirmfreigabe bleibt bestehen, bis Sie die Bildschirmfreigabe beenden und erneut starten.

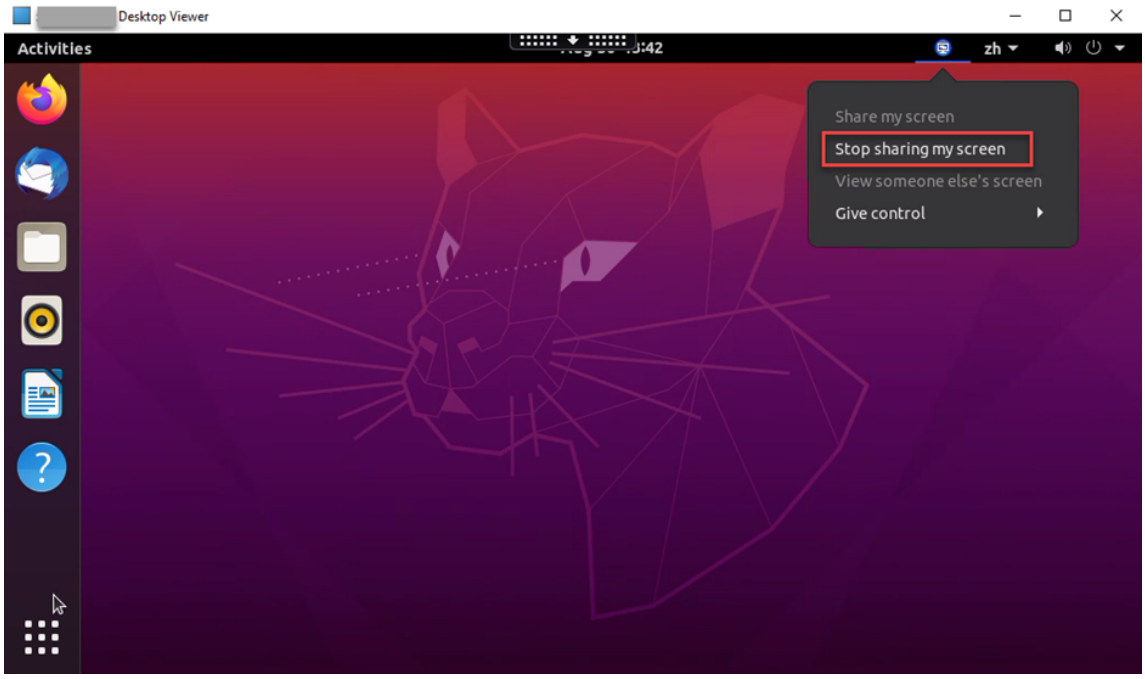


> **Tipp:**
>
> Während der Bildschirmfreigabe ist Ihr Bildschirm rot umrandet.

3. Teilen Sie den kopierten Code mit Sitzungsbenutzern auf anderen virtuellen Desktops, für die Sie Ihren Bildschirm freigeben möchten.
4. Damit ein anderer Benutzer Ihren Bildschirm steuern kann, wählen Sie **Steuerung übergeben** und dann den Namen des Benutzers. Um die Steuerungsübergabe zu beenden, löschen Sie den Namen des Benutzers.

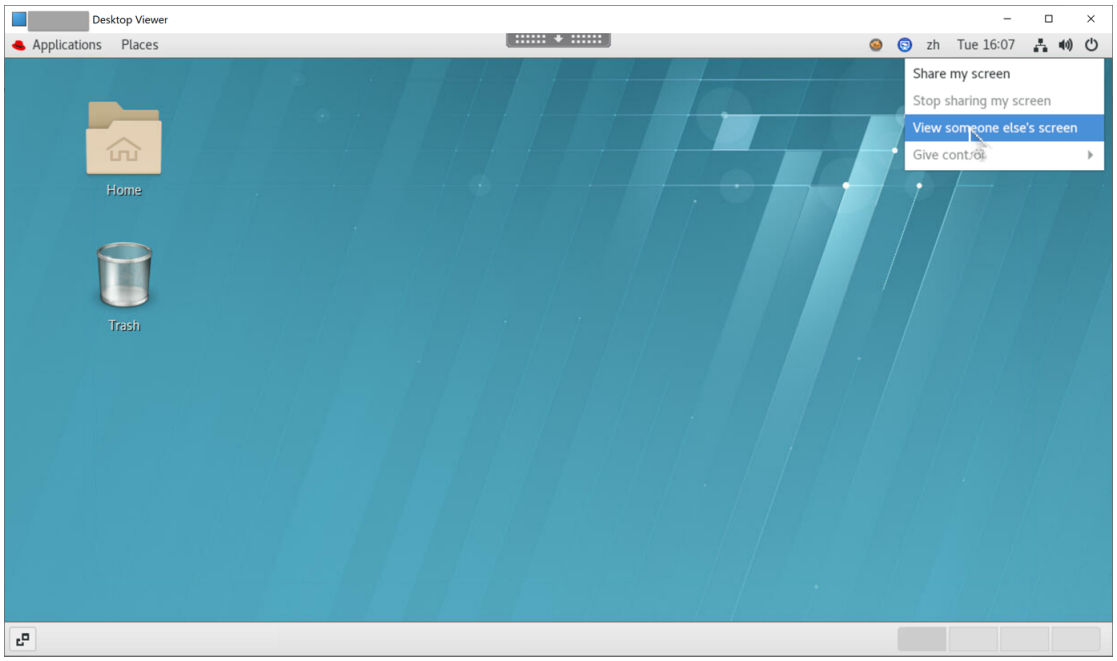


5. Um die Bildschirmfreigabe zu beenden, wählen Sie **Bildschirmfreigabe stoppen**.

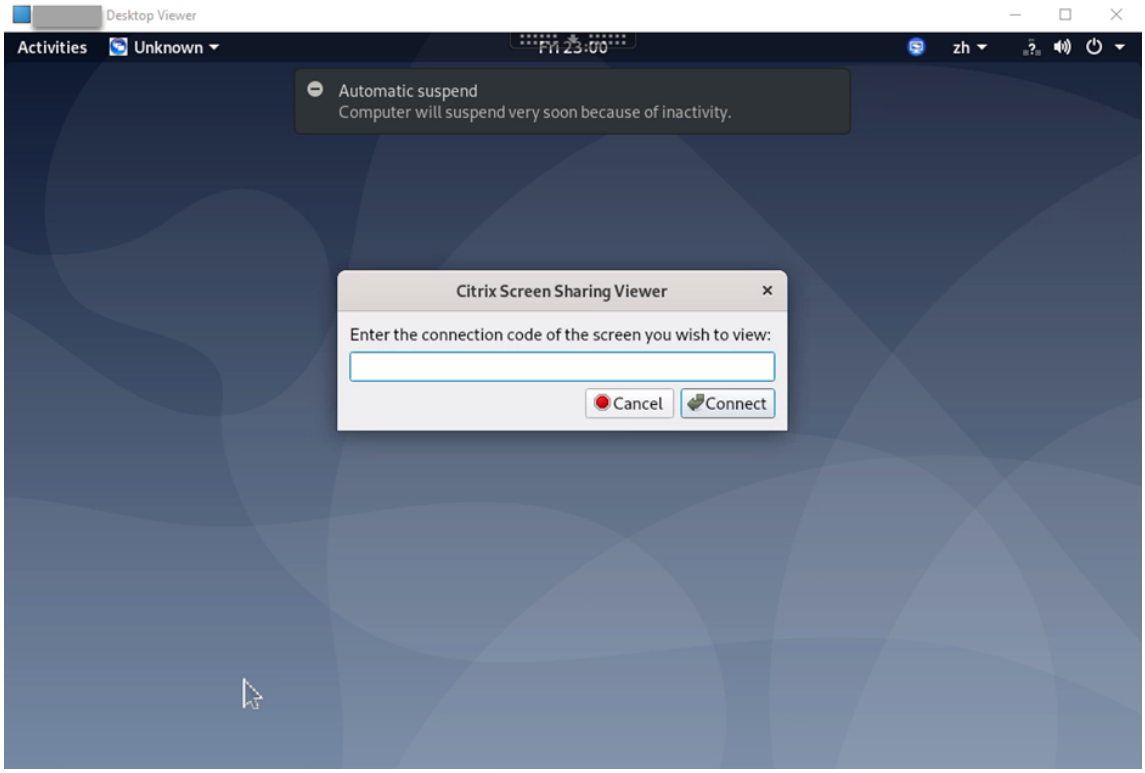


Bildschirm einer anderen Person anzeigen:

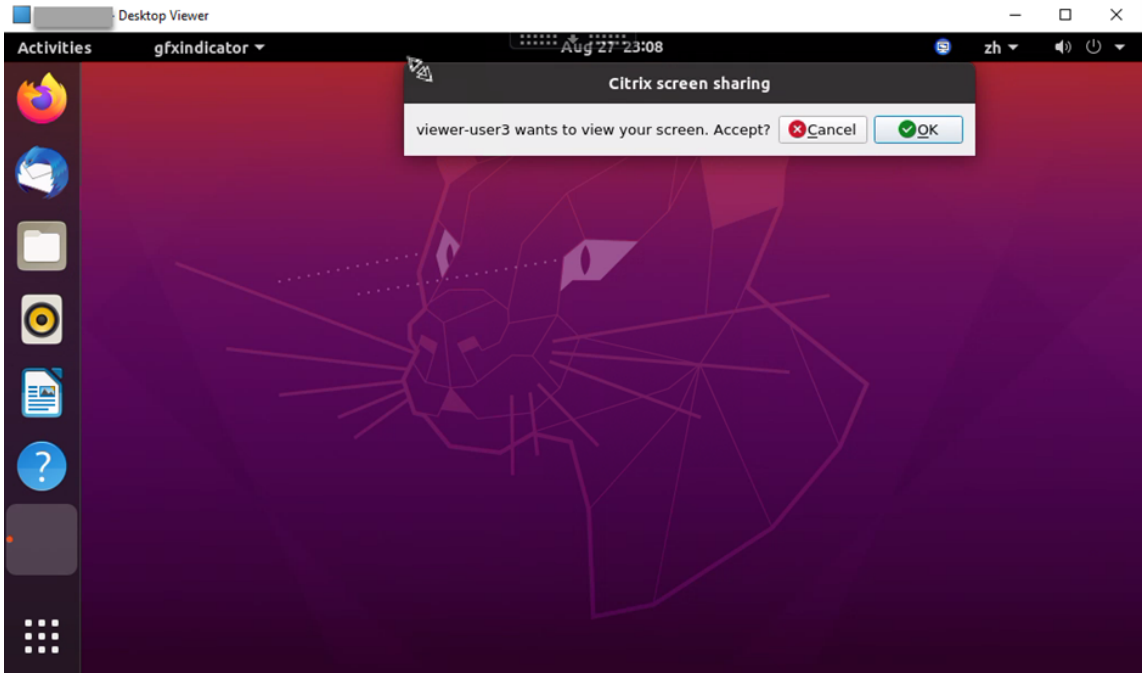
1. Klicken Sie im Infobereich Ihres virtuellen Desktops auf das Symbol für die **Bildschirmfreigabe** und wählen Sie **Bildschirm einer anderen Person anzeigen**.



2. Geben Sie den Verbindungscode des anzuzeigenden Bildschirms ein und klicken Sie auf **Verbinden**.



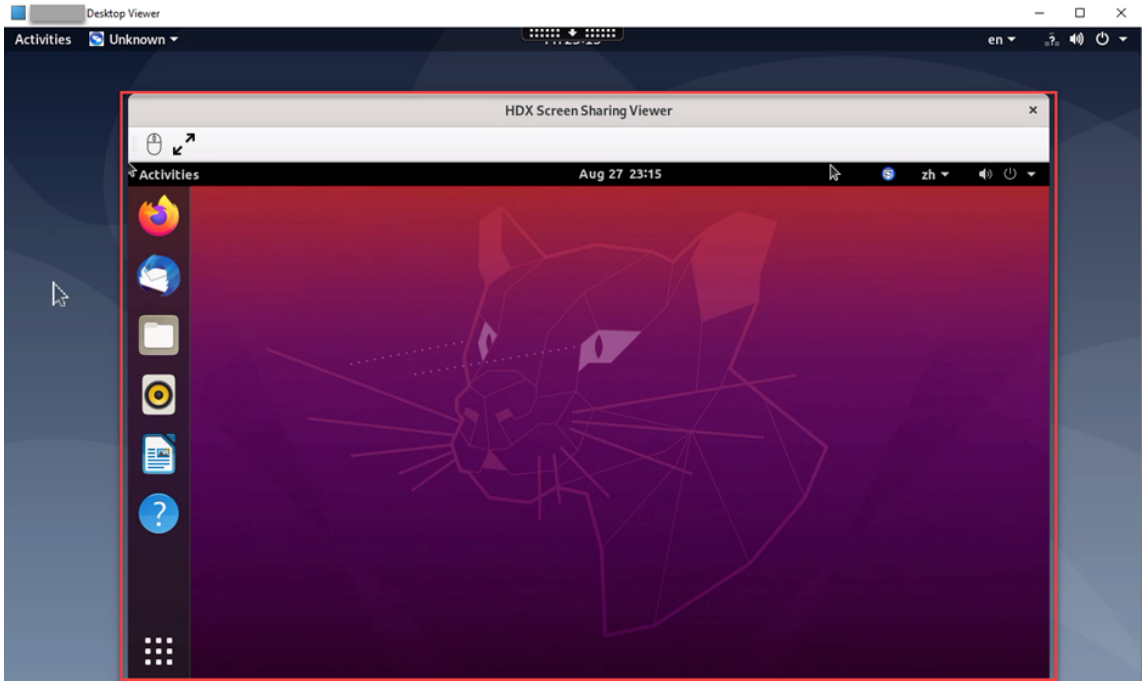
3. Warten Sie, bis der andere Benutzer Ihre Anforderung akzeptiert. Beispiel:



> **Tipp:**
>
> - Der Besitzer des freizugebenden Bildschirms erhält vom Linux-System eine Benachrichtigung zu Ihrer Anforderung.

> - Wenn der andere Benutzer Ihre Anforderung nicht innerhalb von 30 Sekunden akzeptiert, läuft sie ab und es wird eine Eingabeaufforderung angezeigt.

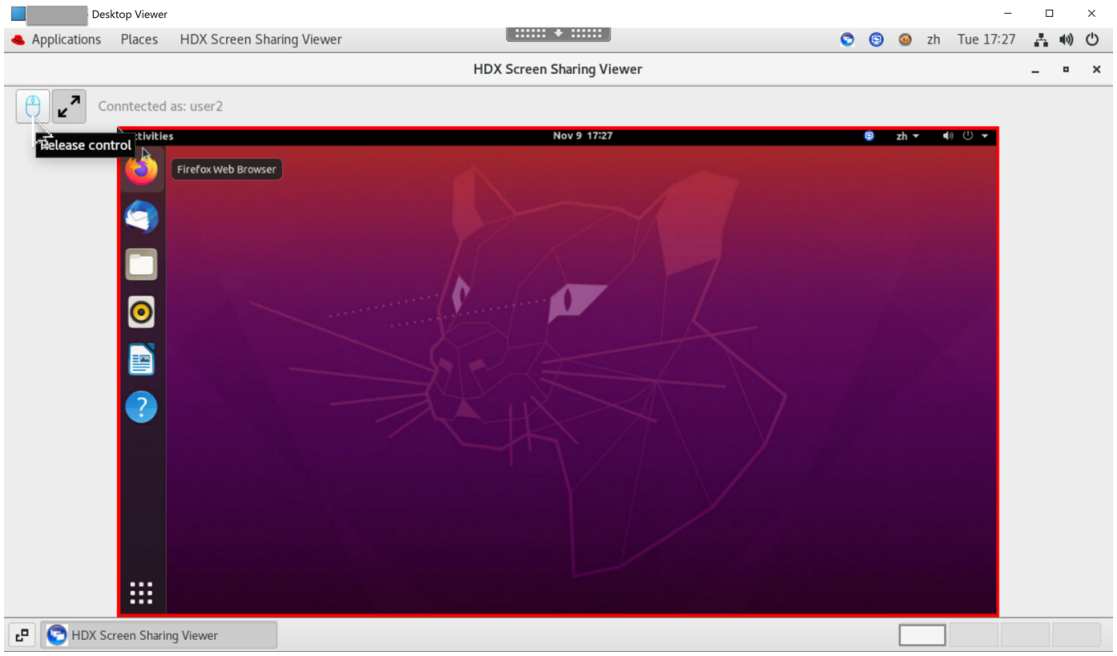
4. Wenn der Benutzer Ihre Anforderung durch Klicken auf **OK** akzeptiert, wird der freigegebene Bildschirm in Ihrem Desktop Viewer angezeigt. Sie sind als Leseberechtigter mit automatisch zugewiesenem Benutzernamen verbunden.



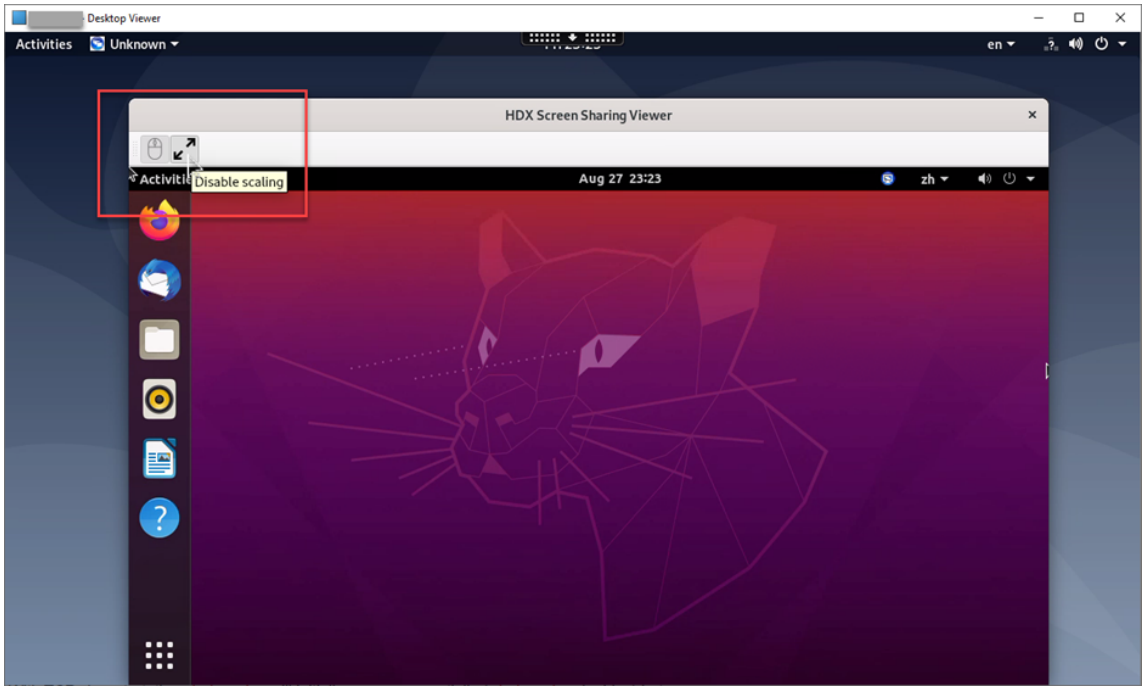
5. Um die Steuerung des freigegebenen Bildschirms anzufordern, klicken Sie links oben auf das Maussymbol.

> **Tipp:**
>
> - Wenn der Besitzer des freizugebenden Bildschirms Ihre Anforderung nicht innerhalb von 30 Sekunden akzeptiert, läuft sie ab.
> - Ein freigegebener Bildschirm kann nur von jeweils einem Leseberechtigten gesteuert werden.

Klicken Sie erneut auf das Maussymbol, um die Steuerung einer Bildschirmfreigabe abzugeben.



6. Um die Anzeigeskalierung zu deaktivieren oder auf die Fenstergröße zu skalieren, klicken Sie auf das Symbol neben dem Maussymbol.



Konfiguration

Die Bildschirmfreigabe ist standardmäßig deaktiviert. Um sie zu aktivieren, legen Sie die folgenden Einstellungen fest:

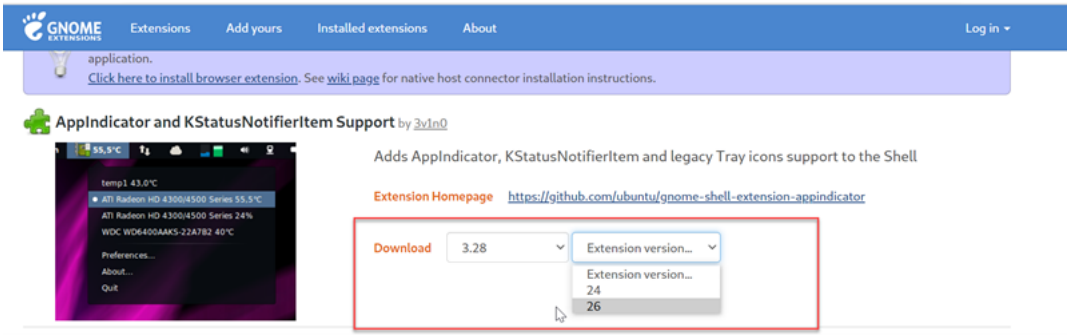
1. Aktivieren Sie die Richtlinie zur Grafikstatusanzeige in Citrix Studio.
2. Für Citrix Virtual Apps and Desktops 2112 und höher aktivieren Sie die Richtlinie **Bildschirmfreigabe** in Citrix Studio.
3. (Optional) Für Citrix Virtual Apps and Desktops 2109 und früher aktivieren Sie die Bildschirmfreigabe auf dem Linux VDA, indem Sie folgenden Befehl ausführen:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -v "
   EnableScreenSharing" -d "0x00000001"
<!--NeedCopy-->
```

4. Erlauben Sie den Zugriff auf die Ports 52525—52625 in Ihrer Firewall.
5. (Optional) Bei Verwendung von mit GNOME installiertem RHEL 8.x, Debian 11 oder SUSE 15.x installieren Sie eine kompatible Erweiterung für die GNOME-Shell, um die AppIndicator-Unterstützung zu aktivieren:

   a) Führen Sie den Befehl `gnome-shell --version` aus, um Ihre GNOME-Shellversion zu überprüfen.

   b) Laden Sie eine kompatible Erweiterung für die GNOME-Shell von https://extensions.gnome.org/extension/615/appindicator-support herunter. Wenn Ihre Shellversion beispielsweise 3.28 ist, können Sie 24 oder 26 als Erweiterungsversion auswählen.



   c) Entpacken Sie das heruntergeladene TAR-Paket. Stellen Sie sicher, dass der Wert **uuid** in der Datei **metadata.json** im Paket auf `appindicatorsupport@rgcjonas.gmail.com` gesetzt ist.

   d) Führen Sie den Befehl `mv` aus, um das Verzeichnis `appindicatorsupport@rgcjonas.gmail.com` unter `/usr/share/gnome-shell/extensions/` zu speichern.

   e) Führen Sie den Befehl `chmod a+r metadata.json` aus, um die Datei **metadata.json** für andere Benutzer lesbar zu machen.

> **Tipp:**
>
> Die Datei **metadata.json** im Verzeichnis `appindicatorsupport@rgcjonas.`

> `gmail.com` kann standardmäßig nur vom Root-Benutzer gelesen werden. Um die Bildschirmfreigabe zu unterstützen, machen Sie die Datei **metadata.json** auch für andere Benutzer lesbar.

f) Installieren Sie GNOME Tweaks.

g) Laden Sie in der Desktopumgebung Ihre GNOME-Shell neu, indem Sie nacheinander die Tasten `Alt`+`F2`, `r` und `Enter` drücken oder aber den Befehl `killall -SIGQUIT gnome-shell` ausführen.

h) Führen Sie in der Desktopumgebung GNOME Tweaks aus und aktivieren Sie **KStatusNotifierItem/AppIndicator Support** im Tweaks-Tool.

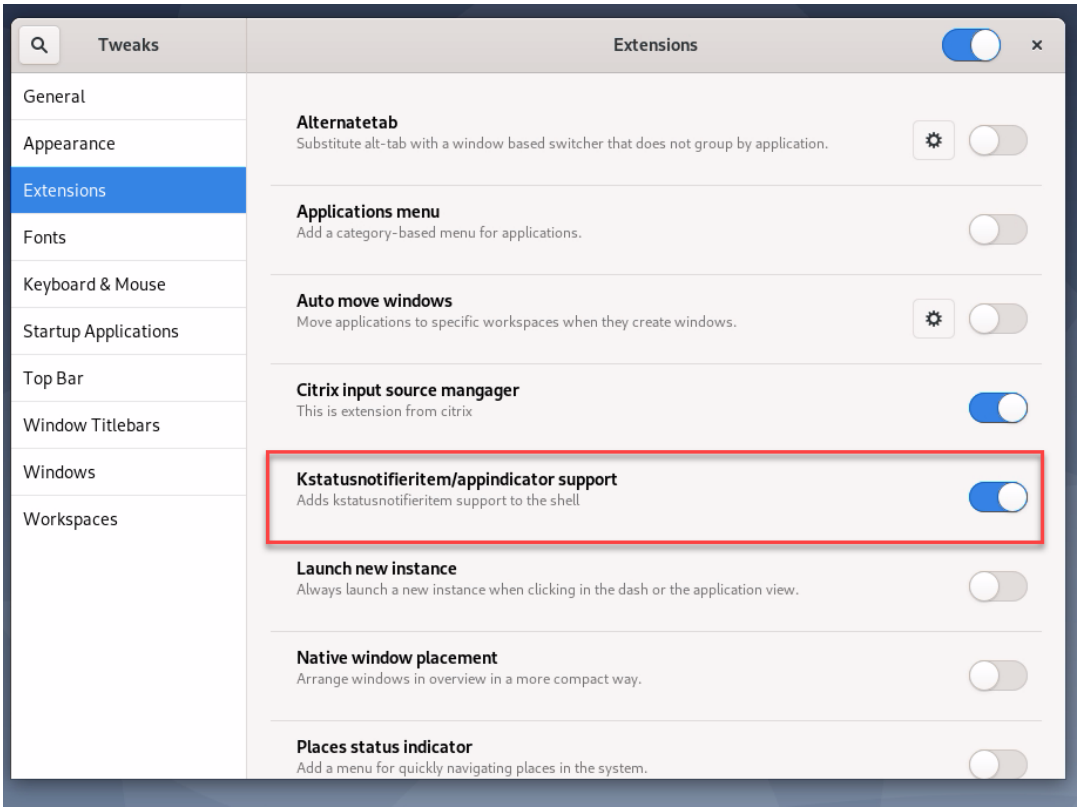
6. (Optional) Bei Verwendung von mit GNOME installiertem Debian 11.3 führen Sie die folgenden Schritte aus, um Symbole im GNOME-Benachrichtigungsfeld zu installieren und zu aktivieren:

a) Führen Sie den Befehl `sudo apt install gnome-shell-extension-appindicator` aus. Sie müssen sich möglicherweise abmelden und erneut anmelden, damit die Erweiterung von GNOME erkannt wird.

b) Suchen Sie im Bildschirm **Activities** nach Tweaks.

c) Wählen Sie im Tweaks-Tool **Extensions**.

d) Aktivieren Sie **Kstatusnotifieritem/appindicator support**.



Überlegungen

- Der H.265-Videocodec wird von der Bildschirmfreigabe nicht unterstützt.
- Die Bildschirmfreigabe ist für App-Sitzungen nicht verfügbar.
- Benutzer von Desktopsitzungen können ihre Sitzungsbildschirme standardmäßig für bis zu 10 Leseberechtigte freigeben. Die maximale Anzahl von Leseberechtigten ist über `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix \Thinwire"-v "ScreenSharingViewerMaxNum"-d <hex_value>` konfigurierbar. Wenn die maximale Anzahl erreicht ist, wird eine Meldung angezeigt, wenn Benutzer versuchen, zusätzliche Verbindungsanforderungen anzunehmen.

Multimonitorunterstützung

January 8, 2024

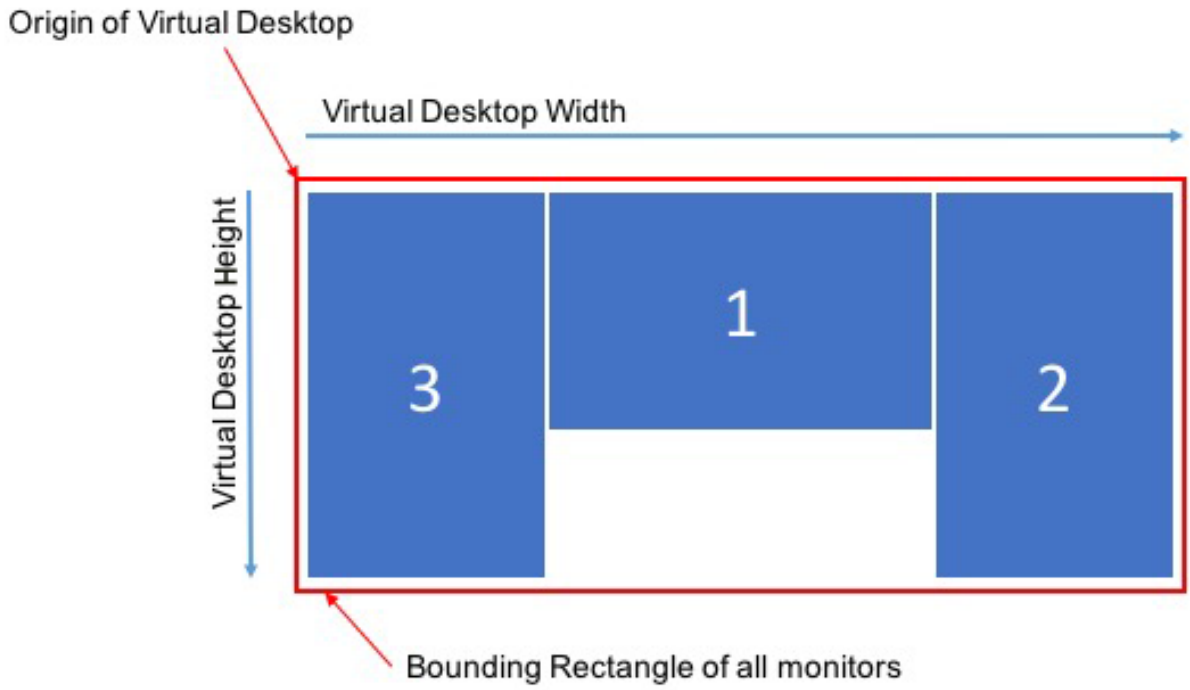
Übersicht

Der Linux VDA bietet eine vorkonfigurierte Multimonitorunterstützung mit einer Standardauflösung von 2560×1600 pro Monitor. Standard-VDAs unterstützen bis zu neun Monitore, und HDX 3D Pro-VDAs unterstützen bis zu vier Monitore.

In diesem Artikel wird beschrieben, wie Sie den Linux VDA für verschiedene Bildschirmauflösungen und Layouts konfigurieren.

Virtueller Sitzungsdesktop

Wie der Windows VDA ist auch der Linux VDA als virtueller Desktop mit mehreren Monitoren konzipiert. Er basiert auf dem Begrenzungsrechteck aller Monitore und nicht auf dem tatsächlichen Monitorlayout. Die Fläche des virtuellen Desktops kann somit theoretisch größer sein als die Fläche, die von den Monitoren des Clients abgedeckt wird.



Größe des virtuellen Sitzungsdesktops

Der Ursprung des virtuellen Sitzungsdesktops wird von der oberen linken Ecke des Begrenzungsrechtecks aller Monitore aus berechnet. Dieser Punkt befindet sich bei X = 0, Y = 0, wobei X und Y die horizontale bzw. vertikale Achse darstellen.

Die Breite des virtuellen Sitzungsdesktops ist der horizontale Abstand (in Pixeln) vom Ursprung bis zur oberen rechten Ecke des Begrenzungsrechtecks aller Monitore.

Dementsprechend ist die Höhe des virtuellen Sitzungsdesktops der vertikale Abstand (in Pixeln) vom Ursprung bis zur unteren linken Ecke des Begrenzungsrechtecks aller Monitore.

Diese Berechnung ist für Folgendes von Bedeutung:

- Verwendung unterschiedlicher Clientmonitorlayouts
- Verständnis der Speichernutzung auf dem Linux VDA

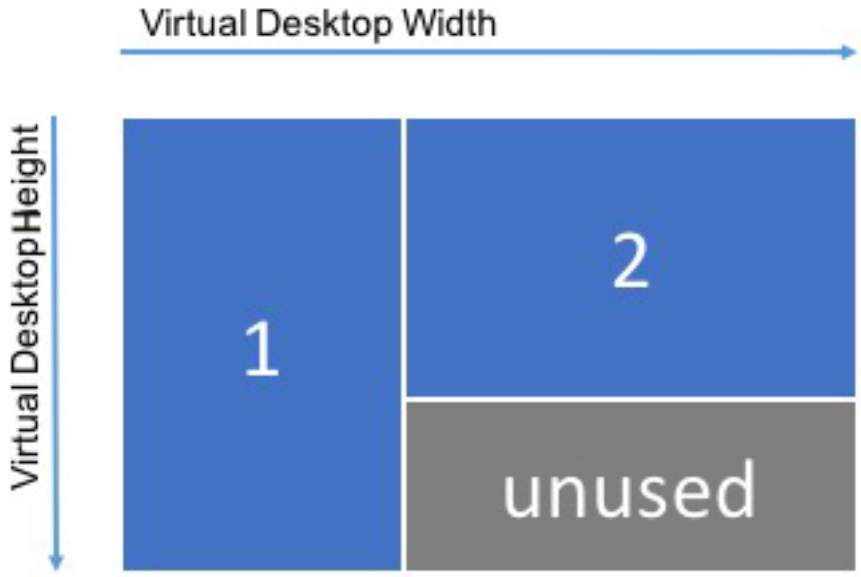
Verwendung unterschiedlicher Clientmonitorkonfigurationen

Wenn Sie die maximale virtuelle Desktopgröße für Ihre verschiedenen Clientmonitorkonfigurationen kennen, können Sie den Linux VDA so konfigurieren, dass er flexible Clientmonitorkonfigurationen zulässt.

Betrachten Sie die folgende Clientmonitorkonfiguration:

Das obige Diagramm zeigt eine vorkonfigurierte Multimonitorkonfiguration mit zwei Monitoren, jeweils mit einer Auflösung von 2560×1600.

Angenommen, Sie möchten mit der folgenden Clientmonitorkonfiguration eine Verbindung zu diesem Linux VDA herstellen:



Wenn jeder Monitor im obigen Diagramm eine Auflösung von 2560×1600 hat, sind die Parameter der vorkonfigurierten Multimonitorkonfiguration nicht ausreichend. Die maximale Höhe ist zu klein, um den virtuellen Sitzungsdesktop für dieses Monitorlayout aufzunehmen. Sie müssen 4160×2560 für den virtuellen Desktop des Linux VDA wählen, um die Clientmonitorkonfiguration im Beispiel zu nutzen.

Um die größtmögliche Flexibilität in einer Multimonitorkonfiguration zu erzielen, wählen Sie das kleinste Begrenzungsrechteck aller Monitorlayouts, die Sie unterstützen möchten. Mögliche Layouts für Konfigurationen mit zwei 2560×1600-Monitoren:

- **Monitor1** 2560×1600 und **Monitor2** 2560×1600
- **Monitor1** 1600×2560 und **Monitor2** 2560×1600
- **Monitor1** 2560×1600 und **Monitor2** 1600×2560
- **Monitor1** 1600×2560 und **Monitor2** 1600×2560

Um alle oben genannten Layouts umzusetzen, benötigen Sie einen virtuellen Sitzungsdesktop mit einer Größe von 5120 × 2560. Dies ist das kleinste Begrenzungsrechteck, das alle gewünschten Layouts aufnehmen kann.

Wenn Ihre Benutzer nur einen Monitor im typischen Querformat haben, legen Sie die maximale Größe des virtuellen Desktops auf die höchste Auflösung des Monitors fest.

In diesem Beispiel muss der virtuelle Desktop eine Größe von 2560×1600 haben. Da die Standardkonfiguration bei 5120×1600 und 2 Monitoren liegt, müssen Sie die Konfiguration ändern, um die Speichernutzung für Bereitstellungen mit nur einem Monitor zu optimieren.

> **Hinweis:**
>
> Wenn für einen Desktop in einer Multimonitorkonfiguration eine fehlerhafte Auflösung gewählt ist, passen Sie die DPI-Einstellungen (Dots Per Inch) in der Citrix Workspace-App an. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX230017.

Verständnis der Speichernutzung auf dem Linux VDA

Wenn Sie die Größe des virtuellen Desktops kennen, können Sie den von jeder HDX-Sitzung verwendeten Speicherplatz berechnen. Dies ist die Speichermenge, die einer Sitzung zu Beginn für Grafikdaten zugewiesen wird. Sie bleibt während der gesamten Sitzungsdauer gleich. Es ist zwar nicht die gesamte Speichermenge, die für die Sitzung verwendet wird, aber die einfachste Methode, die Speicherauslastung pro Sitzung zu berechnen.

Verwenden Sie die folgende Formel, um für jede HDX-Sitzung die zugewiesene Speichermenge zu berechnen:

M = X × Y × Z.

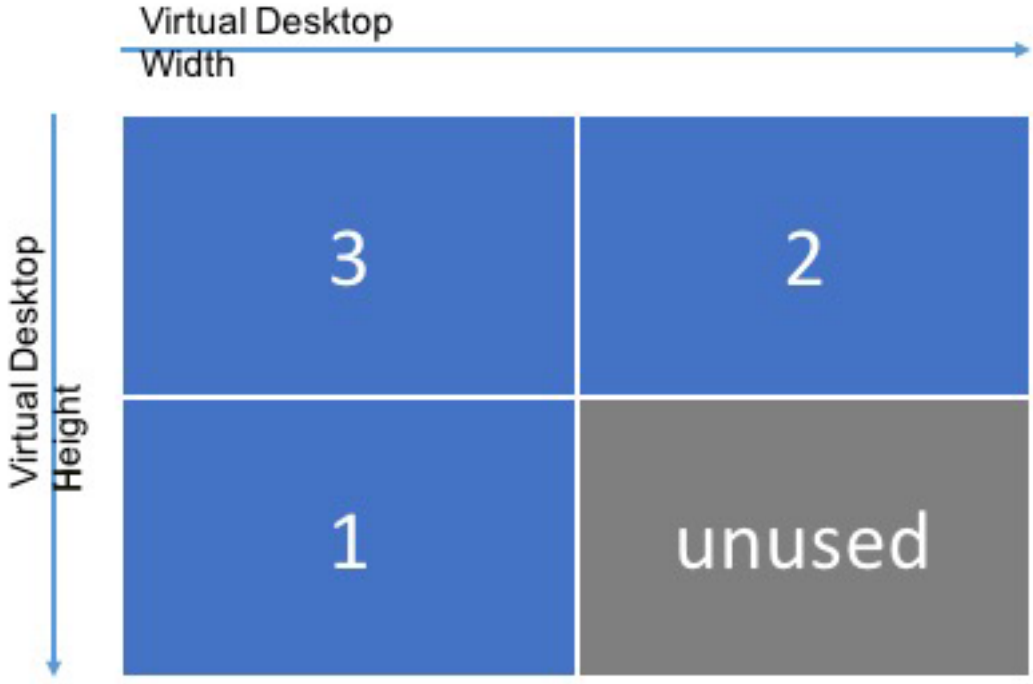
Dabei gilt:

- **M** ist die Speichermenge, die für Sitzungsgrafiken verwendet wird.
- **X** ist die Breite des virtuellen Sitzungsdesktops.
- **Y** ist die Höhe des virtuellen Sitzungsdesktops.
- **Z** ist die Farbtiefe des HDX-Sitzungsfensters. Der Wert wird in Byte und nicht in Bits angegeben. Verwenden Sie also 4 für 32-Bit-Farben.

> **HINWEIS:**
>
> Die Farbtiefe des X-Servers bleibt während der gesamten Sitzung gleich (**von der Anmeldung über abgebrochene/erneute Verbindungen bis zur Abmeldung**). Daher weist der Linux VDA den virtuellen Sitzungsdesktop stets als 32-Bit-Version zu und reduziert dann auf die für die Sitzung geforderte Farbtiefe.
>
> Für eine 1024×768-Sitzung wird zum Beispiel folgender Speicher verwendet:
>
> 1024 × 768 × 4 / 2^20 MB = 3 MB

Das Verständnis der Speichernutzung ist wichtig, um die Sitzungsdichte auf jedem Linux VDA zu erhöhen.

Betrachten Sie die folgende Clientmonitorkonfiguration:



Wenn für jeden Monitor eine Auflösung von 2560×1600 gilt, muss der virtuelle Sitzungsdesktop eine Größe von 5120×3200 haben, um die vorliegende Clientmonitorkonfiguration umzusetzen. Beachten Sie, dass der graue Bereich ungenutzt ist und 16.384.000 (d. h. 2560 x 1600 x 4) Byte an verschwendetem Speicher entspricht.

Parameter für Citrix Multimonitorkonfiguration

Sie können die Multimonitorfunktion des Linux VDA mit folgenden Konfigurationsparametern steuern:

- **`MaxScreenNum`**

  Parameter: HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/Thinwire/MaxScreenNum

  Beschreibung: Anzahl der zu unterstützenden Monitore

  Typ: DWORD

  Standard: 2

  Höchstwert: 9 für Standard-VDA, 4 für HDX 3D Pro-VDA

- **`MaxFbWidth`**

  Parameter: HKEY_LOCAL_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/-MaxFbWidth

  Beschreibung: Maximale Breite eines virtuellen Sitzungsdesktops

  Typ: DWORD

  Standard: 5.120

  Höchstwert: 16.384 (8.192 x 2)

- **`MaxFbHeight`**

  Parameter: HKEY_LOCAL_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/-MaxFbHeight

  Beschreibung: Maximale Höhe eines virtuellen Sitzungsdesktops

  Typ: DWORD

  Standard: 1.600

  Höchstwert: 16.384 (8.192 x 2)

Linux VDA-Multimonitorkonfiguration ändern

Im folgenden Abschnitt wird beschrieben, wie Sie die Multimonitorfunktion auf dem Linux VDA aktivieren, konfigurieren und deaktivieren.

Hiermit legen Sie die maximale Anzahl von Monitoren fest:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\
    Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxScreenNum" -d "
    NumMons" --force
<!--NeedCopy-->
```

Wobei **NumMons** ein Wert zwischen 1 und 9 für Standard-VDA bzw. 1 und 4 für HDX 3D Pro-VDA ist.

Hiermit legen Sie die maximale Breite eines virtuellen Sitzungsdesktops fest:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\
    Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxFbWidth" -d "
    MaxWidth" --force
<!--NeedCopy-->
```

Wobei **MaxWidth** ein Wert zwischen **1,024** und **16,384** ist.

Hiermit legen Sie die maximale Höhe eines virtuellen Sitzungsdesktops fest:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\
    Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxFbHeight" -d "
    MaxHeight" --force
<!--NeedCopy-->
```

Wobei **MaxHeight** ein Wert zwischen **1,024** und **16,384** ist.

Nicht virtualisierte GPUs

March 13, 2024

In der Linux VDA-Dokumentation beziehen sich nicht virtualisierte GPUs auf:

- GPUs, die in Remote-PC-Zugriff-Szenarios verwendet werden
- GPUs, die von einem Hypervisor übergeben werden

Dieser Artikel enthält Informationen zur Unterstützung nicht virtualisierter GPUs.

Sie HDX 3D Pro für NVIDIA-GPUs aktivieren, die das NVIDIA Capture SDK für Linux unterstützen

Aktivieren Sie bei NVIDIA-GPUs, die das NVIDIA Capture SDK für Linuxunterstützen, HDX 3D Pro einfach durch Festlegen von **CTX_XDL_HDX_3D_PRO** auf **Y** bei der Installation des Linux VDA. Eine zusätzliche Konfiguration ist nicht erforderlich. Die Hardwarebeschleunigung wird standardmäßig aktiviert, wenn Sie HDX 3D Pro aktivieren.

Kompatibel mit NVIDIA-GPUs, die das NVIDIA Capture SDK für Linux nicht unterstützen, und mit GPUs anderer Hersteller wie AMD und Intel

> **Hinweis:**
>
> In diesem Szenario wird nur Softwarecodierung unterstützt.

Schritt 1: CTX_XDL_HDX_3D_PRO bei der Installation des Linux VDA auf Y festlegen

Informationen zu Umgebungsvariablen finden Sie unter Schritt 8: Einrichten der Laufzeitumgebung für die Installation.

Schritt 2: Xdamage installieren

Sie können beispielsweise **sudo apt-get install -y libxdamage1** ausführen, um Xdamage auf Ubuntu 20.04 zu installieren. Normalerweise ist XDamage als eine Erweiterung von XServer vorhanden.

Schritt 3: Xdamage mit folgendem Befehl aktivieren

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\XDamage" -t "REG_DWORD" -v "
     XDamageEnabled" -d "0x00000001" --force
2 <!--NeedCopy-->
```

Schritt 4: Xorg-Konfigurationsdateien anpassen

Sie finden die folgenden vier Vorlagenkonfigurationsdateien unter **/etc/X11**. Ändern Sie basierend auf der Anzahl der angeschlossenen Bildschirme die Vorlagenkonfigurationsdateien mit der entsprechenden Zahl im Namen. Wenn beispielsweise nur ein Bildschirm angeschlossen ist, ändern Sie die Vorlagenkonfigurationsdatei mit der Zahl 1 im Namen, d. h. ctx-driver_name-1.conf. Wenn zwei Bildschirme angeschlossen sind, ändern Sie die Vorlagenkonfigurationsdatei mit der Zahl 2 im Namen, d. h. ctx-driver_name-2.conf.

- ctx-driver_name-1.conf
- ctx-driver_name-2.conf
- ctx-driver_name-3.conf
- ctx-driver_name-4.conf

Verwenden Sie die Datei **ctx-driver_name-1.conf** als Beispiel, um die folgenden Änderungen an den Vorlagenkonfigurationsdateien zu machen:

1. Ersetzen Sie ***driver_name*** durch den Namen Ihres Treibers.

   Wenn der Treibername beispielsweise `intel` ist, ändern Sie den Namen der Konfigurationsdatei in `ctx-intel-1.conf`.

2. Fügen Sie die Videotreiberinformationen hinzu.

   Jede Vorlagenkonfigurationsdatei enthält einen Abschnitt "Device", der auskommentiert ist. Dieser Abschnitt beschreibt die Informationen zum Videotreiber. Aktivieren Sie in diesen Abschnitt, bevor Sie die Videotreiberinformationen hinzufügen. Sie aktivieren den Abschnitt wie folgt:

   a) Sie finden Konfigurationsinformationen in der Dokumentation des GPU-Herstellers. Es wird eine native Konfigurationsdatei erstellt. Stellen Sie sicher, dass Ihre GPU in einer lokalen Umgebung mit der nativen Konfigurationsdatei funktioniert.

   b) Kopieren Sie den Abschnitt "Device"aus der nativen Konfigurationsdatei nach **ctx-driver_name-1.conf**

3. Führen Sie den folgenden Befehl aus, um den Registrierungsschlüssel festzulegen, mit dem der Linux VDA den in Schritt 1 festgelegten Konfigurationsdateinamen erkennt.

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\System\
     CurrentControlSet\Control\Citrix\XDamage" -t "REG_SZ" -v "
     DriverName" -d "intel" --force
2 <!--NeedCopy-->
```

Ausblenden des Bildschirms für VDAs mit Remote-PC-Zugriff

Der Linux VDA unterstützt das Ausblenden physischer Monitore für VDAs mit Remote-PC-Zugriff, die nicht virtualisierte GPUs verwenden.

Zu den vollständig getesteten Linux-Distributionen, die das Feature unterstützen, gehören Ubuntu 20.04 und Debian 11.3.

Dieses Feature ist standardmäßig deaktiviert. Führen Sie zum Aktivieren die folgenden beiden Schritte aus:

1. Installieren Sie das `evdi-dkms`-Paket gemäß Ihrer Linux-Distribution:


```
sudo apt install evdi-dkms
<!--NeedCopy-->
```

2. Aktivieren Sie das Auslagern der Grafikanzeige auf EVDI:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   Evdi" -d "0x00000001" --force
<!--NeedCopy-->
```

3. Deaktivieren Sie bei Verwendung einer GPU von Intel den Anzeigemanager. Andernfalls belegt der Anzeigeanager die Intel-GPU und diese ist für Citrix-Remotesitzungen nicht verfügbar.

```
sudo systemctl disable --now gdm
<!--NeedCopy-->
```

Problembehandlung

Keine oder fehlerhafte Grafikausgabe

Wenn Sie 3D-Anwendungen lokal ausführen können und alle Konfigurationen richtig sind, ist keine oder eine fehlerhafte Grafikausgabe das Ergebnis eines Fehlers. Verwenden Sie /opt/Citrix/VDA/bin/setlog und legen Sie GFX_X11 auf "verbose"fest, um die Ablaufverfolgungsinformationen für das Debuggen zu sammeln.

Sitzungswasserzeichen

January 8, 2024

Sitzungswasserzeichen helfen bei der Verhinderung und Verfolgung von Datendiebstahl. Verfolgbare Informationen erscheinen auf den Sitzungsdesktops als Abschreckung für Benutzer, die Daten per Foto oder Screenshot stehlen möchten. Sie können ein Wasserzeichen als Textebene oder als PNG-Bild mit Alphakanal angeben. Das Wasserzeichen wird über dem gesamten Sitzungsbildschirm angezeigt, ohne das Originaldokument zu ändern.

> **Wichtig:**
>
> Sitzungswasserzeichen sind kein Sicherheitsfeature. Sie verhindern einen Datendiebstahl nicht vollständig, bieten jedoch ein gewisses Maß an Abschreckung und Rückverfolgbarkeit. Bei Verwendung des Features kann keine vollständige Rückverfolgbarkeit von Informationen garantiert

> werden. Es wird jedoch empfohlen, dieses Feature nach Bedarf mit anderen Sicherheitslösungen zu kombinieren.

Sitzungswasserzeichen enthalten Informationen zur Rückverfolgung von Datendiebstahl. Die wichtigste Angabe ist die Identität des angemeldeten Benutzers, in dessen Sitzung das Bildschirmbild erstellt wurde. Zur besseren Rückverfolgung von Datenlecks sollten Sie weitere Informationen wie die IP-Adresse des Servers oder des Clients und die Verbindungszeit einschließen.

Um die Benutzererfahrung anzupassen, verwenden Sie die folgenden Einstellungen der Richtlinie "Sitzungswasserzeichen", um die Platzierung und Erscheinung von Wasserzeichen auf dem Bildschirm zu konfigurieren.

Sitzungswasserzeichen - Richtlinieneinstellungen

Sitzungswasserzeichen aktivieren

Wenn Sie diese Einstellung aktivieren, werden Sitzungen mit einem undurchsichtigen Wasserzeichen angezeigt, das sitzungsspezifische Informationen enthält. Die anderen Wasserzeicheneinstellungen hängen davon ab, dass dieses aktiviert ist.

Standardmäßig ist das Sitzungswasserzeichen deaktiviert.

Client-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die aktuelle Client-IP-Adresse als Wasserzeichen angezeigt.

Die Option **Client-IP-Adresse einschließen** ist standardmäßig deaktiviert.

Verbindungszeit einschließen

Wenn Sie diese Einstellung aktivieren, wird im Sitzungswasserzeichen eine Verbindungszeit angezeigt. Das Format ist JJJJ/MM/TT hh:mm. Die angezeigte Zeit basiert auf der Systemuhr und der Zeitzone.

Die Option **Verbindungszeit einschließen** ist standardmäßig deaktiviert.

Anmeldename einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der aktuelle Anmeldename als Wasserzeichen angezeigt. Das Anzeigeformat ist BENUTZERNAME@DOMÄNENNAME. Es wird empfohlen, Benutzernamen auf maximal 20 Zeichen zu beschränken. Wenn ein Benutzername mehr als 20 Zeichen

hat, wird dieser evtl. kleiner oder abgeschnitten angezeigt, was die Wirksamkeit des Wasserzeichens verringert.

Die Option **Anmeldename einschließen** ist standardmäßig aktiviert.

VDA-Hostname einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung der VDA-Hostname der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Die Option **VDA-Hostname einschließen** ist standardmäßig aktiviert.

VDA-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, wird in der Sitzung die VDA-IP-Adresse der aktuellen ICA-Sitzung als Wasserzeichen angezeigt.

Die Option **VDA-IP-Adresse einschließen** ist standardmäßig deaktiviert.

Sitzungswasserzeichenstil

Diese Einstellung steuert, ob eine einzelne oder mehrere Wasserzeichenbeschriftungen angezeigt werden sollen. Wählen Sie in dem Dropdownmenü **Wert** die Option **Einzeln** oder **Mehrere**.
Informationen zu weiteren Stiloptionen finden Sie im Abschnitt **Benutzerdefinierter Wasserzeichentext** in diesem Artikel.

Bei Auswahl von **Mehrere** werden fünf Wasserzeichenbeschriftungen in der Sitzung angezeigt: eine in der Mitte und vier in den Ecken.

Bei Auswahl von **Einzeln** wird nur eine Wasserzeichenbeschriftung in der Mitte angezeigt.

Standardmäßig ist für **Sitzungswasserzeichenstil** die Option **Mehrere** ausgewählt.

Wasserzeichentransparenz

Sie können eine Wasserzeichendeckkraft von 0–100 angeben. Je größer der Wert, desto deckender ist das Wasserzeichen.

Der Standardwert ist 17.

Benutzerdefinierter Wasserzeichentext

Der Wert ist standardmäßig leer. Sie können eine nicht leere Zeichenfolge eingeben, eine Syntax festlegen, um eine Zeichenfolge zu bilden, oder die Kombination zur Anzeige im Sitzungswasserzeichen verwenden. Nicht leere Zeichenfolgen unterstützen bis zu 25 Unicode-Zeichen pro Zeile. Längere Zeichenfolgen werden auf 25 Zeichen gekürzt.

Sie können die Richtlinie beispielsweise auf den folgenden Wert festlegen:

```
<date> <time><newline><username><style=single><fontsize=40><font=
Ubuntu><position=center><rotation=0><newline><serverip><newline><
clientip><newline>Citrix Linux VDA<newline>Version 2207
```

Eine Beschreibung aller Syntaxoptionen finden Sie in der folgenden Tabelle:

Syntaxoption	Beschreibung	Gültige Einstellung (Groß-/Kleinschreibung beachten)	Standardwert	Bemerkungen
<style>	Layoutstil für Wasserzeichen	xstyle, single, tile, horizontal	xstyle	-
<position>	Wasserzeichenposition	center, topleft, topright, bottomleft, bottomright	center	Nur gültig, wenn der Layoutstil auf **Einzeln** festgelegt ist.
<rotation>	Drehung des Wasserzeichens um einen bestimmten Winkel	-180–180	0	-
<transparency>	Wasserzeichendeckkraft	0–100	17	-
<font>	-	Eine vom System unterstützte Schriftart	Sans	-
<fontsize>	-	20–50	0 (automatisch berechnet)	-

Syntaxoption	Beschreibung	Gültige Einstellung (Groß-/Kleinschreibung beachten)	Standardwert	Bemerkungen
<fontzoom>	Prozentsatz der von Ihnen über <fontsize> und <image> eingestellten Schrift- und Bildgrößen	0 –	100	-
<image>	PNG-Wasserzeichen	Pfad zu einem PNG-Bild auf dem VDA	–	Diese Syntax konfiguriert ein PNG-Wasserzeichen. Nur PNG mit Alphakanal wird unterstützt. Bei Verwendung eines PNG-Wasserzeichens können nur die Syntaxoptionen <style>, <position>, <rotation>, <transparency> und <fontzoom> wirksam sein.
<date>	Platzhalter für das Datum der Sitzungsverbindung (JJJJ/MM/TT)	–	–	-
<time>	Platzhalter für die Uhrzeit der Sitzungsverbindung (HH:MM)	–	–	-

Syntaxoption	Beschreibung	Gültige Einstellung (Groß-/Kleinschreibung beachten)	Standardwert	Bemerkungen
<domain>	Platzhalter für die Domäne des Benutzerkontos	–	–	-
<username>	Platzhalter für den aktuellen Anmeldenamen (ohne die Domäne des Benutzerkontos)	–	–	-
<hostname>	Platzhalter für den Hostnamen des VDAs	–	–	-
<clientip>	Platzhalter für die Client-IP-Adresse	–	–	-
<serverip>	Platzhalter für die VDA-IP-Adresse	–	–	-

> **Hinweis:**
>
> Wenn **Benutzerdefinierter Wasserzeichentext** mit einer gültigen Syntaxeinstellung festgelegt ist, werden alle anderen Richtlinien für Sitzungswasserzeichen außer **Sitzungswasserzeichen aktivieren** ignoriert.
>
> Wenn Sie eine Syntaxoption nicht festlegen oder auf einen nicht unterstützten Wert festlegen, wird ihr Standardwert verwendet.

Einschränkungen

- Sitzungswasserzeichen werden in folgenden Fällen unterstützt:
  - Wenn für **Videocodec zur Komprimierung verwenden** die Einstellung **Für den gesamten Bildschirm** verwendet wird.
  - Wenn für **Videocodec zur Komprimierung verwenden** die Einstellung **Verwenden, wenn bevorzugt** verwendet wird und Optimierung für 3D-Grafikworkload aktiviert ist.
- In Sitzungen mit aktiver Browserinhaltsumleitung werden Sitzungswasserzeichen nicht unterstützt. Wenn Sie Sitzungswasserzeichen verwenden möchten, deaktivieren Sie bitte die

Browserinhaltsumleitung.

- Sitzungswasserzeichen werden nicht unterstützt und nicht angezeigt, wenn eine Sitzung im Vollbildmodus mit Hardwarebeschleunigung (H.264- oder H.265-Codierung) mit Legacy-NVIDIA-Treibern ausgeführt wird. (In diesem Fall ist NvCaptureType in der Registrierung auf 2 festgelegt).
- Wasserzeichen sind für die Sitzungsspiegelung nicht sichtbar.
- Wenn Sie die Taste Druck/S-Abf drücken, um einen Screenshot zu erstellen, enthält der Screenshot VDA-seitig kein Wasserzeichen. Es wird empfohlen, Maßnahmen zu ergreifen, damit Bildschirmaufnahmen nicht kopiert werden.

Beschleunigung durch GPU-Freigabe auf einem Linux VDA mit mehreren Sitzungen

January 8, 2024

HDX 3D PRO unterstützt nur die Linux-VDAs, die für VDI-Desktops konfiguriert sind (Einzelsitzungsmodus). Für einen Linux VDA mit mehreren Sitzungen können Sie die Beschleunigung durch GPU-Freigabe aktivieren, um OpenGL 3D-Anwendungen zu beschleunigen.

> **Hinweis:**
>
> Die Beschleunigung durch GPU-Freigabe wird für Wayland-Anzeigeserver nicht unterstützt.

Konfiguration

Führen Sie die folgenden Konfigurationsschritte aus, um OpenGL 3D-Anwendungen durch Aktivieren der GPU-Freigabe auf einem Linux VDA mit mehreren Sitzungen zu beschleunigen:

Schritt 1: VirtualGL installieren

Laden Sie **VirtualGL** von https://sourceforge.net/projects/virtualgl/files herunter und installieren Sie es. Laden Sie **.deb-Pakete** für Debian-basierte Linux-Distributionen und **.rpm-Pakete** für RHEL-basierte Linux-Distributionen herunter.

Schritt 2: VirtualGL konfigurieren

1. Beenden Sie den Linux-Anzeigemanager, zum Beispiel LightDM oder GNOME Display Manager (GDM).

2. Führen Sie das VirtualGL-Konfigurationsskript aus:

```
#/opt/VirtualGL/bin/vglserver_config
<!--NeedCopy-->
```

Wir empfehlen Ihnen, während der Skriptausführung die folgenden Auswahlen zu treffen:

- Wählen Sie "1"für "Configure server for use with VirtualGL (GLX + EGL back ends)".
- Wählen Sie "n"für "Restrict 3D X server access to **vglusers** group".
- Wählen Sie "n"für "Restrict framebuffer devices access to **vglusers** group".
- Wählen Sie "n"für "Disable XTEST extension".

3. Beenden Sie das Konfigurationsskript und starten Sie den Linux-Anzeigemanager neu.

Schritt 3: OpenGL 3D-Anwendungen mit GPU-Beschleunigung ausführen

Es gibt zwei Verfahren, um OpenGL 3D-Anwendungen mit GPU-Beschleunigung in einer Linux VDA-Sitzung auszuführen:

- **Verfahren 1:** Beschleunigung durch GPU-Freigabe für alle OpenGL 3D-Anwendungen aktivieren

  Öffnen Sie ein Bash-Terminal auf dem Linux VDA, führen Sie folgenden Befehl aus und starten Sie das Bash-Terminal neu. Dieser Ansatz ermöglicht eine Beschleunigung durch GPU-Freigabe für alle OpenGL 3D-Anwendungen, die vom Bash-Terminal aus gestartet werden.

```
#/opt/Citrix/VDA/sbin/ctxgpushare.sh enable
<!--NeedCopy-->
```

- **Verfahren 2:** Aktivieren Sie die Beschleunigung durch GPU-Freigabe für eine bestimmte OpenGL 3D-Anwendung:

  Öffnen Sie ein Terminal auf dem Linux VDA und führen Sie den folgenden Befehl aus, wobei Sie den Namen der Anwendung angeben:

```
#vglrun <AppName>
<!--NeedCopy-->
```

Einschränkungen

- Die Beschleunigung durch GPU-Freigabe basiert auf dem engen Zusammenspiel von Anzeigemanager und Linux VDA. Zum Erzielen der erwarteten Funktionalität und Leistung wird empfohlen, LightDM als Anzeigemanager für die Beschleunigung durch GPU-Freigabe zu verwenden.
- Die WebGL-Hardwarebeschleunigung wird in Firefox nur unter Ubuntu und Debian unterstützt.

Skalierbarkeit

Die maximal unterstützte Anzahl gleichzeitiger Sitzungen, die eine GPU gemeinsam nutzen, hängt von der CPU und dem Systemspeicher ab. Sie hängt außerdem in hohem Maß vom maximalen Videospeicher der GPU ab.

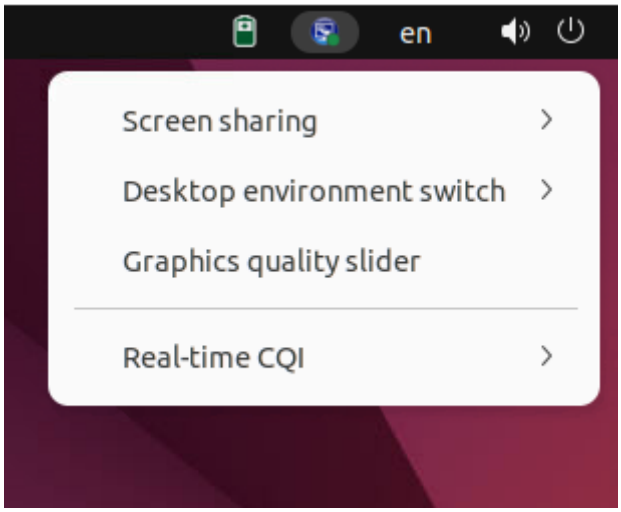
Beispiel:

Wenn…	Dann…
die NVIDIA **M10-2B** vGPU über 2.048 MB Videospeicher verfügt, und eine OpenGL-Anwendung wie VariCAD Viewer in jeder Sitzung 100 MB Videospeicher für den Workload verwendet,	darf die maximal unterstützte Anzahl gleichzeitiger Sitzungen theoretisch nicht 20 überschreiten.

Infobereich

January 8, 2024

Sitzungsbenutzer können im Infobereich auf das folgende Symbol klicken, um auf die Menüelemente für folgende Aktionen zuzugreifen:



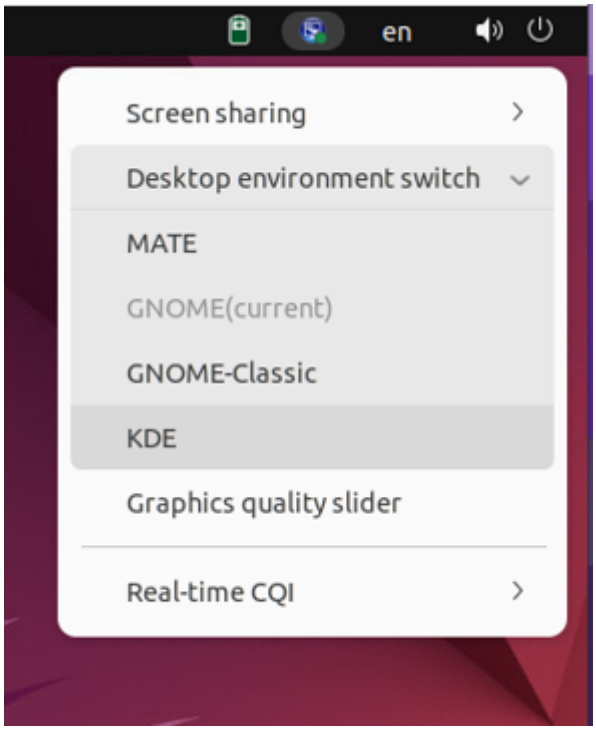
Jedes Menüelement entspricht einem Feature mit Umschaltfläche. Wenn das Feature zu einem Menüelement deaktiviert ist, ist das Menüelement ausgeblendet und wird nicht angezeigt.

- **Bildschirmfreigabe**

  Weitere Informationen zu diesem Feature finden Sie unter HDX-Bildschirmfreigabe.

- **Wechsel der Desktopumgebung**

  Dieses Menüelement ist eine GUI für **ctxdesktopswitch.sh**. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen nach Sitzungsbenutzern



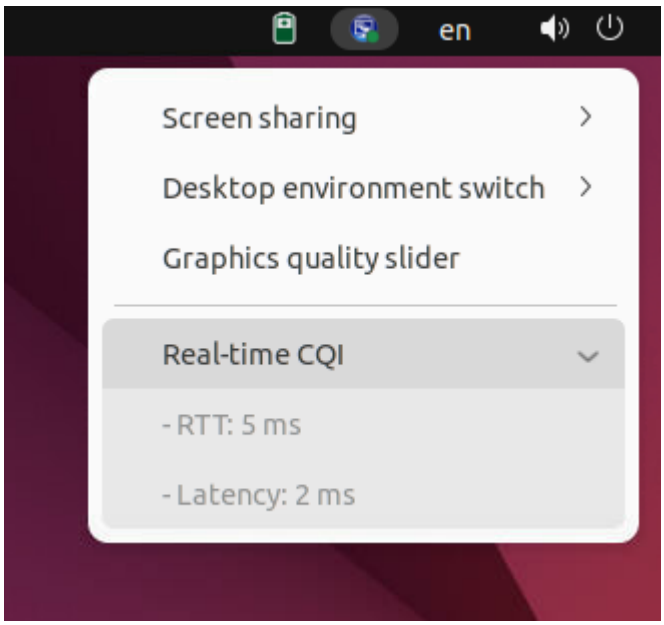
  Das Anpassen der Desktopumgebung für Sitzungsbenutzer ist standardmäßig aktiviert. Führen Sie folgenden Befehl aus, um es zu deaktivieren:

```
1  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
       CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
       EnableDesktopSwitch" -d "0x00000000" --force
2  <!--NeedCopy-->
```

- **Schieberegler für Grafikqualität**

  Weitere Informationen finden Sie im Abschnitt zum Schieberegler für die Grafikqualität im Artikel zur Grafikkonfiguration.

- **CQI in Echtzeit**



Derzeit werden Daten für Roundtripzeit (RTT) und Latenz angezeigt. Weitere Informationen finden Sie unter Hilfsprogramm zur Abfrage von Sitzungsdaten.

Die Symbolanzeige im Infobereich ist je nach Status der Verbindungsqualitätsanzeige (CQI) unterschiedlich:

Schwellenwerte steuern, wann sich die Symbolanzeige ändert. Ihre Standardeinstellung ist wie folgt:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   HighLatencyThreshold" -d "0x000000dc" --force
<!--NeedCopy-->
```

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   HighRttThreshold" -d "0x00000104" --force
<!--NeedCopy-->
```

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   LowLatencyThreshold" -d "0x00000078" --force
<!--NeedCopy-->
```

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
   CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
   LowRttThreshold" -d "0x00000096" --force
```



```
<!--NeedCopy-->
```

Bei einem RTT-Istwert kleiner oder gleich **LowRttThreshold** und einem Latenz-Istwert kleiner oder gleich **LowLatencyThreshold** ist das Symbol grün markiert. Bei einem RTT-Istwert größer als **HighRttThreshold** oder einem Latenz-Istwert größer als **HighLatencyThreshold** ist das Symbol rot markiert. Unter anderen Umständen ist das Symbol gelb markiert. Wenn "CQI in Echtzeit"deaktiviert ist, besitzt das Symbol keine Farbmarkierung.

Die Funktion "CQI in Echtzeit"ist standardmäßig aktiviert und wird angezeigt. Führen Sie den folgenden Befehl aus, um die Funktion zu deaktivieren und auszublenden, sodass das Symbol im Infobereich nicht farblich markiert ist:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    EnableCqiShow" -d "0x00000000" --force
<!--NeedCopy-->
```

Progressive Anzeige für Thinwire

January 8, 2024

Die Sitzungsinteraktivität kann sich bei Verbindungen mit niedriger Bandbreite oder hoher Latenz verschlechtern. Das Scrollen auf einer Webseite kann dann beispielsweise langsam oder abgehackt sein oder nicht funktionieren. Tastatur- und Mausoperationen können hinter Grafikaktualisierungen zurückbleiben.

Bis Version 7.17 konnten Sie den Bandbreitenverbrauch über Richtlinieneinstellungen verringern, indem Sie für Sitzungen eine **niedrige** Bildqualität oder geringere Farbtiefe (16- oder 8-Bit-Grafik) festlegten. Sie mussten jedoch wissen, dass ein Benutzer eine schwache Verbindung nutzte. HDX Thinwire hat die Qualität statischer Bilder nicht je nach Netzwerkbedingungen dynamisch angepasst.

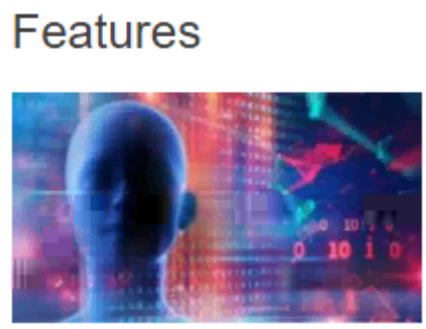
Ab Version 7.18 wechselt HDX Thinwire standardmäßig in einen progressiven Aktualisierungsmodus, wenn eine der folgenden Situationen vorliegt:

- Die verfügbare Bandbreite fällt unter 2 MBit/s.
- Die Netzwerklatenz überschreitet 200 ms.

In diesem Modus gilt:

In der folgenden Beispielgrafik mit aktivierter progressiver Aktualisierung sieht man blaue Artefakte an den Buchstaben **F** und **e** und das Bild ist stark komprimiert. Durch dieses Verfahren wird der Bandbreitenverbrauch erheblich reduziert, sodass Bilder und Text schneller empfangen werden und sich die Interaktivität der Sitzung verbessert.

Sobald Sie die Interaktion mit der Sitzung beenden, werden die unscharf angezeigten Bilder und Textsegmente kontinuierlich optimiert, bis sie verlustfrei sind. In der folgenden Beispielgrafik zeigen die Buchstaben keine blauen Artefakte mehr und das Bild erscheint in Originalqualität.



Für Bilder wird beim Scharfzeichnen eine zufällige blockartige Methode verwendet. Für Text werden einzelne Buchstaben oder Wortteile geschärft. Das Scharfzeichnen erfolgt über mehrere Frames hinweg. Dies vermeidet Bildverzögerungen, die durch das Scharfzeichnen eines einzelnen großen Frames auftreten würden.

Bewegliche Bilder (Video) werden weiterhin per adaptive Anzeige oder selektives H.264 verarbeitet.

Verwendung des progressiven Modus

Standardmäßig ist der progressive Modus auf Standby für die Einstellungen der Richtlinie für **Bildqualität** auf **Hoch**, **Mittel** (Standard) und **Niedrig** festgelegt.

Der progressive Modus ist in folgenden Situationen deaktiviert:

- **Bildqualität** = **Immer verlustfrei** oder **Zu verlustfrei verbessern**
- **Bevorzugte Farbtiefe für einfache Grafiken** = 8-Bit
- **Videocodec zur Komprimierung verwenden** = **Für den gesamten Bildschirm** (wenn Vollbild-H.264 gewünscht wird)

Wenn der progressive Modus auf Standby ist, wird er standardmäßig aktiviert, wenn eine der folgenden Bedingungen eintritt:

- Die verfügbare Bandbreite fällt unter 2 MBit/s.
- Die Netzwerklatenz steigt über 200 ms.

Nach einem Moduswechsel bleibt der neue Modus mindestens 10 Sekunden aktiv, selbst wenn die ungünstigen Netzwerkbedingungen nur vorübergehend sind.

Ändern des progressiven Modusverhaltens

Sie können das progressive Modusverhalten ändern, indem Sie den folgenden Befehl ausführen:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     ProgressiveDisplay" -d "<value>" --force
2 <!--NeedCopy-->
```

Wobei <value> Folgendes angibt:

0 = Immer deaktiviert (niemals verwenden)

1 = Automatisch (Umschalten je nach Netzwerkbedingungen, Standardwert)

2 = Immer aktiviert

Im automatischen Modus (1) können Sie über einen der folgenden Befehle die Schwellenwerte ändern, bei denen ein Moduswechsel erfolgt:

```
1 sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

<value> ist der <Schwellenwert in KBit/s> (Standardwert = 2.048)

Beispiel: 4096 = progressiven Modus einschalten, wenn die Bandbreite unter 4 MBit/s fällt

```
1 sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SOFTWARE
     \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
     ProgressiveDisplayLatencyThreshold" -d "<value>" --force
2 <!--NeedCopy-->
```

<value> ist der <Schwellenwert in ms> (Standardwert = 200)

Beispiel: 100 = progressiven Modus einschalten, wenn die Netzwerklatenz unter 100 ms fällt.

Allgemeine Inhaltsumleitung

January 8, 2024

Clientlaufwerkzuordnung und Clientordnerumleitung

Wenn…	Dann…
Sie nur die Clientlaufwerkzuordnung auf dem Host (VDA) aktivieren,	werden vollständige Volumes auf der Clientseite automatisch den Sitzungen im Unterverzeichnis **ctxmnt** des Basisverzeichnisses zugeordnet.
Sie die Clientordnerumleitung auf dem Host (VDA) aktivieren und der Benutzer sie auf dem Benutzergerät (Client) konfiguriert,	wird der vom Benutzer angegebene Teil des lokalen Volumes umgeleitet.

USB-Geräteumleitung

USB-Geräte werden von der Citrix Workspace-App und Linux VDA-Desktop gemeinsam verwendet. Wenn ein USB-Gerät an einen Desktop umgeleitet wird, können Sie es wie ein lokal verbundenes Gerät verwenden.

Clientlaufwerkzuordnung

January 8, 2024

Mit der Clientlaufwerkzuordnung und Clientordnerumleitung können Sie clientseitige Dateien in der hostseitigen Sitzung verfügbar machen. Clientlaufwerkzuordnung und Clientordnerumleitung im Vergleich:

Wenn…	Dann…
Sie nur die Clientlaufwerkzuordnung auf dem Host (VDA) aktivieren,	werden vollständige Volumes auf der Clientseite automatisch den Sitzungen im Unterverzeichnis **ctxmnt** des Basisverzeichnisses zugeordnet.
Sie die Clientordnerumleitung auf dem Host (VDA) aktivieren und der Benutzer sie auf dem Benutzergerät (Client) konfiguriert,	wird der vom Benutzer angegebene Teil des lokalen Volumes umgeleitet.

Clientlaufwerkzuordnung aktivieren

Um die Clientlaufwerkzuordnung zu aktivieren, setzen Sie die Richtlinie **Clientlaufwerkumleitung** in Citrix Studio auf **Zugelassen**. Weitere Informationen zur Richtlinie finden Sie unter Dateiumleitung –

Richtlinieneinstellungen.

Clientordnerumleitung aktivieren und umzuleitende Ordner festlegen

Zum Aktivieren der Clientordnerumleitung führen Sie folgenden Befehl auf dem VDA aus:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\Client
   Folder Redirection" -t "REG_DWORD" -v "CFROnlyModeAvailable" -d "0
   x00000001" --force
<!--NeedCopy-->
```

Um anzugeben, welche Ordner vom Client zur hostseitigen Sitzung umgeleitet werden, führen Sie auf dem Benutzergerät die folgenden Schritte aus:

1. Stellen Sie sicher, dass die neueste Version der Citrix Workspace-App installiert ist.
2. Starten Sie vom Installationsverzeichnis der Citrix Workspace-App aus **CtxCFRUI.exe**.
3. Wählen Sie das Optionsfeld **Benutzerdefiniert** und fügen Sie Ordner hinzu oder bearbeiten oder entfernen Sie Ordner.
4. Trennen Sie die Sitzungen und stellen Sie dann neue Verbindungen her, damit die Einstellung wirksam wird.

USB-Geräteumleitung

February 9, 2024

USB-Geräte werden von der Citrix Workspace-App und Linux VDA-Desktop gemeinsam verwendet. Wenn ein USB-Gerät an einen Desktop umgeleitet wird, können Sie es wie ein lokal verbundenes Gerät verwenden.

> **Tipp:**
>
> Bei einer Netzwerklatenz unter 100 Millisekunden empfehlen wir die Verwendung einer USB-Geräteumleitung. Verwenden Sie keine USB-Geräteumleitung, wenn die Netzwerklatenz höher als 200 Millisekunden ist.

Die USB-Geräteumleitung umfasst drei hauptsächliche Funktionalitätsbereiche:

- Open-Source-USB/IP-Projekt
- Citrix USB-Sitzungsmodul
- Citrix USB-Servicemodul

Open-Source-USB/IP-Projekt:

Das USB/IP-Projekt umfasst einen Linux-Kerneltreiber und einige Benutzermodusbibliotheken für die Kommunikation mit dem Kerneltreiber zum Abruf aller USB-Daten.

Der Linux VDA implementiert die USB-Geräteumleitung auf der Grundlage des Open-Source-USB/IP-Projekts und verwendet den Kerneltreiber und die Benutzermodusbibliotheken von USB/IP wieder. Alle USB-Datenübertragungen zwischen dem Linux VDA und der Citrix Workspace-App erfolgen jedoch gekapselt im Citrix ICA USB-Protokoll.

Citrix USB-Sitzungsmodul:

Das Citrix USB-Sitzungsmodul fungiert als Kommunikationsbrücke zwischen dem USB/IP-Kernelmodul und der Citrix Workspace-App.

Citrix USB-Servicemodul:

Das Citrix USB-Servicemodul verwaltet alle Vorgänge auf USB-Geräten, z. B. das Anschließen oder Trennen von USB-Geräten.

Funktionsweise der USB-Geräteumleitung

Wenn ein USB-Gerät an den Linux VDA umgeleitet wird, werden normalerweise ein oder mehrere Geräteknoten im Systempfad /dev erstellt. Gelegentlich kann das umgeleitete Gerät jedoch nicht für eine aktive Linux VDA-Sitzung verwendet werden. USB-Geräte funktionieren nur mit Treibern, und manche Geräte erfordern auch Spezialtreiber. Sind diese Treiber nicht vorhanden, kann in der aktiven Linux VDA-Sitzung nicht auf das umgeleitete USB-Gerät zugegriffen werden. Installieren Sie die Treiber und konfigurieren Sie das System, um eine Verbindung mit USB-Geräten zu ermöglichen.

Der Linux VDA unterstützt diverse USB-Geräte, die erfolgreich von dem Client umgeleitet werden können.

Unterstützte USB-Geräte

> **Tipp:**
>
> Wir haben Unterstützung für USB 3.0-Anschlüsse hinzugefügt. Sie können USB 3.0-Geräte an USB 3.0-Anschlüsse eines Clientgeräts anschließen.

Bei den folgenden Geräten wurde die Unterstützung dieser Version des Linux VDA in Tests verifiziert. Andere Geräte können verwendet werden, jedoch können unerwartete Ergebnisse auftreten.

USB-Massenspeichergerät	VID:PID	Dateisystem
`Netac Technology Co., Ltd`	0dd8:173c	FAT32, NTFS

USB-Massenspeichergerät	VID:PID	Dateisystem
Kingston Datatraveler 101 II	0951:1625	FAT32, NTFS
Kingston Datatraveler GT101 G2	1567:8902	FAT32, NTFS
SanDisk SDCZ80 flash drive	0781:5580	FAT32, NTFS
WD HDD	1058:10B8	FAT32, NTFS
Toshiba Kingston DataTraveler 3.0 USB device	0930:6545	FAT32, NTFS
Taiwan OEM – OBSOLETE VendorCo ProductCode Disk 2.0	FFFF:5678	FAT32, NTFS
TD-RDF5A Transcend USB device	8564:4000	FAT32, NTFS

> **Hinweis:**
>
> Um NTFS auf Amazon Linux 2, CentOS, RHEL, Rocky Linux und SUSE zu verwenden, aktivieren Sie zuerst die NTFS-Unterstützung für diese Distributionen.

USB-3D-Maus	VID:PID
3DConnexion SpaceMouse Pro	046d: c62b

USB-Scanner	VID:PID
Epson Perfection V330 photo	04B8: 0142

Yubico USB	VID:PID
Yubico YubiKey OTP+FIDO+CCID - Keyboard, HID	1050:0407

Webcam USB	VID:PID
`Logitech composite USB device – WebCam, Audio`	0460:0825

Konfigurieren der USB-Geräteumleitung

Installieren oder Kompilieren des USB/IP-Kernelmoduls (nur für CentOS, RHEL und Rocky Linux)

Der Linux VDA verwendet USB/IP als virtuellen Hostcontroller für die USB-Geräteumleitung. Da das USB/IP-Kernelmodul in den meisten Fällen mit der Linux-Kernelversion 3.17 und höher veröffentlicht wird, müssen Sie das Kernelmodul nicht standardmäßig erstellen. Das USB/IP-Kernelmodul ist jedoch nicht für CentOS, RHEL und Rocky Linux verfügbar. Um die USB-Geräteumleitung mit diesen Linux-Distributionen zu verwenden, müssen Sie das USB/IP-Kernelmodul installieren oder kompilieren. Führen Sie Download und Installation des USB/IP-Kernelmoduls von https://pkgs.org/download/kmod-usbip gemäß Ihrer Linux-Distribution durch.

Richtlinien für die USB-Geräteumleitung festlegen

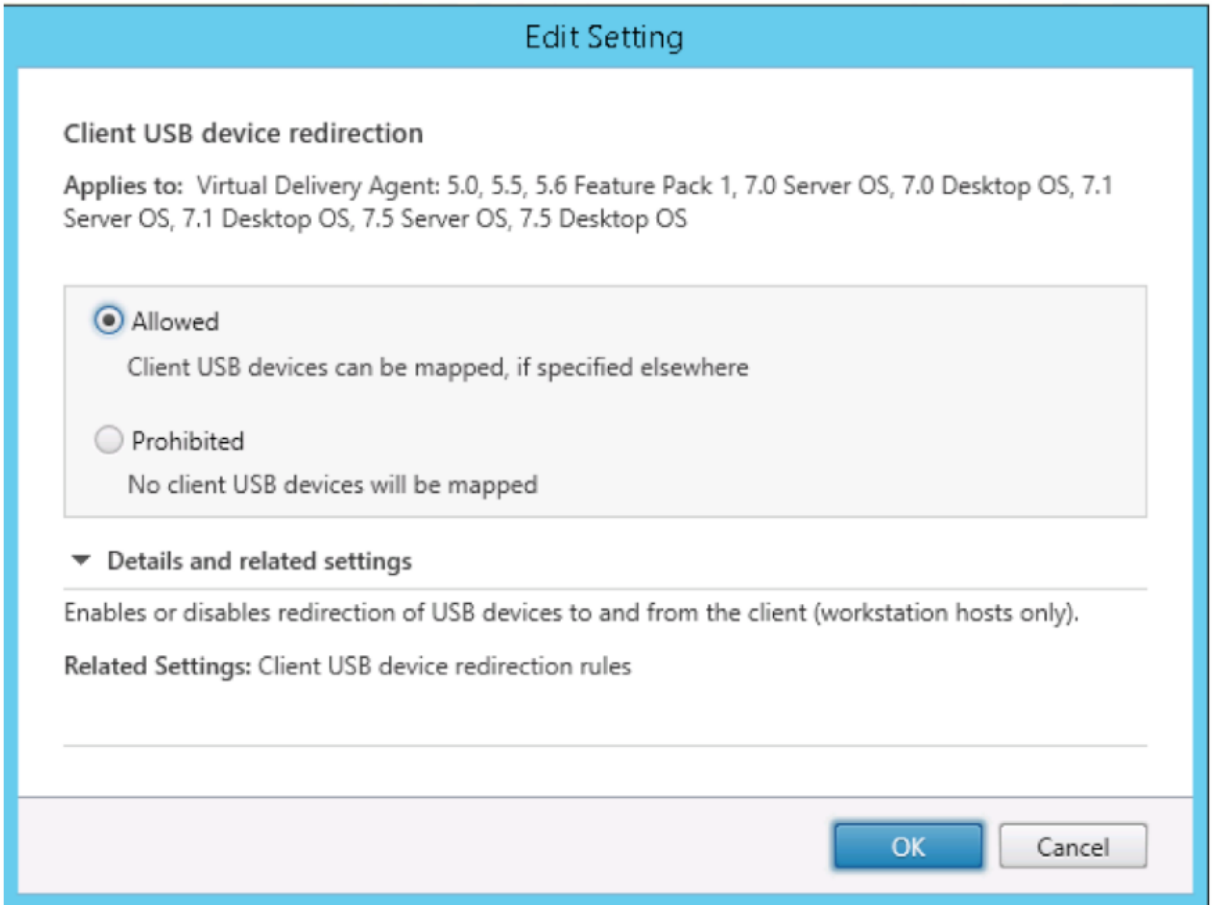
Die USB-Geräteumleitung wird über eine Citrix Richtlinie aktiviert bzw. deaktiviert. Der Gerätetyp kann außerdem über eine Delivery Controller-Richtlinie festgelegt werden. Konfigurieren Sie die folgenden Richtlinien und Regeln, um die USB-Geräteumleitung für den Linux VDA zu aktivieren:

- Richtlinie für die Client-USB-Geräteumleitung
- Regeln für die Client-USB-Geräteumleitung

USB-Geräteumleitung aktivieren In Citrix Studio können Sie die Umleitung von USB-Geräten vom Client (nur Arbeitsstationshosts) aktivieren und deaktivieren.

Führen Sie im Dialogfeld **Einstellung bearbeiten** folgende Schritte aus:

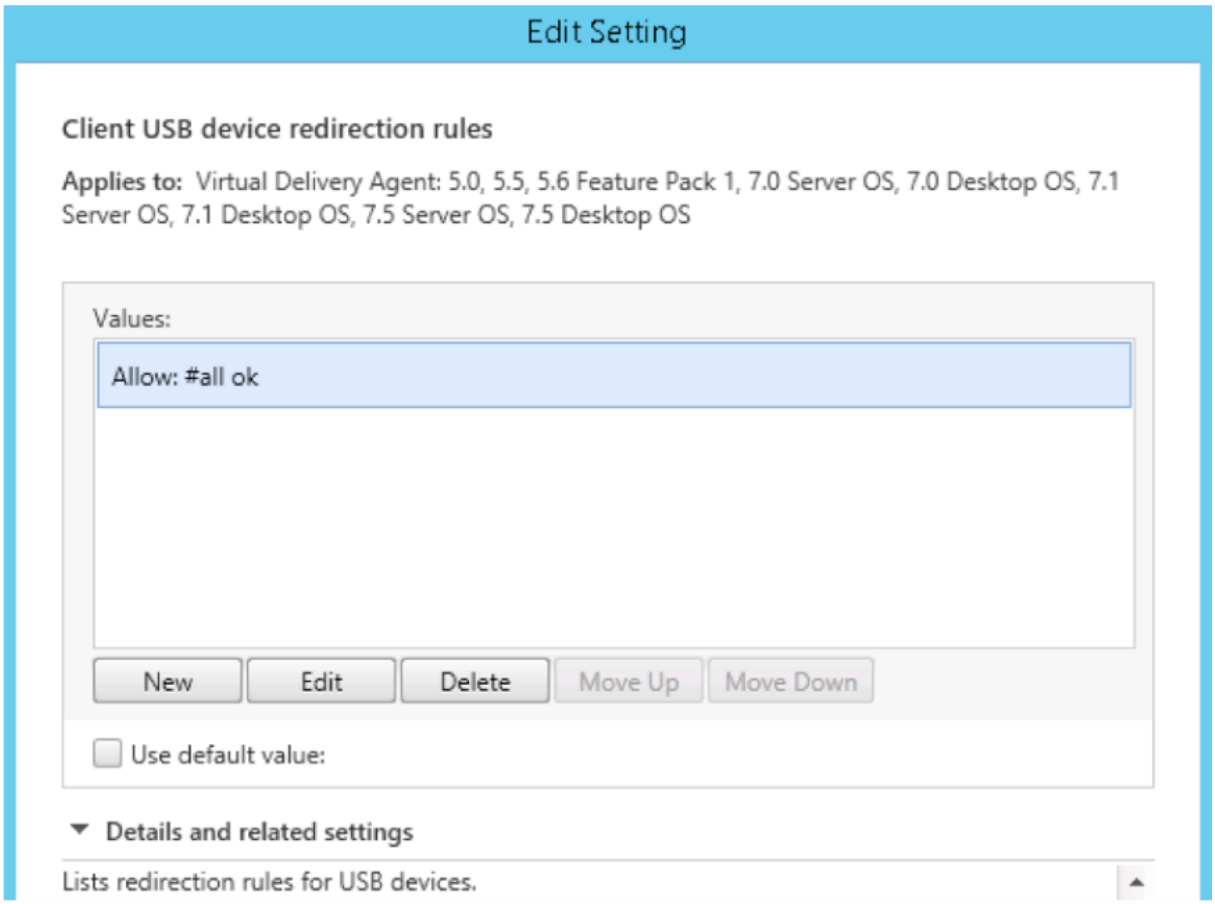
1. Wählen Sie **Zugelassen**.
2. Klicken Sie auf **OK**.



Regeln für die USB-Geräteumleitung festlegen Nach dem Aktivieren der USB-Umleitungsrichtlinie legen Sie mit Citrix Studio die Regeln für die Umleitung fest, d. h. welche Geräte auf dem Linux VDA zulässig sind und welche nicht.

Führen Sie im Dialogfeld **Regeln für die Client-USB-Geräteumleitung** folgende Schritte aus:

1. Klicken Sie auf **Neu**, um eine Umleitungsregel hinzuzufügen oder auf **Bearbeiten**, um eine vorhandene Regel zu prüfen.
2. Nach dem Erstellen bzw. Ändern der Regel klicken Sie auf **OK**.



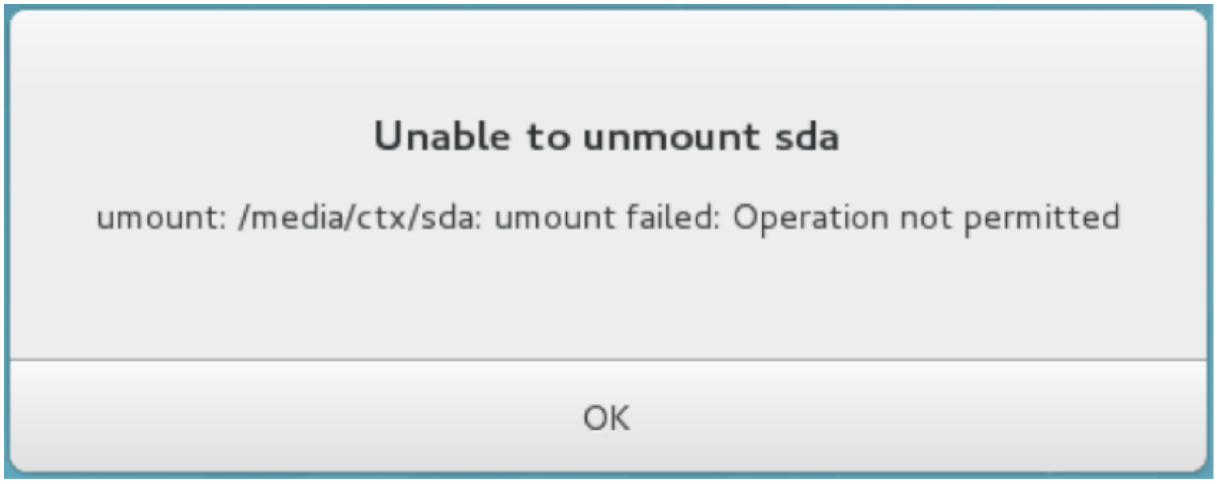
Weitere Informationen zum Konfigurieren der generischen USB-Geräteumleitung finden Sie im Citrix Generic USB Redirection Configuration Guide.

Behandeln von Problemen bei der USB-Geräteumleitung

Anhand der Informationen in diesem Abschnitt können Sie diverse Probleme beheben, die bei der Verwendung des Linux VDA auftreten können.

Bereitstellung eines umgeleiteten USB-Datenträgers kann nicht aufgehoben werden

Der Linux VDA verwaltet alle von der Citrix Workspace-App umgeleiteten USB-Datenträger unter Verwendung von Administratorrechten, damit nur der Besitzer eines umgeleiteten Geräts darauf zugreifen kann. Daher können Sie die Bereitstellung des Geräts nur mit Administratorrechten aufheben.



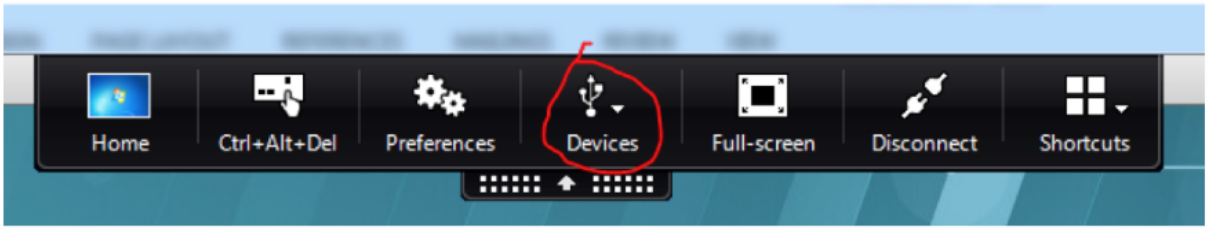
Dateiverlust beim Beenden der Umleitung eines USB-Datenträgers

Wenn Sie die Umleitung eines USB-Datenträgers sofort über die Symbolleiste der Citrix Workspace-App beenden, können die Dateien, die Sie auf dem Datenträger geändert oder erstellt haben, verloren gehen. Dieses Problem tritt auf, weil beim Schreiben von Daten in ein Dateisystem der Speichercache im Dateisystem eingebunden wird. Die Daten werden nicht auf den Datenträger selbst geschrieben. Wenn Sie die Umleitung über die Symbolleiste der Citrix Workspace-App beenden, bleibt keine Zeit zum Übertragen der Daten auf den Datenträger, und die Daten gehen verloren.

Zur Problemlösung verwenden Sie den **sync**-Befehl in einem Terminal, um die Daten auf den Datenträger zu übertragen, bevor Sie die USB-Umleitung beenden.

Keine Geräte in der Symbolleiste der Citrix Workspace-App

Es kann vorkommen, dass in der Symbolleiste der Citrix Workspace-App keine Geräte aufgeführt werden, d. h. dass keine USB-Umleitung stattfindet.



Prüfen Sie in diesem Fall Folgendes:

- Die Richtlinie ist auf Zulassen der USB-Geräteumleitung konfiguriert.
- Das Citrix USB-Servicemodul wird ausgeführt.

Wenn die Richtlinie nicht richtig festgelegt ist, korrigieren Sie sie unter Bezugnahme auf den Abschnitt Festlegen von Richtlinien für die USB-Geräteumleitung in diesem Artikel.

Wenn das Citrix USB-Servicemodul nicht ausgeführt wird, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie mit dem folgenden Befehl, ob ein USB/IP-Kernelmodul in Ihrer Linux-Distribution verfügbar ist:

```
modinfo usbip-core
<!--NeedCopy-->
```

2. Wenn die Ausgabe wie folgt angezeigt wird, installieren oder kompilieren Sie das USB/IP-Kernelmodul entsprechend Ihrer Linux-Distribution:

```
modinfo: ERROR: Module usbip-core not found.
<!--NeedCopy-->
```

   - Informationen zu Amazon Linux 2, CentOS, RHEL und Rocky Linux finden Sie im Abschnitt Installieren oder Kompilieren des USB/IP-Kernelmoduls in diesem Artikel.
   - Laden Sie für SUSE das USB/IP-Paket von https://software.opensuse.org/package/usbip herunter und installieren Sie es.
   - Führen Sie für Ubuntu/Debian die folgenden Schritte aus, um das USB/IP-Kernelmodul zu kompilieren und zu installieren:

     a) Laden Sie den Quellcode des USB/IP-Kernelmoduls herunter.

     Rufen Sie das Linux-Kernel-Repository unter https://github.com/torvalds/linux/tree/master/drivers/usb/usbip auf, wählen Sie die Ziel-Linux-Kernelversion (v4.15 oder höher) aus und fordern Sie den Link an, z. B. https://github.com/torvalds/linux/tree/v4.15/drivers/usb/usbip.

     Gehen Sie zu DownGit und geben Sie den vorherigen Link ein, um einen Download-Link zum Herunterladen des USB/IP-Quellcodes zu erstellen.

     b) Entpacken Sie die Quelldatei mit den folgenden Befehlen:

```
unzip ${
 USBIP_SRC }
 .zip

cd usbip
<!--NeedCopy-->
```

     c) Ändern Sie die Datei **Makefile** wie folgt:

```
# SPDX-License-Identifier: GPL-2.0

ccflags-$(CONFIG_USBIP_DEBUG) := -DDEBUG
```



```
4
5  obj-$(CONFIG_USBIP_CORE) += usbip-core.o
6
7  usbip-core-y := usbip_common.o usbip_event.o
8
9  obj-$(CONFIG_USBIP_VHCI_HCD) += vhci-hcd.o
10
11 vhci-hcd-y := vhci_sysfs.o vhci_tx.o vhci_rx.o vhci_hcd.o
12
13 #obj-$(CONFIG_USBIP_HOST) += usbip-host.o
14
15 #usbip-host-y := stub_dev.o stub_main.o stub_rx.o stub_tx.o
16
17 #obj-$(CONFIG_USBIP_VUDC) += usbip-vudc.o
18
19 #usbip-vudc-y := vudc_dev.o vudc_sysfs.o vudc_tx.o vudc_rx.
      o vudc_transfer.o vudc_main.o
20 <!--NeedCopy-->
```

d) Kompilieren Sie den Quellcode:

```
1  apt-get install linux-headers-`uname -r`
2
3  make -C /lib/modules/`uname -r`/build M=$PWD
4  <!--NeedCopy-->
```

e) Installieren Sie das USB/IP-Kernelmodul:

```
1  cp usbip-core.ko vhci-hcd.ko /opt/Citrix/VDA/lib64/
2  <!--NeedCopy-->
```

f) Starten Sie den Dienst **ctxusbsd** neu, um das USB/IP-Kernelmodul zu laden:

```
1  service ctxusbsd restart
2  <!--NeedCopy-->
```

Fehlschlagen der Umleitung, wenn in der Symbolleiste der Citrix Workspace-App angezeigte USB-Geräte als richtlinienbeschränkt ausgewiesen sind

Wenn das Problem auftritt, führen Sie die folgenden Schritte aus:

- Konfigurieren Sie die Linux VDA-Richtlinie zum Aktivieren der Umleitung.
- Prüfen Sie, ob in der Registrierung der Citrix Workspace-App weitere Richtlinieneinschränkungen konfiguriert sind. Prüfen Sie **DeviceRules** im Registrierungspfad, um sicherzustellen, dass dem Gerät durch diese Einstellung kein Zugriff verweigert wird:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

Weitere Informationen finden Sie im Knowledge Center-Artikel How to Configure Automatic Redirection of USB Devices.

Ein USB-Gerät wird umgeleitet, kann jedoch nicht in einer Sitzung verwendet werden

In der Regel können nur unterstützte USB-Geräte umgeleitet werden. Auch andere Geräte werden evtl. in eine aktive Linux VDA-Sitzung umgeleitet. Es wird für jedes umgeleitete Gerät ein im Besitz des Benutzers stehender Knoten im Systempfad **/dev** erstellt. Allerdings bestimmen Treiber und Konfiguration, ob der Benutzer das Gerät verwenden kann. Wenn Sie ein angeschlossenes Gerät finden, auf das nicht zugegriffen werden kann, fügen Sie es einer uneingeschränkten Richtlinie hinzu.

> **Hinweis:**
>
> Für USB-Laufwerke erfolgt die Konfiguration und Einbindung durch den Linux VDA. Der Benutzer, der das Laufwerk installiert hat (und kein anderer), kann ohne zusätzliche Konfiguration auf das Laufwerk zugreifen. Dies ist bei Geräten, die nicht auf der Liste der unterstützten Geräte stehen, evtl. nicht möglich.

Zwischenablagenumleitung

January 8, 2024

Die Umleitung der Zwischenablage ermöglicht das Kopieren und Einfügen von Daten zwischen Anwendungen in der VDA-Sitzung und Anwendungen auf dem Clientgerät.

In diesem Artikel werden die verfügbaren Citrix-Richtlinien beschrieben, mit denen Sie eine Zwischenablagenumleitung aktivieren.

Citrix-Richtlinien für die Zwischenablagenumleitung

Clientzwischenablagenumleitung

Mit dieser Einstellung legen Sie fest, ob die Zwischenablage auf dem Clientgerät der Zwischenablage auf dem VDA zugeordnet wird.

Die Standardeinstellung der Zwischenablagenumleitung ist **Zugelassen**.

Wählen Sie **Nicht zugelassen**, um die Datenübertragung zwischen einer Sitzung und der lokalen Zwischenablage durch Kopieren und Einfügen zu verhindern. Benutzer können weiterhin die Zwischenablage für das Kopieren von Daten zwischen Anwendungen einsetzen, die in Sitzungen ausgeführt werden.

Bandbreitenlimit für Zwischenablagenumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite (in KBit/s) für Datenübertragungen zwischen der Sitzung und den lokalen Zwischenablagen an.

Bandbreitenlimit für Zwischenablagenumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für Datenübertragungen zwischen der Sitzung und den lokalen Zwischenablagen als Prozentsatz der Gesamtsitzungsbandbreite an.

Client-zu-Sitzung-Übertragungsgröße für Zwischenablage beschränken

Mit dieser Einstellung legen Sie die maximale Datenmenge in der Zwischenablage fest, die durch einmaliges Kopieren und Einfügen von einem Clientgerät an eine virtuelle Sitzung übertragen werden kann.

Um die per Zwischenablage übertragene Datenmenge zu begrenzen, aktivieren Sie die Einstellung **Client-zu-Sitzung-Übertragungsgröße für Zwischenablage beschränken**. Geben Sie dann im Feld **Größenbeschränkung** einen Wert in Kilobyte ein, um die Größe der Datenübertragung zwischen der lokalen Zwischenablage und einer Sitzung zu definieren.

Diese Einstellung ist standardmäßig deaktiviert, d. h. es gibt keine Beschränkung für Client-zu-Sitzung-Übertragungen.

Sitzung-zu-Client-Übertragungsgröße für Zwischenablage beschränken

Mit dieser Einstellung legen Sie die maximale Datenmenge in der Zwischenablage fest, die durch einmaliges Kopieren und Einfügen von einer virtuellen Sitzung zu einem Clientgerät übertragen werden kann.

Um die per Zwischenablage übertragene Datenmenge zu begrenzen, aktivieren Sie die Einstellung **Sitzung-zu-Client-Übertragungsgröße für Zwischenablage beschränken**. Geben Sie dann im Feld **Größenbeschränkung** einen Wert in Kilobyte ein, um die Größe der Datenübertragung zwischen einer Sitzung und der lokalen Zwischenablage zu definieren.

Diese Einstellung ist standardmäßig deaktiviert, d. h. es gibt keine Beschränkung für Sitzung-zu-Client-Übertragungen.

Einstellungen "Schreiben in Clientzwischenablage einschränken"und "Zum Schreiben in Clientzwischenablage zugelassene Formate"

Durch Aktivieren dieser beiden Einstellungen können Sie zulassen, dass bestimmte Datenformate durch Kopieren und Einfügen aus der Sitzung auf den Client geschrieben werden.

Die folgenden Zwischenablageformate sind vom System definiert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_UNICODETEXT
- CF_LOCALE
- CF_DIBV5
- CF_HDROP

Einstellungen "Schreiben in Sitzungszwischenablage einschränken"und "Zum Schreiben in Sitzungszwischenablage zugelassene Formate"

Durch Aktivieren dieser beiden Einstellungen können Sie zulassen, dass bestimmte Datenformate durch Kopieren und Einfügen vom Client in die Sitzung geschrieben werden.

Die folgenden Zwischenablageformate sind vom System definiert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_UNICODETEXT
- CF_LOCALE
- CF_DIBV5
- CF_HDROP

Tastatur

January 8, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Client-IME
- Synchronisierung der Client-IME-Benutzeroberfläche
- Dynamische Tastaturlayoutsynchronisierung
- Bildschirmtastatur
- Unterstützung der Eingabe in mehreren Sprachen

Client-Eingabemethoden-Editor (IME)

January 8, 2024

Übersicht

Doppelbytezeichen (z. B. Chinesisch, Japanisch und Koreanisch) müssen über einen IME eingegeben werden. Solche Zeichen können mit jedem clientseitig mit der Citrix Workspace-App kompatiblen Eingabemethoden-Editor eingegeben werden (z. B. Windows-eigener CJK IME).

Installation

Dieses Feature wird automatisch installiert, wenn Sie den Linux VDA installieren.

Verwendung

Öffnen Sie wie gewohnt eine Citrix Virtual Apps- oder Citrix Virtual Desktops-Sitzung.

Ändern Sie die Eingabemethode nach Bedarf auf der Clientseite, um das IME-Feature zu verwenden.

Bekannte Probleme

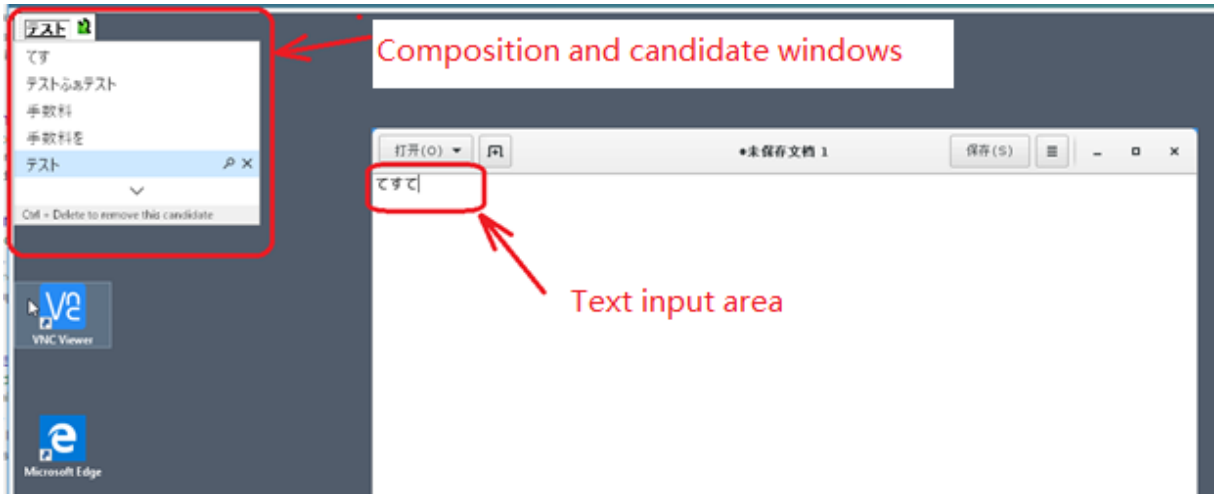
- Sie müssen auf eine Zelle in einer Google-Kalkulationstabelle doppelklicken, damit Sie mit dem Client-IME-Feature Zeichen in die Zelle eingeben können.
- Das Client-IME-Feature wird in Kennwortfeldern nicht automatisch deaktiviert.
- Die IME-Benutzerschnittstelle folgt nicht dem Cursor im Eingabebereich.

Synchronisierung der Client-IME-Benutzeroberfläche

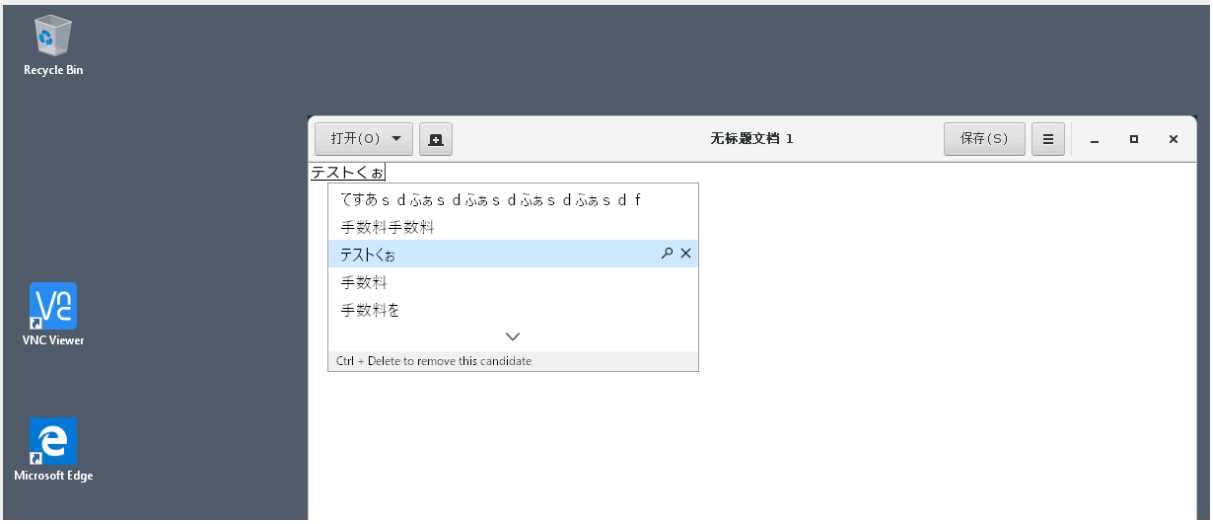
January 8, 2024

Übersicht

Bislang befand sich die Client-IME-Benutzeroberfläche (einschließlich Kompositionsfenster und Kandidatenfenster) in der linken oberen Ecke des Bildschirms. Sie folgte dem Cursor nicht und war unter Umständen weit von ihm entfernt im Texteingabebereich.



Citrix bietet für die Client-IME mehr Benutzerfreundlichkeit und eine optimierte Anwendung:



Voraussetzungen für die Verwendung des Features

1. Aktivieren Sie Intelligent Input Bus (`IBus`) auf dem Linux VDA. Informationen zum Aktivieren von `IBus` auf einem Linux-Betriebssystem finden Sie in der Betriebssystemdokumentation des Herstellers. Beispiel:
   - Ubuntu: https://help.ubuntu.com/community/ibus
   - CentOS, RHEL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/7.0_release_notes/sect-red_hat_enterprise_linux-7.0_release_notes-internationalization-input_methods
   - Debian: https://wiki.debian.org/I18n/ibus
   - SUSE: https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-gnome-settings.html#sec-gnome-settings-lang
2. Das Feature wird automatisch installiert, Sie müssen es jedoch vor der Verwendung aktivieren.

Aktivieren und Deaktivieren des Features

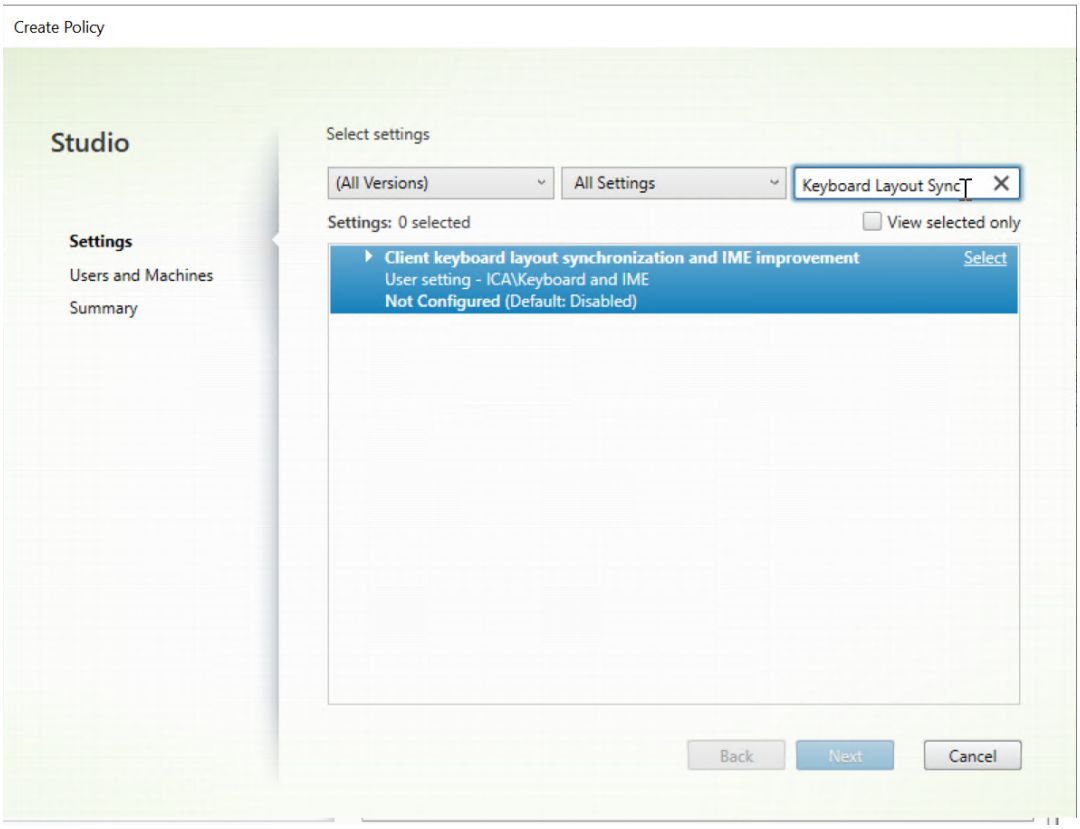
Die Synchronisierung der Client-IME-Benutzeroberfläche ist standardmäßig deaktiviert. Um das Feature zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, oder bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg`.

> **Hinweis:**
>
> Die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Maschinenobjekte oder auf alle Objekte in Ihrer Site angewendet werden. Registrierungseinstellungen

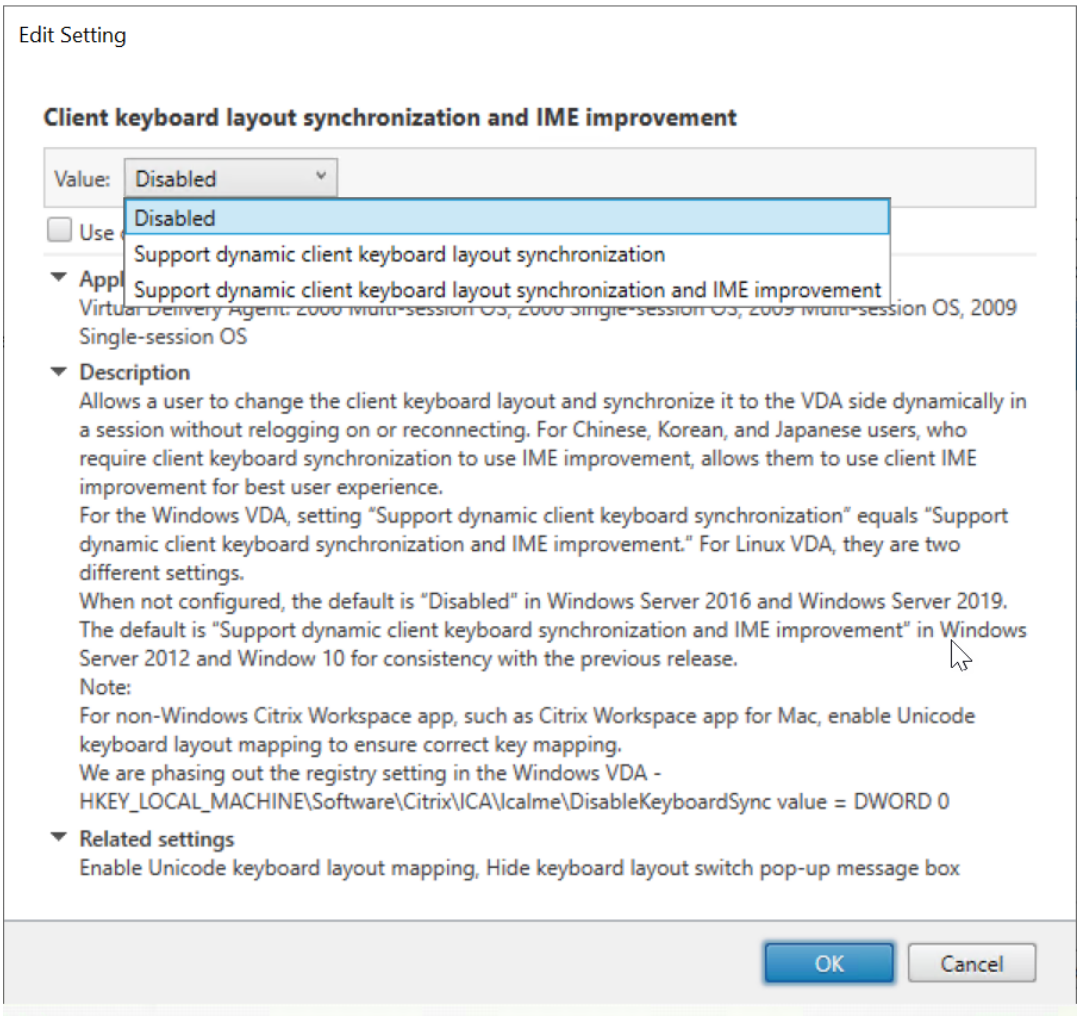
> auf einem bestimmten Linux VDA gelten für alle Sitzungen auf diesem VDA.

- Legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, um die Synchronisierung der Client-IME-Benutzeroberfläche zu aktivieren oder zu deaktivieren:

  1. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.
  2. Suchen Sie nach der Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME**.



  3. Klicken Sie neben dem Richtliniennamen auf **Auswählen**.
  4. Legen Sie die Richtlinie fest.



Es stehen drei Optionen zur Verfügung:

- **Deaktiviert**: Deaktiviert die dynamische Tastaturlayoutsynchronisierung und die Synchronisierung der Client-IME-Benutzeroberfläche
- **Dynamische Client-Tastaturlayoutsynchronisierung unterstützen**: Aktiviert die dynamische Tastaturlayoutsynchronisierung unabhängig vom DWORD-Wert des Registrierungsschlüssels **SyncKeyboardLayout** unter `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Dynamische Client-Tastaturlayoutsynchronisierung und Verbesserung des IME unterstützen**: Aktiviert sowohl die dynamische Tastaturlayoutsynchronisierung als auch die Synchronisierung der Client-IME-Benutzeroberfläche unabhängig von den DWORD-Werten der Registrierungsschlüssel **SyncKeyboardLayout** und **SyncClientIME** unter `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg`, um die Synchronisierung der Client-IME-Benutzeroberfläche zu aktivieren oder zu deaktivieren:

Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v  "
   SyncClientIME" -d "0x00000001"
<!--NeedCopy-->
```

Führen Sie folgenden Befehl aus, um das Feature zu deaktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncClientIME" -d "0x00000000"
<!--NeedCopy-->
```

Dynamische Tastaturlayoutsynchronisierung

January 8, 2024

Bisher musste das Tastaturlayout auf dem Linux VDA mit dem auf dem Clientgerät identisch sein. Probleme bei der Tastenzuordnung konnten beispielsweise auftreten, wenn das Tastaturlayout auf dem Clientgerät von Englisch auf Deutsch geändert wurde, nicht jedoch auf dem VDA.

Das Problem wurde von Citrix behoben. Das Tastaturlayout des VDAs wird automatisch mit dem des Clientgeräts synchronisiert. Jedes Mal, wenn sich das Tastaturlayout auf dem Clientgerät ändert, ändert sich das Layout auf dem VDA entsprechend mit.

> **Hinweis:**
>
> Die Citrix Workspace-App für HTML5 bietet keine Unterstützung für die dynamische Tastaturlayoutsynchronisierung.

Konfiguration

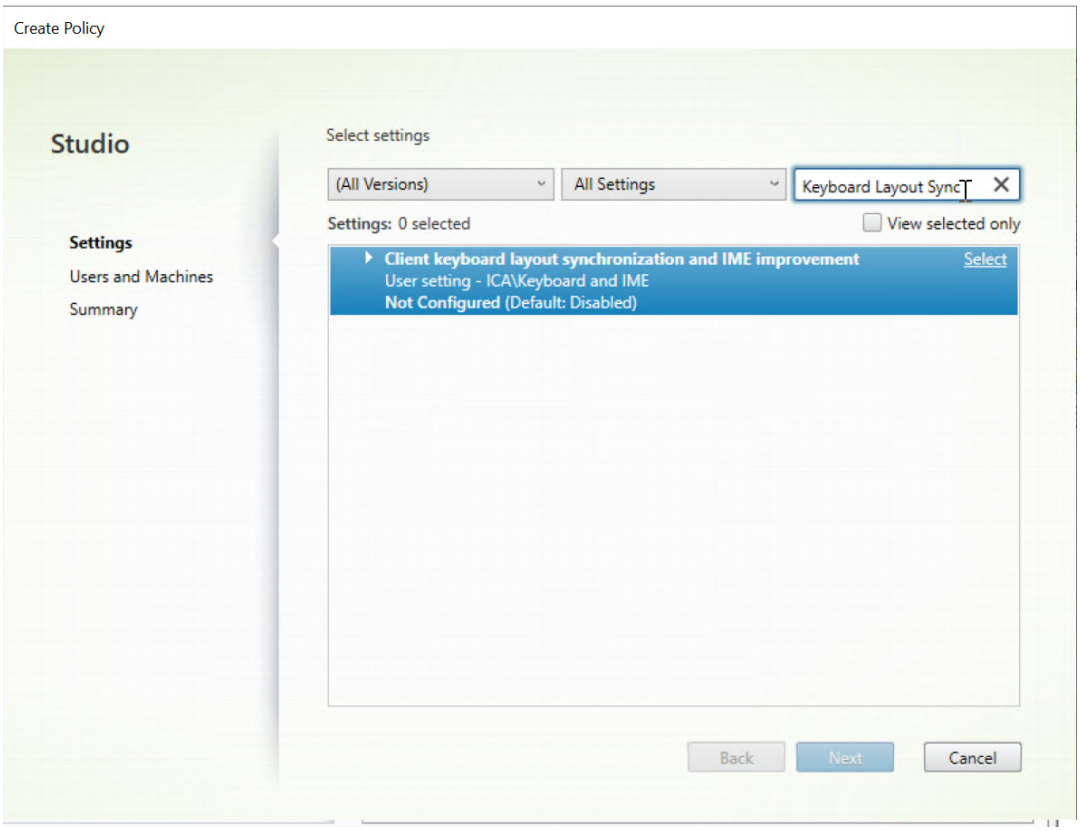
Die dynamische Tastaturlayoutsynchronisierung ist standardmäßig deaktiviert. Um das Feature zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, oder bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg` .

> **Hinweis:**
>
> Die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Maschinenobjekte oder auf alle Objekte in Ihrer Site angewendet werden. Registrierungseinstellungen

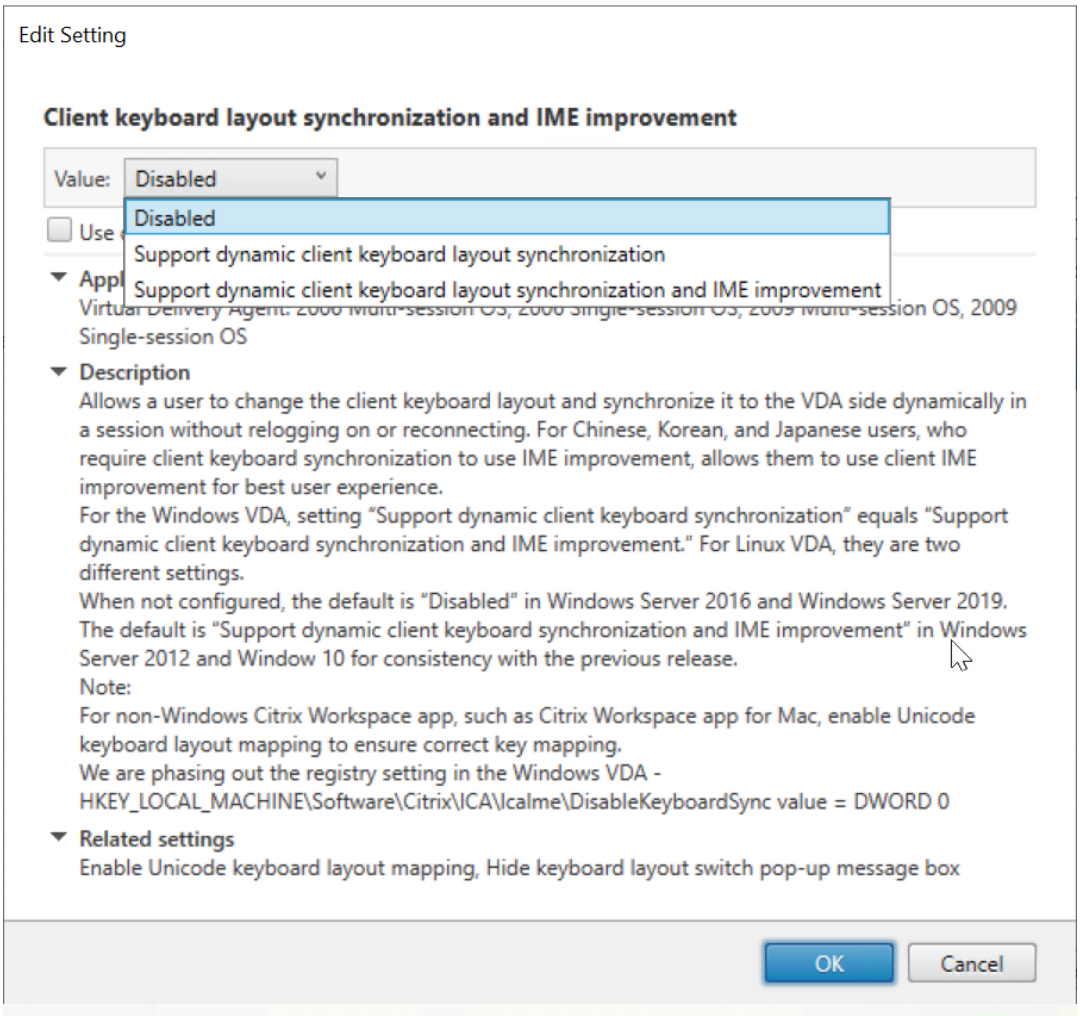
> auf einem bestimmten Linux VDA gelten für alle Sitzungen auf diesem VDA.

- Legen Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME** fest, um die dynamische Tastaturlayoutsynchronisierung zu aktivieren oder zu deaktivieren.

  1. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.
  2. Suchen Sie nach der Richtlinie **Client-Tastaturlayoutsynchronisierung und Verbesserung des IME**.



  3. Klicken Sie neben dem Richtliniennamen auf **Auswählen**.
  4. Legen Sie die Richtlinie fest.



Es stehen drei Optionen zur Verfügung:

- **Deaktiviert**: Deaktiviert die dynamische Tastaturlayoutsynchronisierung und die Synchronisierung der Client-IME-Benutzeroberfläche
- **Dynamische Client-Tastaturlayoutsynchronisierung unterstützen**: Aktiviert die dynamische Tastaturlayoutsynchronisierung unabhängig vom DWORD-Wert des Registrierungsschlüssels **SyncKeyboardLayout** unter `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.
- **Dynamische Client-Tastaturlayoutsynchronisierung und Verbesserung des IME unterstützen**: Aktiviert sowohl die dynamische Tastaturlayoutsynchronisierung als auch die Synchronisierung der Client-IME-Benutzeroberfläche unabhängig von den DWORD-Werten der Registrierungsschlüssel **SyncKeyboardLayout** und **SyncClientIME** unter `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Citrix\LanguageBar`.

- Bearbeiten Sie die Registrierung über das Hilfsprogramm `ctxreg`, um die dynamische Tastaturlayoutsynchronisierung zu aktivieren oder zu deaktivieren:

Führen Sie folgenden Befehl aus, um dieses Feature zu aktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncKeyboardLayout" -d "0x00000001"
<!--NeedCopy-->
```

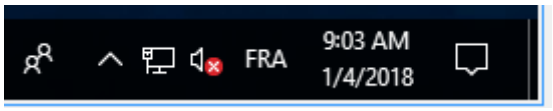
Führen Sie folgenden Befehl aus, um dieses Feature zu deaktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Control\Citrix\LanguageBar" -v "
   SyncKeyboardLayout" -d "0x00000000"
<!--NeedCopy-->
```

Verwendung

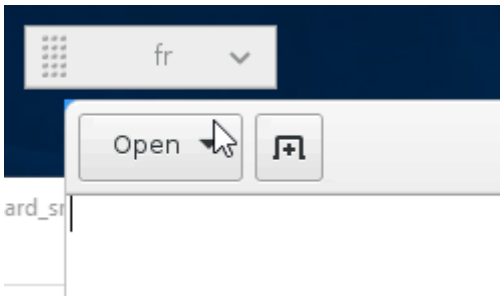
Wenn das Feature aktiviert ist, ändert sich das Tastaturlayout auf dem VDA automatisch zusammen mit dem auf dem Clientgerät.

Wenn Sie beispielsweise das Tastaturlayout auf einem Clientgerät auf Französisch ändern:

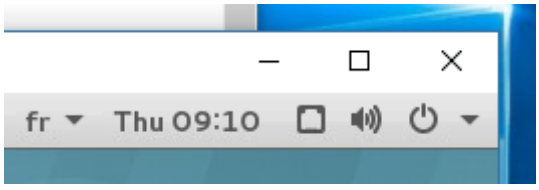


Ändert sich das Tastaturlayout der Linux VDA-Sitzung ebenfalls in “fr”.

In Anwendungssitzungen können Sie diese automatische Änderung sehen, wenn Sie die Sprachenleiste aktiviert haben:



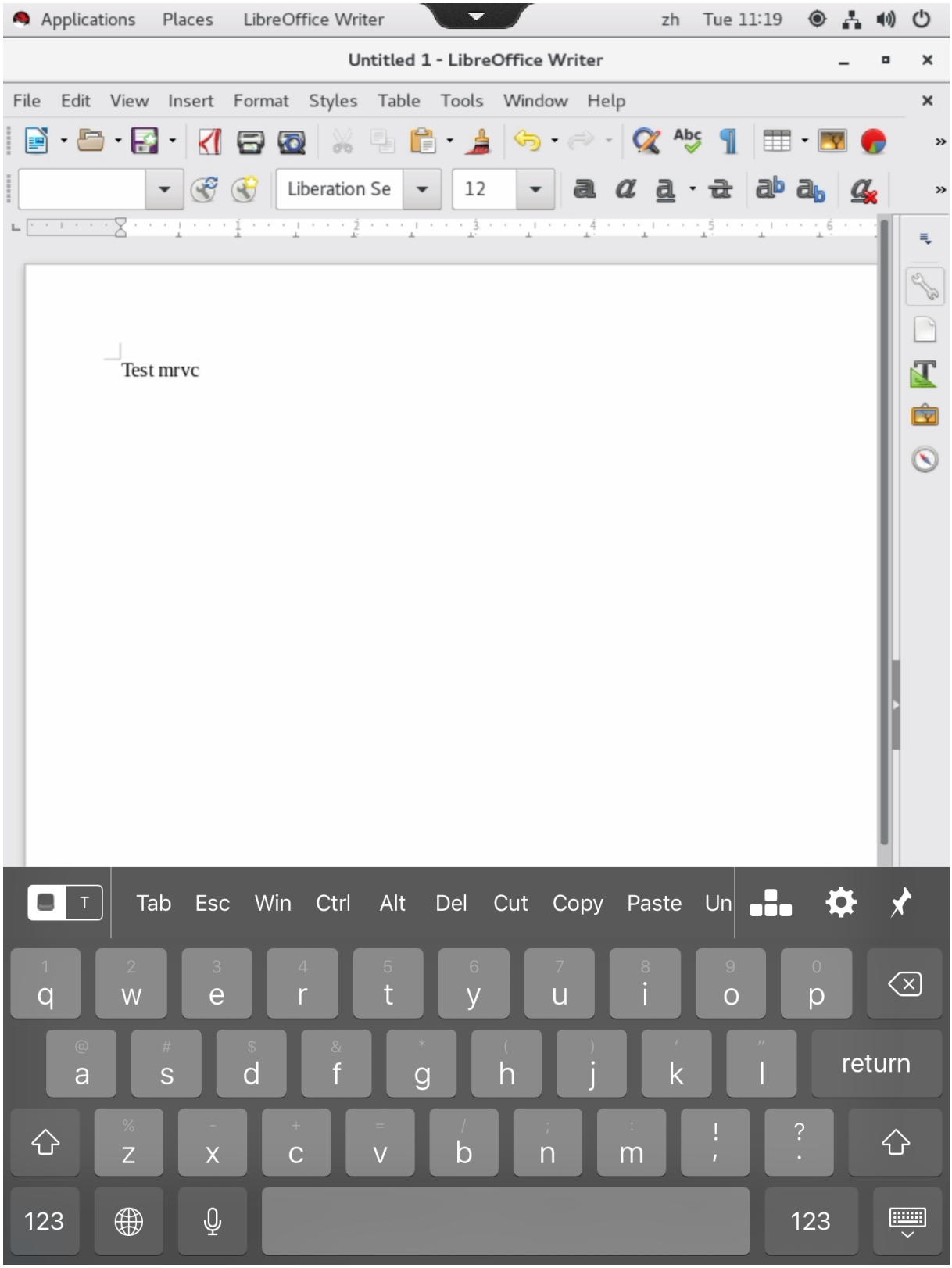
In einer Desktop-Sitzung sehen Sie diese automatische Änderung in der Taskleiste:



Bildschirmtastatur

January 8, 2024

Die Funktion der Bildschirmtastatur ist in einem virtuellen Linux-Desktop oder in einer Anwendungssitzung verfügbar. Die Bildschirmtastatur wird automatisch ein- oder ausgeblendet, wenn Sie auf ein Eingabefeld gehen oder es verlassen.



> **Hinweis:**
>
> Das Feature wird für die Citrix Workspace-App für iOS und Android unterstützt.

Aktivieren und Deaktivieren des Features

Dieses Feature ist standardmäßig deaktiviert. Sie können es mit dem Hilfsprogramm **ctxreg** aktivieren oder deaktivieren. Die Konfiguration des Features auf einem Linux VDA gilt für alle Sitzungen auf diesem VDA.

Aktivieren des Features:

1. Führen Sie diesen Befehl aus:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\
     CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v "
     Enabled" -d "0x00000001"
2 <!--NeedCopy-->
```

2. Legen Sie in Citrix Studio die Richtlinie **Automatische Anzeige der Tastatur** auf **Zulässig** fest.
3. (Optional) Führen Sie für RHEL 7 und CentOS 7 den folgenden Befehl aus, um Intelligent Input Bus (IBus) als den Standard-IM-Dienst zu konfigurieren:

```
1 echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
2 <!--NeedCopy-->
```

Führen Sie folgenden Befehl aus, um das Feature zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKLM\System\CurrentControlSet\
     Control\Citrix\VirtualChannels\MrVc"  -v "Enabled" -d "0x00000000"
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die vorherigen Einstellungen werden wirksam, wenn Sie sich an einer neuen Sitzung anmelden oder sich bei der aktuellen Sitzung abmelden und wieder anmelden.

Einschränkungen

- Das Feature funktioniert möglicherweise nicht wie erwartet mit Google Chrome, LibreOffice und anderen Apps.
- Um die Bildschirmtastatur wieder anzuzeigen, nachdem sie manuell ausgeblendet wurde, klicken Sie auf ein Nicht-Eingabefeld und dann wieder auf das aktuelle Eingabefeld.

- Die Bildschirmtastatur wird möglicherweise nicht angezeigt, wenn Sie in einem Webbrowser von einem Eingabefeld zu einem anderen klicken. Als Workaround klicken Sie auf ein Nicht-Eingabefeld und dann wieder auf das Zieleingabefeld.
- Das Feature unterstützt keine Unicode-Zeichen und Doppelbyte-Zeichen (z. B. chinesische, japanische und koreanische Zeichen).
- Die Bildschirmtastatur ist für Kennworteingabefelder nicht verfügbar.
- Die Bildschirmtastatur kann das aktuelle Eingabefeld überlappen. Verschieben Sie in diesem Fall das App-Fenster oder scrollen Sie auf dem Bildschirm nach oben, um das Eingabefeld an eine zugängliche Position zu verschieben.
- Aufgrund von Kompatibilitätsproblemen zwischen der Citrix Workspace-App und Huawei-Tablets erscheint die Bildschirmtastatur auf Huawei-Tablets sogar dann, wenn eine physische Tastatur angeschlossen ist.

Unterstützung der Eingabe in mehreren Sprachen

January 8, 2024

Citrix unterstützt ab Linux VDA Version 1.4 auch veröffentlichte Anwendungen. Benutzer können damit auch ohne Linux-Desktopumgebung auf eine gewünschte Linux-Anwendung zugreifen.

Die systemeigene Sprachleiste auf dem Linux VDA war jedoch für veröffentlichte Anwendungen nicht verfügbar, da sie eng in die Linux-Desktopumgebung integriert ist. Daher konnten Benutzer keinen Text in einer Sprache eingeben, für die IME erforderlich ist, z. B. Chinesisch, Japanisch oder Koreanisch. Außerdem war während einer Anwendungssitzung kein Wechsel des Tastaturlayouts möglich.

Dieses Feature bietet nun eine Sprachleiste für veröffentlichte Anwendungen, bei denen eine Texteingabe möglich ist. Über die Sprachleiste können Benutzer einen serverseitigen Eingabemethoden-Editor auswählen und während Anwendungssitzungen das Tastaturlayout wechseln.

Konfiguration

Sie können das Feature mit dem Hilfsprogramm **ctxreg** aktivieren oder deaktivieren (standardmäßig ist es deaktiviert). Die Konfiguration des Features auf einem Linux VDA-Server gilt für alle Anwendungen, die auf diesem VDA veröffentlicht werden.

Der Schlüssel zur Konfiguration ist "HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Control\Citrix\LanguageI
, der Typ ist "DWORD".

Führen Sie folgenden Befehl aus, um dieses Feature zu aktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
     x00000001"
2 <!--NeedCopy-->
```

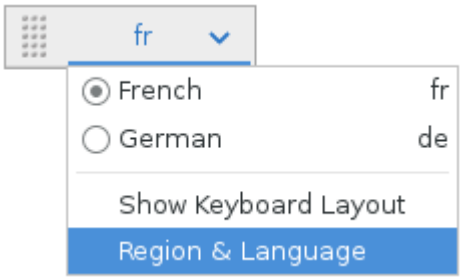
Führen Sie folgenden Befehl aus, um dieses Feature zu deaktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
     CurrentControlSet\Control\Citrix\LanguageBar" -v "Enabled" -d "0
     x00000000"
2 <!--NeedCopy-->
```

Verwendung

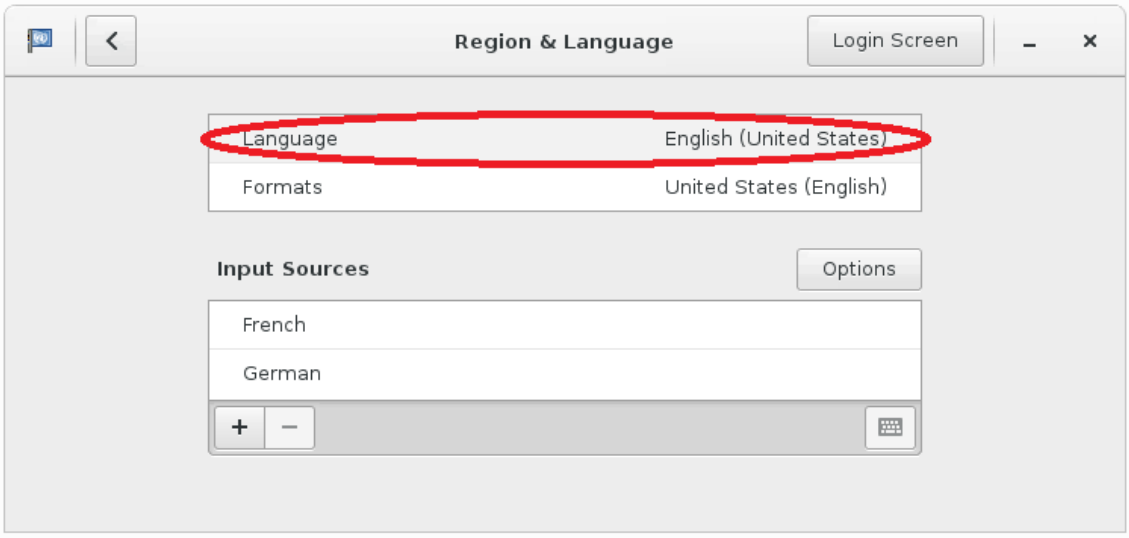
Die Verwendung ist einfach.

1. Aktivieren Sie das Feature.
2. Rufen Sie eine veröffentlichte Anwendung auf, die Texteingabe ermöglicht. Eine Sprachleiste wird in der Sitzung zusätzlich zur Anwendung angezeigt.
3. Wählen Sie im Dropdownmenü **Region und Sprache**, um die gewünschte Sprache (Eingabequelle) hinzuzufügen.



4. Wählen Sie den IME oder das Tastaturlayout aus dem Dropdownmenü.
5. Geben Sie Text mit dem ausgewählten IME- oder Tastaturlayout ein.

> **Hinweis:**
>
> - Wenn Sie ein Tastaturlayout in der VDA-seitigen Sprachleiste ändern, stellen Sie sicher, dass das gleiche Tastaturlayout auf dem Client (mit Citrix Workspace-App) verwendet wird.
> - Das Paket **accountsservice** muss auf Version 0.6.37 oder höher aktualisiert werden, damit Sie Einstellungen im Dialogfeld **Region und Sprache** vornehmen können.



Multimedia

January 8, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Audiofeatures
- Browserinhaltsumleitung
- HDX-Webcamvideokomprimierung

Audiofeatures

January 8, 2024

Adaptives Audio

Adaptives Audio ist standardmäßig aktiviert. Folgende Citrix Workspace-App-Clients werden unterstützt:

- Citrix Workspace-App für Windows –2109 und höher
- Citrix Workspace-App für Linux –2109 und höher
- Citrix Workspace-App für Mac –2109 und höher

Wenn Sie einen Client verwenden, der nicht auf der Liste steht, greift adaptives Audio auf Legacy-Audio zurück.

Bei adaptivem Audio müssen Sie die Audioqualitätsrichtlinien auf dem VDA nicht manuell konfigurieren. Adaptives Audio passt die Audio-Abtastrate dynamisch an die Netzwerkbedingungen an, um ein erstklassiges Audioerlebnis zu bieten.

Die folgende Tabelle vergleicht adaptives Audio mit Legacy-Audio:

Adaptives Audio	Legacy-Audio
Max. Audio-Abtastrate: 48 kHz	Max. Audio-Abtastrate: 8 kHz
Stereo-Kanal	Mono-Kanal

> **Tipp:**
>
> Verwenden Sie PulseAudio 13.99 oder höher unter RHEL 8.x und Rocky Linux 8.x.

Browserinhaltsumleitung

January 8, 2024

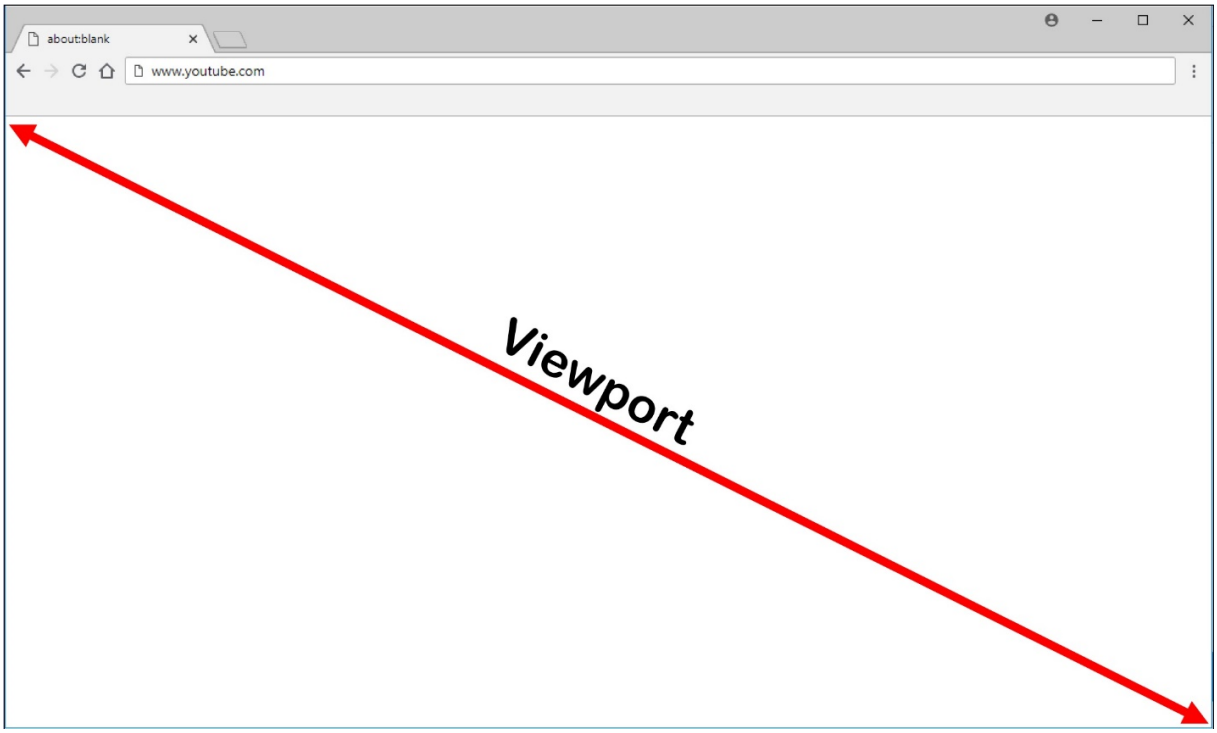
Übersicht

Die Browserinhaltsumleitung bietet die Möglichkeit der Wiedergabe von Webseiten in der Positivliste auf Clientseite. Dabei wird von der Citrix Workspace-App clientseitig die Instanz einer entsprechenden Renderingengine erzeugt, die den HTTP- und HTTPS-Inhalt von der URL abruft.

> **Hinweis:**
>
> Der Linux VDA unterstützt die Browserinhaltsumleitung in Google Chrome.

Diese Overlay-Weblayoutengine wird statt auf dem VDA auf dem Client ausgeführt und verwendet dessen CPU, GPU, Arbeitsspeicher und Netzwerk.

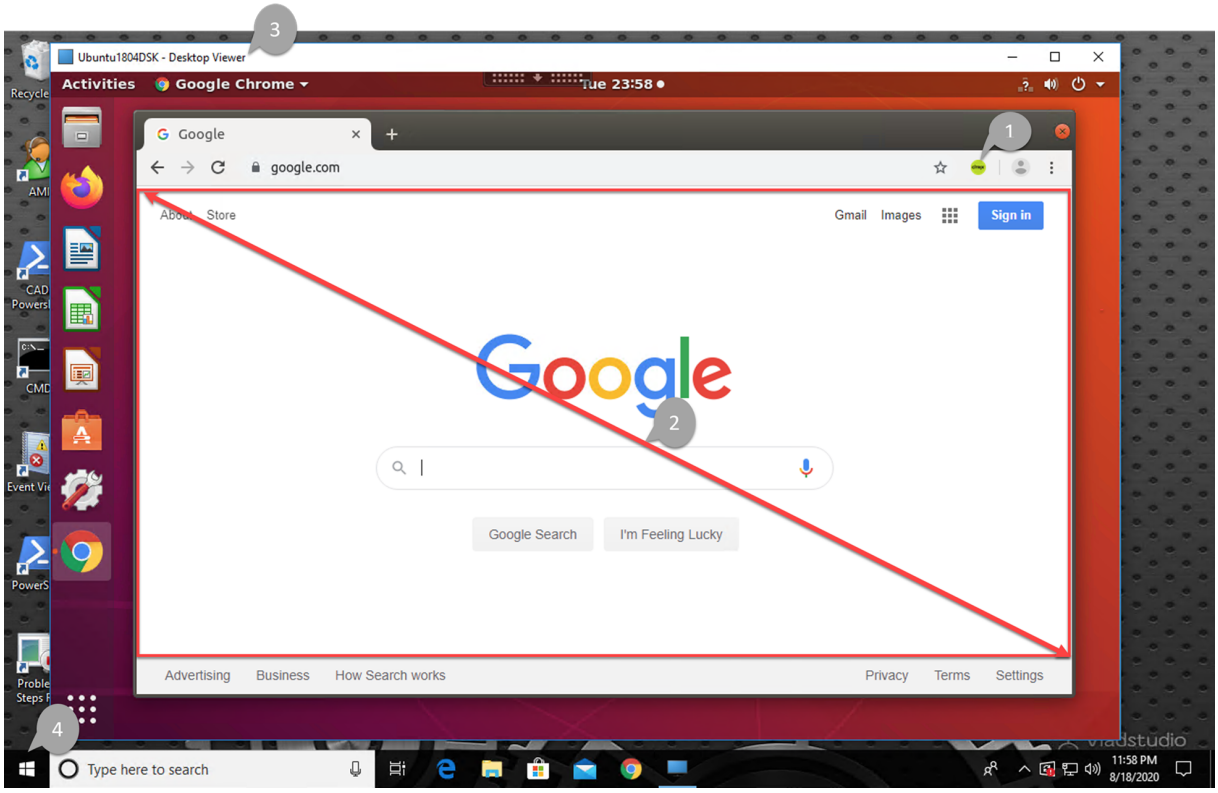
Es wird nur der Browserviewport umgeleitet. Der Viewport ist der rechteckige Browserbereich, in dem der Inhalt angezeigt wird. Der Viewport enthält keine Elemente wie Adressleiste, Favoritenleiste und Statusleiste. Diese Elemente werden weiterhin im Browser auf dem VDA ausgeführt.



Konfigurieren Sie eine Studio-Richtlinie mit einer Zugriffssteuerungsliste, die die Positivliste der URLs für die Umleitung enthält. Konfigurieren Sie eine Sperrliste, die die Umleitung für bestimmte URLs deaktiviert.

Wird eine Übereinstimmung mit einer URL in einer Positivliste gefunden, jedoch nicht in einer Sperrliste, weist ein virtueller Kanal (CTXCSB) die Citrix Workspace-App an, dass eine Umleitung erforderlich ist, und leitet die URL weiter. Die Citrix Workspace-App erzeugt dann eine lokale Renderingengine-Instanz und zeigt die Website an.

Anschließend fügt die Citrix Workspace-App die Website nahtlos in den Inhaltsbereich des virtuellen Desktopbrowsers ein.



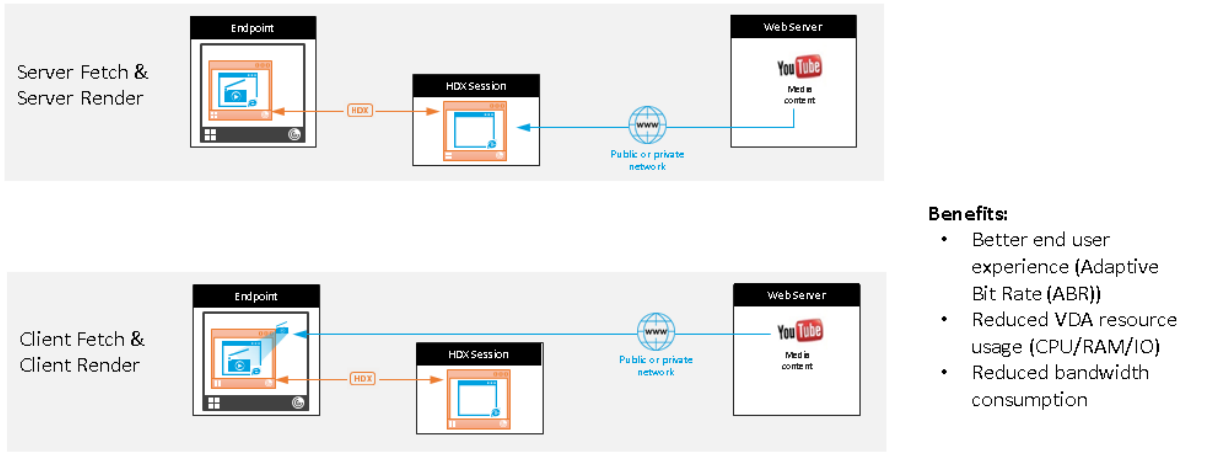
1. Symbol der Citrix-Browserinhaltsumleitungs-Erweiterung

   Die Farbe des Erweiterungssymbols gibt den Status der Chrome-Erweiterung an. Folgende drei Farben sind möglich:

   - Grün: Aktiv und verbunden
   - Grau: Nicht aktiv/Leerlauf auf der aktuellen Registerkarte
   - Rot: Defekt/außer Betrieb

2. Wiedergabe von Viewport auf dem Client oder nahtloses Einfügen in den virtuellen Desktop
3. Linux VDA
4. Windows-Client

Szenarien für den Inhaltsabruf durch die Citrix Workspace-App:



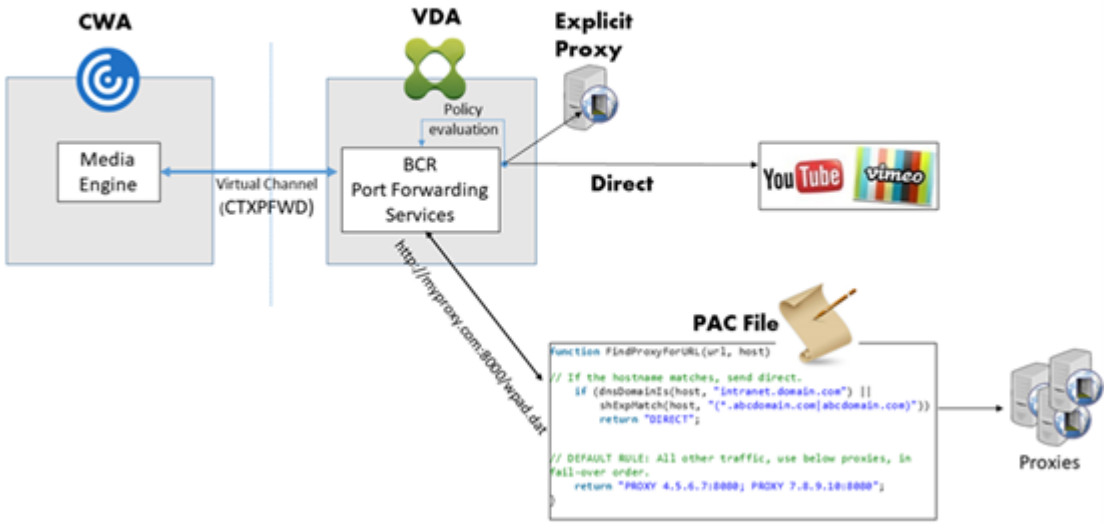
- **Abruf und Wiedergabe auf dem Server:** Es findet keine Umleitung statt, weil die Site nicht auf der Positivliste steht oder ein Fehler aufgetreten ist. Die Wiedergabe findet dann auf dem VDA statt und das Grafikremoting mithilfe von Thinwire. Verwenden Sie Richtlinien, um dieses Fallbackverhalten zu steuern. Dieses Szenario führt zu einem hohen CPU-, RAM- und Bandbreitenverbrauch auf dem VDA.
- **Abruf auf dem Server, Wiedergabe auf dem Client:** Die Citrix Workspace-App ruft den Inhalt über den VDA und einen virtuellen Kanal (CTXPFWD) vom Webserver ab. Diese Option ist nützlich, wenn Clients (z. B. Thin Clients) keinen Zugriff auf einen Webserver haben. Sie senkt den CPU- und RAM-Verbrauch auf dem VDA, verbraucht jedoch Bandbreite im virtuellen ICA-Kanal.

  Es gibt drei Betriebsmodi für dieses Szenario. CTXPFWD leitet Daten an ein Proxygerät weiter, über das der VDA Zugriff auf den Webserver erhält.

  Geeignete Richtlinienoption:

  - Expliziter Proxy - Wenn Sie einen einzelnen expliziten Proxy im Datencenter haben.
  - Direkt oder transparent: Wenn Sie keine Proxys haben oder transparente Proxys verwenden.
  - PAC-Dateien: Wenn Sie PAC-Dateien verwenden, sodass Browser auf dem VDA automatisch den geeigneten Proxyserver zum Abrufen einer angegebenen URL auswählen können.

  Weitere Informationen finden Sie weiter unten im Artikel unter der Einstellung **Proxykonfiguration für die Browserinhaltsumleitung**.



- **Abruf und Wiedergabe auf dem Client:** Da die Citrix Workspace-App direkt auf den Webserver zugreift, ist Internetzugang erforderlich. In diesem Szenario wird die gesamte Netzwerk-, CPU- und RAM-Last von der Citrix Virtual Apps and Desktops-Site abgeladen.

  Vorteile:

  - Bessere Endbenutzererfahrung (adaptive Bitrate (ABR))
  - Reduzierte VDA-Ressourcennutzung (CPU/RAM/IO)
  - Reduzierter Bandbreitenverbrauch

Systemanforderungen

Windows-Client:

- Citrix Workspace-App 1809 für Windows oder höher

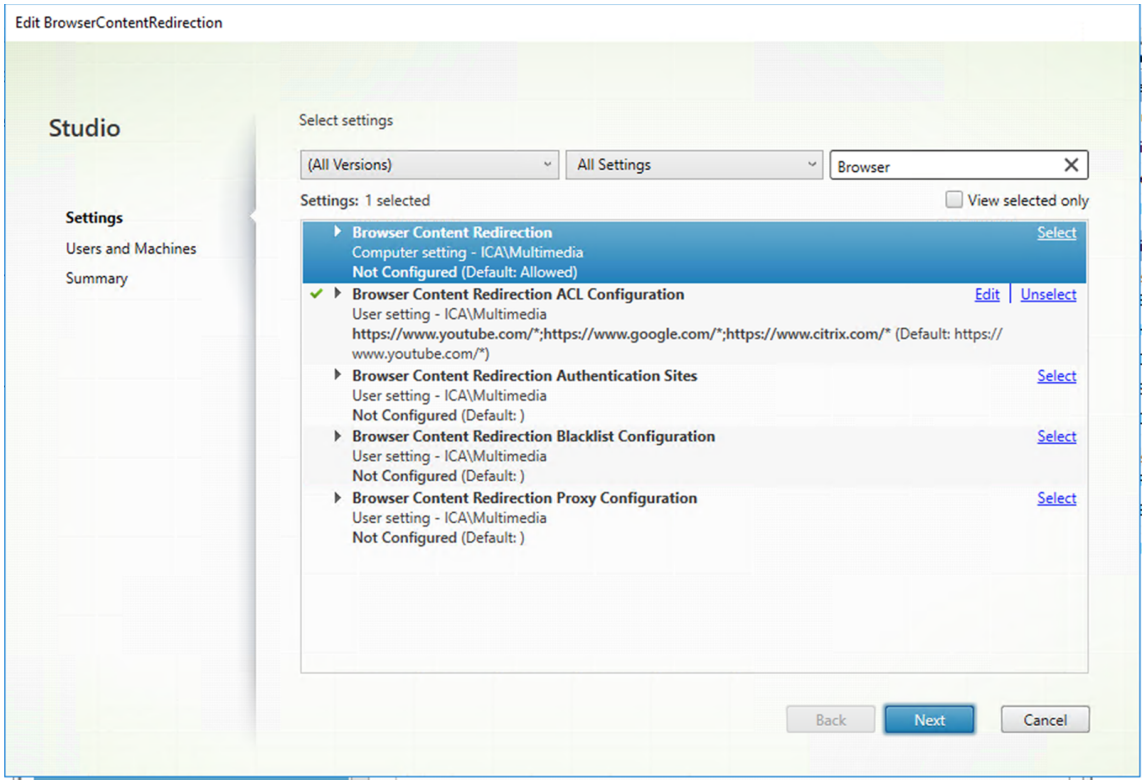
Linux VDA:

- Browser auf dem VDA: Google Chrome v66 oder höher mit der hinzugefügten Citrix-Browserinhaltsumleitungs-Erweiterung

Konfigurieren der Browserinhaltsumleitung

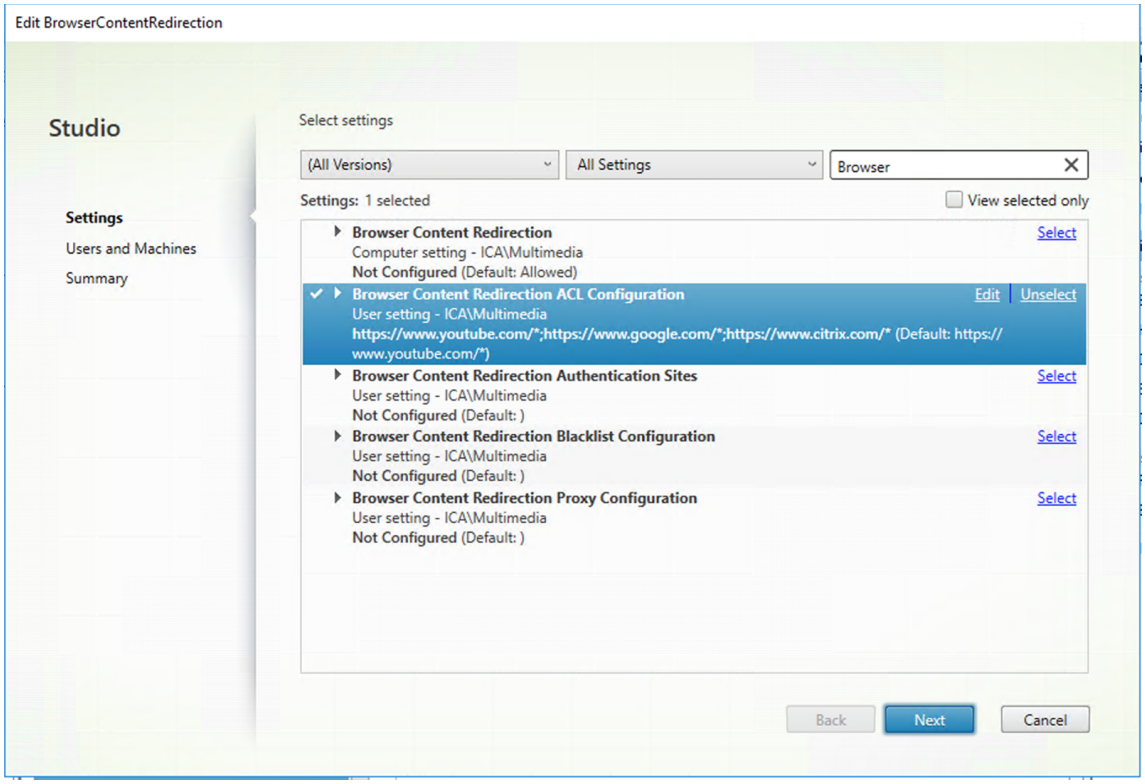
Um die Browserinhaltsumleitung zu verwenden, konfigurieren Sie die entsprechenden Richtlinien und installieren die Erweiterung für die Browserinhaltsumleitung in Google Chrome. Führen Sie hierzu die folgenden Schritte aus:

1. Um die Browserinhaltsumleitung zu aktivieren, setzen Sie in Citrix Studio **Browserinhaltsumleitung** auf **Zulässig**.



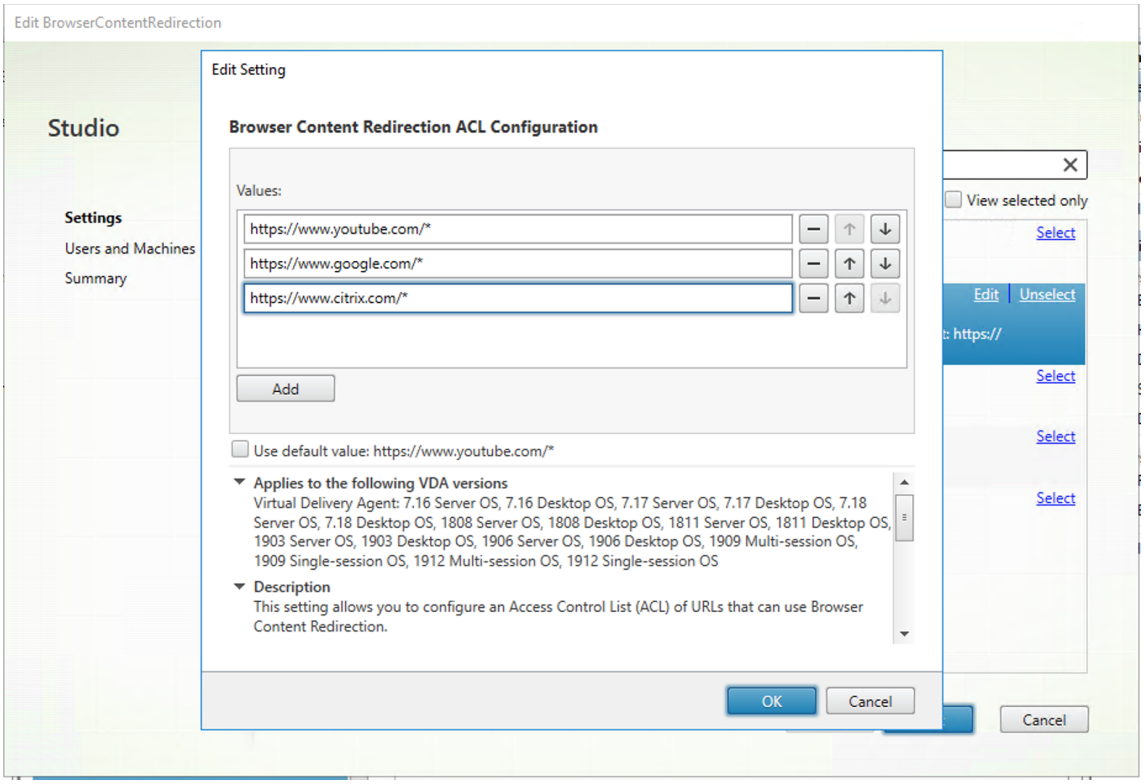
2. Geben Sie eine Positivliste mit URLs an, deren Inhalt an den Client umgeleitet werden kann, und eine Sperrliste, die die Umleitung für bestimmte URLs deaktiviert. Die Konfiguration einer Sperrliste ist optional.

   Die Einstellung **ACL-Konfiguration für die Browserinhaltsumleitung** legt eine Positivliste mit URLs fest, deren Inhalt an den Client umgeleitet werden kann. Bei der Angabe von URLs können Sie den Platzhalter * für alle URL-Komponenten mit Ausnahme des Protokolls verwenden.

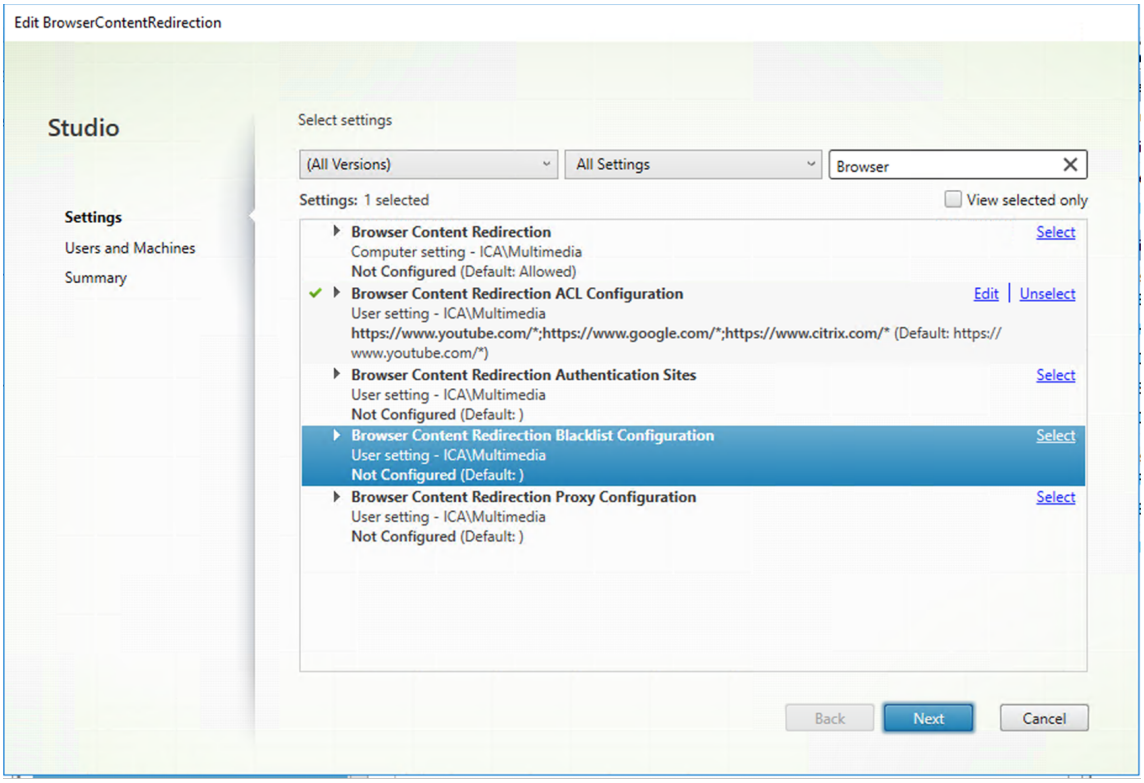


Die folgenden Beispiele sind zulässig:

- `http://www.xyz.com/index.html` (Sie können eine bessere Granularität erzielen, indem Sie Pfade in der URL angeben. Wenn Sie beispielsweise `https://www.xyz.com/sports/index.html` angeben, wird nur die Seite `index.html` umgeleitet.)
- `https://www.xyz.com/*`
- `http://www.xyz.com/*videos*`
- `http://*.xyz.com/`
- `http://*.*.com/`



Die Einstellung **Sperrlistenkonfiguration für die Browserinhaltsumleitung** gibt eine Sperrliste an, die die Umleitung für bestimmte URLs deaktiviert.



3. Um serverseitigen Abruf und clientseitige Wiedergabe zu aktivieren, konfigurieren Sie die Einstellung **Proxykonfiguration für die Browserinhaltsumleitung**.

   Diese Einstellung bietet Proxykonfigurationsoptionen auf dem VDA für die Browserinhaltsumleitung. Wenn mit einer gültigen Proxyadresse und Portnummer, PAC/WPAD-URL oder Direkt/Transparent-Einstellung aktiviert, versucht die Citrix Workspace-App stets zuerst den serverseitigen Abruf und die clientseitige Wiedergabe. Weitere Informationen finden Sie unter Fallbackmechanismus.

   Ist die Einstellung deaktiviert oder nicht konfiguriert und es wird ein Standardwert verwendet, versucht die Citrix Workspace-App den clientseitigen Abruf und die clientseitige Wiedergabe.

   Die Standardeinstellung ist **Nicht zugelassen**.

   Zulässiges Muster für einen expliziten Proxy:

   `http://\<hostname/ip address\>:\<port\>`

   Beispiel:

   `http://proxy.example.citrix.com:80 http://10.10.10.10:8080`

   Zulässige Muster für PAC/WPAD-Dateien:

   `http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

   Beispiel:`http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

   `https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

   Beispiel:`http://10.10.10.10/configuration/pac/wpad.dat`

   Zulässige Muster für direkte oder transparente Proxys:

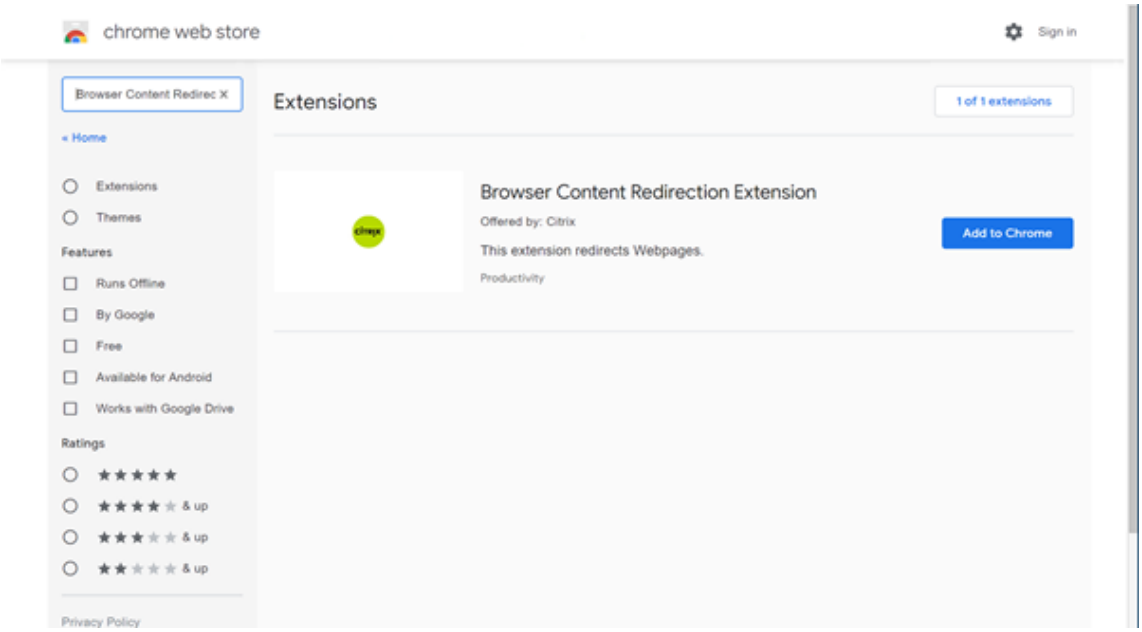
   Geben Sie im Richtlinientextfeld das Wort **DIRECT** ein.

   > **Hinweis:**
   >
   > Sie können auch einen Proxy einrichten, indem Sie den Registrierungswert `HKLM\Software\Citrix\HdxMediastream\WebBrowserRedirectionProxyAddress` bearbeiten. Außerdem können Sie mit dem Registrierungswert `HKLM\Software\Citrix\HdxMediastream\AllowNonTlsPacUri` festlegen, ob Sie das Herunterladen von PAC-Dateien über HTTP zulassen. Der Standardwert ist 0, was bedeutet, dass HTTP nicht erlaubt ist.
   >
   > Optional kann die Registrierung für Richtlinieneinstellungen außer Kraft gesetzt werden. Eine Liste der relevanten Registrierungsschlüssel finden Sie unter Außerkraftsetzung von Registrierungsschlüsseln für die Browserinhaltsumleitung.

4. Klicken Sie auf dem VDA auf **Zu Chrome hinzufügen**, um die Citrix-Erweiterung zur Browserinhaltsumleitung aus dem Chrome Web Store hinzuzufügen. Auf diese Weise kann der

Browser auf dem VDA erkennen, ob eine aufgerufene URL mit einer Positiv- oder Sperrliste übereinstimmt.

> **Wichtig:**
>
> Die Erweiterung ist auf dem Client nicht erforderlich. Fügen Sie sie nur auf dem VDA hinzu.
>
> Chrome-Erweiterungen werden pro Benutzer installiert. Das Update eines Gold-Masterimages zum Hinzufügen oder Entfernen einer Erweiterung ist nicht erforderlich.



Fallbackmechanismus

Wenn Sie die Richtlinie **Proxykonfiguration für die Browserinhaltsumleitung** aktivieren, versucht die Citrix Workspace-App den serverseitigen Abruf und die clientseitige Wiedergabe. Wenn der serverseitige Abruf und die clientseitige Wiedergabe fehlschlagen, wird auf den clientseitigen Abruf und die clientseitige Wiedergabe zurückgegriffen. Wenn die Clientmaschine keinen Zugriff auf den Webserver hat, kann der Browser auf dem VDA die Seite erneut laden und auf dem Server wiedergeben (serverseitiger Abruf und serverseitige Wiedergabe).

Außerkraftsetzung von Registrierungsschlüsseln für die Browserinhaltsumleitung

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des

> Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

`HKLM\Software\Citrix\HdxMediastream`

Name	Typ	Value
WebBrowserRedirection	DWORD	1 = zugelassen, 0 = nicht zugelassen
WebBrowserRedirectionAcl	REG_MULTI_SZ	/
WebBrowserRedirectionProxyAddress	REG_SZ	Wenn Sie einen der folgenden Modi festlegen, ist serverseitiger Abruf und clientseitige Wiedergabe aktiviert: **Expliziter Proxy**: Wenn Sie einen einzelnen expliziten Proxy im Datencenter haben. **Direkt oder transparent**: Wenn Sie keine Proxys haben oder transparente Proxys verwenden. **PAC-Dateien**: Wenn Sie PAC-Dateien verwenden, sodass Browser auf dem VDA automatisch den geeigneten Proxyserver zum Abrufen einer angegebenen URL auswählen können.
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	/

Name	Typ	Value
AllowNonTlsPacUri	DWORD	Legt fest, ob das Herunterladen von PAC-Dateien über HTTP zulässig ist. Der Standardwert ist 0, was bedeutet, dass HTTP nicht erlaubt ist. Wenn Sie den Wert auf 1 setzen, kann **HDXWebProxy.exe** PAC-Dateien über HTTP herunterladen (nicht nur über HTTPS).

HDX-Webcamvideokomprimierung

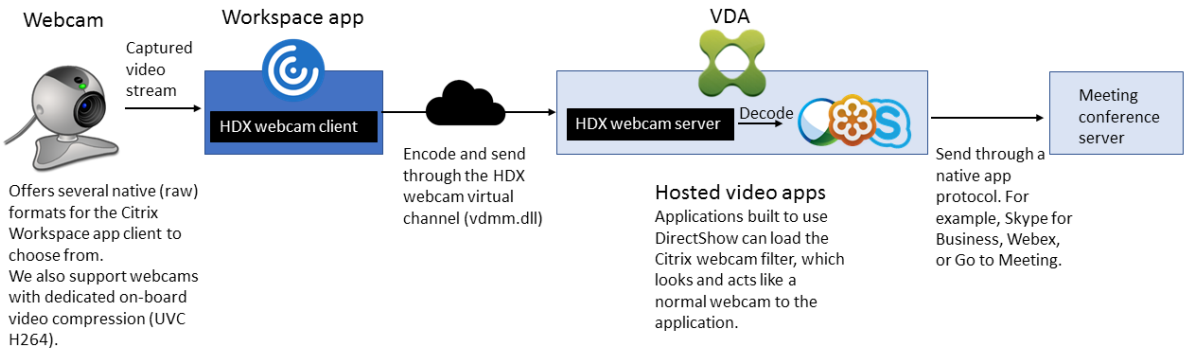
January 8, 2024

Übersicht

Benutzer von Videokonferenzanwendungen, die in Linux VDA-Sitzungen ausgeführt werden, können für ihre Webcams jetzt die HDX-Webcamvideokomprimierung verwenden. Das Feature ist in der Standardeinstellung aktiviert. Wir empfehlen, nach Möglichkeit die HDX-Webcamvideokomprimierung zu verwenden.

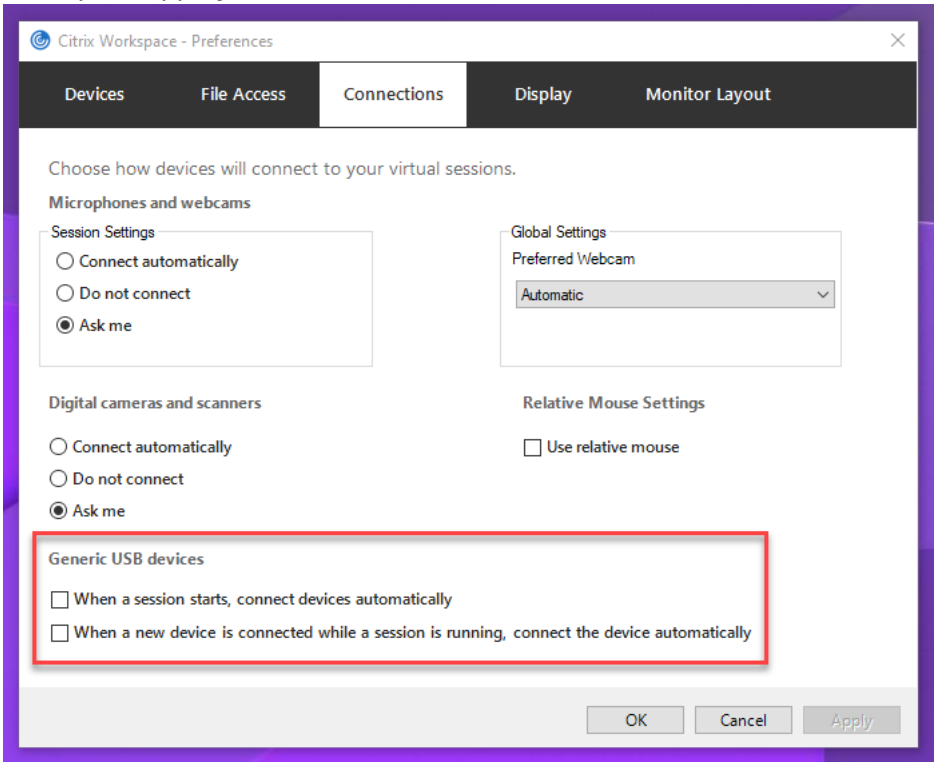
Die HDX-Webcamvideokomprimierung wird auch als **optimierter** Webcammodus bezeichnet. Bei dieser Art der Webcamvideokomprimierung wird das H.264-Video direkt an die Videokonferenzanwendung gesendet, die in der virtuellen Sitzung ausgeführt wird. Bei der HDX-Webcamvideokomprimierung wird die Multimediaframework-Technologie des Clientbetriebssystems verwendet, um Videos von Aufnahmegeräten zu erfassen, zu transcodieren und zu komprimieren. Hersteller von Aufnahmegeräten liefern die Treiber, die sich in die Betriebssystem-Kernelstreaming-Architektur einfügen.

Der Client übernimmt die Kommunikation mit der Webcam. Der Client sendet Videos nur an Server, die es ordnungsgemäß anzeigen können. Der Server ist nicht direkt mit der Webcam verbunden, seine Integration sorgt jedoch dafür, dass die gleiche Erfahrung auf dem Desktop geliefert wird. Die Workspace-App komprimiert Videos zum Einsparen von Bandbreite und zur Gewährleistung einer besseren Ausfallsicherheit in WANs.



Hinweis:

- Das Feature ist nicht für Azure-Maschinen verfügbar, da auf diesen das für das Feature benötigte **videodev**-Kernelmodul fehlt.
- Das Feature unterstützt nur H.264-Videos vom Citrix Workspace-App-Client.
- Es unterstützt eine Webcamauflösung von 48 x 32 bis 1920 x 1080.
- Wählen Sie bei Verwendung einer Webcam nicht **Generische USB-Geräte** auf der Citrix Workspace-App-Symbolleiste aus. Andernfalls können unerwartete Probleme auftreten.



Unterstützte Citrix Workspace-App

Die HDX-Webcam-Videokomprimierung unterstützt die folgenden Versionen der Citrix Workspace-App:

Plattform	Prozessor
Citrix Workspace-App für Windows	Die Citrix Workspace-App für Windows unterstützt die Webcam-Videokomprimierung für 32-Bit- und 64-Bit-Apps unter XenApp und XenDesktop 7.17 und höher. Unter früheren Versionen unterstützt die Citrix Workspace-App für Windows nur 32-Bit-Apps.
Citrix Workspace-App für Chrome	Da manche ARM-Chromebooks die H.264-Codierung nicht unterstützen, können nur 32-Bit-Apps die optimierte HDX-Webcam-Videokomprimierung verwenden.

Vollständig getestete Webcams

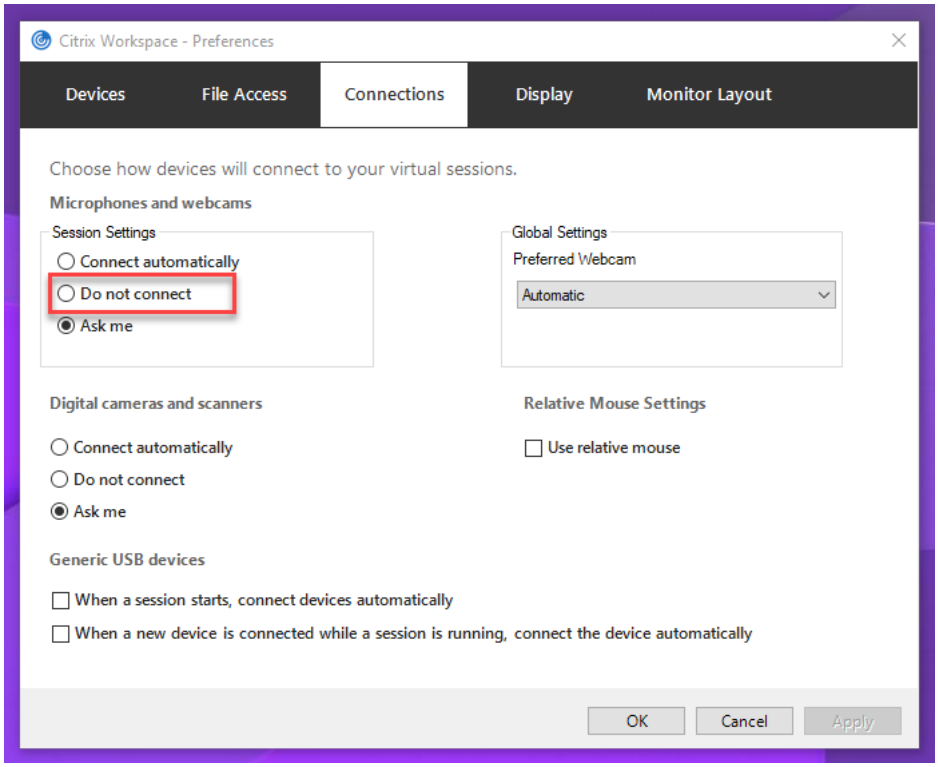
Die Bildfrequenz sowie Helligkeits- und Kontraststufen sind bei den einzelnen Webcams unterschiedlich. Citrix verwendet die folgenden Webcams für die Feature-Erstvalidierung:

- Logitech HD C270
- Logitech C930e
- Microsoft-LifeCam-HD3000

Konfiguration

Dieses Feature ist standardmäßig aktiviert. Zur Verwendung führen Sie die folgende Überprüfung und Konfiguration aus:

> **Tipp:**
>
> Benutzer der Citrix Workspace-App können die Standardeinstellung außer Kraft setzen, indem sie in Desktop Viewer unter **Mikrofon & Webcam** die Einstellung **Nicht verbinden** auswählen.



1. Stellen Sie nach Abschluss der VDA-Installation sicher, dass sich der VDA beim Delivery Controller registrieren kann und dass die veröffentlichten Linux-Desktopsitzungen mit der Windows-Anmeldeinformationen gestartet werden können.
2. Stellen Sie sicher, dass der VDA Internetzugang hat, und führen Sie dann den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um die Webcamkonfiguration abzuschließen. Wenn der VDA keinen Internetzugang hat, gehen Sie zu Schritt 3.

   > **Hinweis:**
   >
   > Es kann vorkommen, dass `uname -r` und Kernel-Header nicht übereinstimmen. Dies führt dazu, dass das Skript ctxwcamcfg.sh nicht ausgeführt werden kann. Zur ordnungsgemäßen Verwendung der HDX-Webcam-Videokomprimierung führen Sie zunächst **sudo apt-get dist-upgrade** aus, starten dann den VDA neu und führen anschließend das Skript ctxwcamcfg.sh erneut aus.

   Wenn Ihr VDA unter Debian bereitgestellt ist, stellen Sie sicher, dass er unter der neuesten Kernelversion ausgeführt wird. Führen Sie andernfalls die folgenden Befehle aus, um ein Update auf die neueste Kernelversion durchzuführen:

```
sudo apt-get update
sudo apt-get dist-upgrade
sudo reboot
<!--NeedCopy-->
```


Wenn Ihr VDA auf SUSE 15.3, SUSE 15.2 oder SUSE 12.5 bereitgestellt ist, führen Sie die folgenden Befehle aus, um den VDA auf die neueste Kernelversion zu aktualisieren und neu zu starten:

```
zypper up kernel-default
reboot
<!--NeedCopy-->
```

Das Skript ctxwcamcfg.sh hat folgende Funktionen:

a) Installation der Programme für `kernel-devel` und DKMS (Dynamic Kernel Module Support) auf dem VDA.

- `kernel-devel` wird verwendet, um ein Kernelmodul der virtuellen Webcam in der benötigten Version zu erstellen.
- DKMS wird zur dynamischen Verwaltung des Kernelmoduls der virtuellen Webcam verwendet.

> **Hinweis:**
>
> Bei Installation der o. g. Programme unter RHEL, Rocky Linux und CentOS installiert und aktiviert das Skript `ctxwcamcfg.sh` die folgenden Repositorys auf dem VDA:
>
> - Extra Pakete für Enterprise Linux (EPEL)
> - RPM Fusion

b) Laden Sie den Open-Source-Code `v4l2loopback` von https://github.com/umlaeute/v4l2loopback herunter und verwenden Sie DKMS zur Verwaltung von `v4l2loopback`. `v4l2loopback` ist ein Kernelmodul, mit dem Sie V4L2-Loopback-Geräte erstellen können.

c) Führen Sie den Befehl `sudo service ctxwcamsd restart` aus. Der Webcamdienst `ctxwcamsd` des Linux VDAs startet neu und lädt das `v4l2loopback`-Kernelmodul für die HDX-Webcamvideokomprimierung.

3. Wenn der VDA keinen Internetzugang hat, erstellen Sie das Kernelmodul v4l2loopback auf einer anderen Maschine und kopieren es dann auf den VDA.

a) Bereiten Sie eine Maschine mit Internetzugriff vor und verwenden Sie dieselbe Kernelversion wie beim VDA. Mit dem Befehl `uname -r` werden Kernelversionen gefunden.

b) Führen Sie auf der Maschine den Befehl `sudo mkdir -p /var/xdl` aus.

c) Kopieren Sie `/var/xdl/configure_*` vom VDA auf die Maschine unter `/var/xdl/`.

d) Führen Sie auf der Maschine den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um das Kernelmodul zu erstellen. Beim erfolgreichen Ausführen des Befehls wird unter dem Pfad `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd2/$(uname -r)/x86_64/module/` die Datei v4l2loopback.ko erstellt. Ignorieren Sie Fehler, die auftreten können, wenn Sie das Skript ctxwcamcfg.sh ausführen.

e) Kopieren Sie v4l2loopback.ko von der Maschine auf den VDA und speichern Sie die Datei unter `/opt/Citrix/VDA/lib64/`.

f) Führen Sie auf dem VDA den Befehl `sudo service ctxwcamsd restart` aus, um den Webcamdienst neu zu starten und das Kernelmodul v4l2loopback zu laden.

Nicht domänengebundene Linux VDAs

January 8, 2024

Übersicht

Nicht domänengebundene VDAs müssen nicht in Active Directory-Domänen eingebunden werden, um die VDA- und Benutzerauthentifizierung zu gewährleisten. Wenn Sie einen nicht domänengebundenen VDA erstellen, generieren Sie ein öffentlich-privates Schlüsselpaar, um den VDA bei der Cloud-Steuerungsebene zu registrieren. Daher ist der Beitritt zu einer Active Directory-Domäne nicht mehr erforderlich. Wenn ein Benutzer eine Sitzung von einem nicht domänengebundenen VDA aus startet, erstellt der VDA ein lokales Zuordnungskonto mit dem Benutzernamen, den der Benutzer für die Anmeldung an der Citrix Workspace-App verwendet. Der VDA weist ein zufälliges Kennwort zu, das das lokale Zuordnungskonto für SSO und das Wiederverbinden der Sitzung verwendet. Wenn Sie das zufällige Kennwort ändern, schlagen SSO und die Wiederverbindung der Sitzung fehl. Informationen zum Deaktivieren von SSO finden Sie unter Authentifizierung ohne Single Sign-On.

> **Wichtig:**
>
> - Nicht domänengebundene VDAs werden nur in Citrix DaaS unterstützt.
>   - Ihre Steuerungsebene muss über Citrix DaaS bereitgestellt werden.
>   - Sie können nicht domänengebundene VDAs in einer öffentlichen Cloud oder einem On-Premises-Datencenter bereitstellen. Die Steuerungsebene in Citrix DaaS verwaltet nicht domänengebundene VDAs.
>   - Sie können Rendezvous V2 so konfigurieren, dass Citrix Cloud Connectors umgangen werden. Andernfalls müssen Sie Cloud Connectors installieren, um VDAs mit Ihrer Steuerungsebene zu verbinden.
> - Um nicht domänengebundene VDAs zu erstellen, müssen Sie die Maschinenerstellungsdienste (MCS) verwenden.
>   - Die Maschinenerstellungsdienste (MCS) unterstützen keine Bare-Metal-Server.

Für nicht domänengebundene Linux VDAs verfügbare Features

Lokaler Benutzer mit angegebenen Attributen auf nicht domänengebundenen VDAs erstellen

Wenn Sie eine Sitzung öffnen, die auf einem nicht domänengebundenen VDA gehostet wird, erstellt der VDA automatisch einen lokalen Benutzer mit Standardattributen. Der VDA erstellt den lokalen Benutzer basierend auf dem Benutzernamen, mit dem Sie sich bei der Citrix Workspace-App angemeldet haben. Sie können auch Benutzerattribute angeben, darunter die **Benutzer-ID** (UID), die **Gruppen-ID** (GID), das **Homeverzeichnis** und die **Login-Shell** des Benutzers. Führen Sie die folgenden Schritte aus, um die Funktion zu nutzen:

1. Führen Sie folgenden Befehl aus, um das Feature zu aktivieren:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
     VirtualDesktopAgent\LocalMappedAccount" -t "REG_DWORD" -v "
     CreateWithUidGid" -d "0x00000001" --force
2 <!--NeedCopy-->
```

2. Geben Sie im Skript `/var/xdl/getuidgid.sh` unter dem Installationspfad des VDAs die folgenden Attribute an:

Attribut	Erforderlich oder optional	Beschreibung
`uid`	Erforderlich	Ein Benutzer-ID (UID) ist eine Nummer, die Linux jedem Benutzer im System zuweist. Sie bestimmt, auf welche Systemressourcen der Benutzer zugreifen kann.
`gid`	Erforderlich	Eine Gruppen-ID (GID) ist eine Zahl, die für eine bestimmte Gruppe steht.
`homedir`	Optional	Das Linux-Homeverzeichnis ist ein Verzeichnis für einen bestimmten Benutzer.
`shell`	Optional	Eine Login-Shell ist eine Shell, die einem Benutzer **bei der Anmeldung** bei seinem Benutzerkonto zugewiesen wird.

Im Folgenden finden Sie ein Beispiel für das Skript `getuidgid.sh`:

> **Hinweis:**
>
> Stellen Sie sicher, dass die im Skript angegebenen Attribute gültig sind.

```
#!/bin/bash

################################################################################

#
# Citrix Virtual Apps & Desktops For Linux Script: Get uid and gid
    for the user
#
# Copyright (c) Citrix Systems, Inc. All Rights Reserved.
#

export LC_ALL="en_US.UTF-8"

function get_uid_gid_for_user()
{

echo "uid:12345"
echo "gid:1003"
echo "homedir:/home/$1"
echo "shell:/bin/sh"
 }


get_uid_gid_for_user $1
<!--NeedCopy-->
```

Authentifizierung ohne Single Sign-On

Standardmäßig ist auf dem Linux VDA Single Sign-On (SSO) aktiviert. Die Benutzer melden sich bei der Citrix Workspace-App und bei VDA-Sitzungen mit einem Satz Anmeldeinformationen an.
Sollen sich Benutzer bei VDA-Sitzungen mit einem anderen Satz Anmeldeinformationen anmelden, deaktivieren Sie SSO auf dem Linux VDA. Weitere Informationen finden Sie unter Authentifizierung ohne Single Sign-On.

Authentifizierung mit Azure Active Directory

Die nicht domänengebundenen VDAs, die Sie in Azure bereitstellen, lassen sich in den AAD-Identitätsdienst integrieren, um die Benutzerauthentifizierung zu ermöglichen. Weitere Informationen finden Sie unter Authentifizierung mit Azure Active Directory.

Rendezvous V2

Nicht domänengebundene VDAs werden für das Umgehen der Citrix Cloud Connectors mit Rendezvous V2 unterstützt. Weitere Informationen finden Sie unter Rendezvous V2.

Nicht domänengebundene Linux VDAs erstellen

Verwenden Sie die Maschinenerstellungsdienste, um nicht domänengebundene Linux-VDAs in Citrix DaaS zu erstellen. Weitere Informationen finden Sie unter Nicht domänengebundene Linux VDAs erstellen.

Liste der unterstützten Richtlinien

January 8, 2024

Liste der für Linux VDA unterstützten Richtlinien

Studio-Richtlinie	Schlüsseltyp	Typname	Modul	Standardwert
Lokale Zeit des Clients verwenden	UseLocalTimeOfClient	ICA\Zeitzonenumleitung	ICA	Serverstandard verwenden
ICA-Roundtripberechnung	IcaRoundTripCheckEnabled	ICA\End User Monitoring	ICA	Benutzerüberwachung (1)
Intervall für ICA-Roundtripberechnung	IcaRoundTripCheckEnabled	ICA\End User Monitoring	ICA	15 Benutzerüberwachung

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
ICA-Roundtrip für Verbindungen im Leerlauf berechnen	IcaRoundTripCalcWhenIdle	Computer	ICA\Endbenutzererlebnisüberwachung	Deaktiviert (0)
Bandbreitenlimit für Sitzung insgesamt	TotalBandwidthLimit	Benutzer	ICA\Bandbreite	
Bandbreitenlimit für die Audioumleitung	AudioBandwidthLimit	Benutzer	ICA\Bandbreite	
Bandbreitenlimit für die Audioumleitung (Prozent)	AudioBandwidthLimitPercent	Benutzer	ICA\Bandbreite	
Bandbreitenlimit für Client-USB-Geräteumleitung	UsbBandwidthLimit	Benutzer	ICA\Bandbreite	

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Bandbreite für Client-USB-Geräteumleitung (Prozent)	TwRCGPercentLimit	DWord	ICA\Bandbreite	
Bandbreitenlimit für Dateiumleitung	TwRCGLimit	DWord	ICA\Bandbreite	
Bandbreitenlimit für Dateiumleitung (Prozent)	TwRCGPercentLimit	DWord	ICA\Bandbreite	
Bandbreitenlimit für Druckerumleitung	TwRPrinterLimit	DWord	ICA\Bandbreite	
Bandbreitenlimit für Druckerumleitung (Prozent)	TwRPrinterPercentLimit	DWord	ICA\Bandbreite	
WebSockets-Verbindungen	AcceptWebSocketsConnections	DWord	ICA\WebSockets	Nicht zugelassen
WebSockets-Portnummer	WebSocketsPort	DWord	ICA\WebSockets	8008
Vertrauenswürdige WebSockets-Ursprungsserverliste	WSTrustedOriginServerList	String	ICA\WebSockets	

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
ICA-Keep-Alives	SendICAKeepAlives	Computer	**ICA-Keep-Alive**	Keine ICA-Keep-Alive-Meldungen senden (0)
ICA-Keep-Alive-Timeout	ICAKeepAliveTimeout	Computer	**ICA-Keep-Alive**	60 Sekunden
ICA-Listenerportnummer	IcaListenerPortNumber	Computer	ICA	1494
Adaptiver HDX-Transport	HDXoverUDP	Computer	ICA	Bevorzugt (2)
Sitzungszuverlässigkeit-Verbindungen	AuthorizedSessionReliabilityConnections	Computer	ICA-Sitzungszuverlässigkeit	Zulässig (1)
UI-Transparenzstufe während Wiederverbindung	ReconnectUiTransparencyLevel	Computer	ICA-Client Reconnect	80 %
Sitzungszuverlässigkeit-Portnummer	SessionReliabilityPort	Computer	ICA-Sitzungszuverlässigkeit	2598
Sitzungszuverlässigkeit-Timeout	SessionReliabilityTimeout	Computer	ICA-Sitzungszuverlässigkeit	180 s

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Automatische Wiederverbindung von Clients	AllowAutoClientReconnect	CA\Auto Client Recon-nect	CA\Auto	Zugelassen (1)
Clientaudioumleitung	AllowAudioRedirection	Audio	Audio	Zugelassen (1)
Clientdruckerumleitung	AllowPrinterRedir	Drucken	Drucken	Zugelassen (1)
Universellen PDF-Drucker automatisch erstellen	AutoCreateUPDFPrinter	Drucken	Drucken	Deaktiviert (0)
Druckertreiberzuordnung und -kompatibilität	DriverMapping	Drucken	Drucken	"Microsoft XPS Document Writer *, Deny; Send to Microsoft OneNote *, Deny"
Clientzwischenablageumleitung	AllowClipboardRedirection	Zwischenablage	Zwischenablage	Zugelassen (1)

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Client-zu-Sitzung-Übertragungsgröße für Zwischenablage beschränken	LimitClipboardTransferC2H	DWORD	ICA	Deaktiviert (0)
Sitzung-zu-Client-Übertragungsgröße für Zwischenablage beschränken	LimitClipboardTransferH2C	DWORD	ICA	Deaktiviert (0)
Bandbreitenlimit für Zwischenablagenumleitung	ClipboardBW	DWORD	ICA\Bandbreite	
Bandbreitenlimit für Zwischenablagenumleitung (Prozent)	ClipboardBWPercent	DWORD	ICA\Bandbreite	

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Schreiben in Clientzwischenablage einschränken	RestrictClientClipboardWrite	User	ZwischenablageVirtualisierung	Deaktiviert (0)
Zum Schreiben in Clientzwischenablage zugelassene Formate	ClientClipboardWriteAllowedFormats	User	ZwischenablageVirtualisierung	Leer
Schreiben in Sitzungszwischenablage einschränken	RestrictSessionClipboardWrite	User	ZwischenablageVirtualisierung	Deaktiviert (0)
Zum Schreiben in Sitzungszwischenablage zugelassene Formate	SessionClipboardWriteAllowedFormats	User	ZwischenablageVirtualisierung	Leer

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Client-USB-Geräteumleitung	AllowUSBRedir	User	USB	Nicht zugelassen (0)
Regeln für die Client-USB-Geräteumleitung	USBDeviceRules	User	USB	”
Bewegtbildkomprimierung	VisualQuality	User	Thinwire	Deaktiviert (1)
Zusätzliche Farbkomprimierung	UseExtraColorCompression	User	Thinwire	Deaktiviert (0)
Mindestframerate	MinimumFramesPerSecond	User	Thinwire	10 f/s
Framerate	TargetFramesPerSecond	User	Thinwire	30 f/s
Bildqualität	VisualQuality	User	Thinwire	Mittel (3)
Videocodec zur Komprimierung verwenden	VideoCodec	User	Thinwire	Bevorzugt verwenden (3)
Hardwarecodierung für Videocodec verwenden	HardwareEncoding	User	ThinwireVideo	Aktiviert (1)

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Regeln für die Client-USB-Geräteumleitung	USBDeviceRules	User	USB	“\0”

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Visuell verlustfreie Komprimierung zulassen	AllowVisuallyLosslessCompression	User	ThinWire	Deaktiviert (0)
Optimierung für 3D-Grafikworkload	OptimizeFor3DWorkload	User	ThinWire	Deaktiviert (0)
Bevorzugte Farbtiefe für einfache Grafiken	PreferredColorDepth	User	ThinWire	24 Bit pro Pixel (1)
Audioqualität	AudioQuality	User	Audio	Hoch - High Definition Audio (2)
Clientmikrofonumleitung	MicrophoneRedirection	User	Audio	Zugelassen (1)
Sitzungshöchstanzahl	MaximumNumberOfSessions	Computer	Server	250

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Toleranzwert für gleichzeitige Anmeldungen	ConcurrentLogonTolerance	Computer	Lastverwaltung	2
Automatische Controllerupdates aktivieren	EnableAutoUpdateOfControllers	Computer	Virtual Delivery Agent	Zugelassen (1)
Aktualisierungsmodus für die Zwischenablageauswahl	ClipboardSelectionUpdateMode	Sitzung	Zwischenablage	
Aktualisierungsmodus für die Primärauswahl	PrimarySelectionUpdateMode	Sitzung	Zwischenablage	
Max. Speex-Qualität	MaxSpeexQuality	Computer	Audio	5
Clientlaufwerke automatisch verbinden	AutoConnectDrives	Benutzer	Dateiumleitung\CDM	Aktiviert (1)

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Optische Client-laufwerke	AllowCdromDrives	UserDrives	Dateiumleitung\CDM	Zugelassen (1)
Lokale Client-festplatten-laufwerke	AllowFixedDrives	UserDrives	Dateiumleitung\CDM	Zugelassen (1)
Clientdiskettenlaufwerke	AllowFloppyDrives	UserDrives	Dateiumleitung\CDM	Zugelassen (1)
Clientnetzlaufwerke	AllowNetworkDrives	UserDrives	Dateiumleitung\CDM	Zugelassen (1)
Clientlaufwerkumleitung	AllowRemotePlugAndPlay	UserDrives	Dateiumleitung\CDM	Zugelassen (1)
Schreibgeschützter Zugriff auf Client-laufwerke	ReadOnlyMappedDrive	UserDrives	Dateiumleitung\CDM	Deaktiviert (0)
Automatische Anzeige der Tastatur	AllowAutoKeyboardPopup	UserDevicesManagement	VDA	Deaktiviert (0)

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Dateiübertragung zwischen Desktop und Client zulassen	AllowFileTransfer	Boolean	Dateiübertragung	Zugelassen
Dateien von Desktop herunterladen	AllowFileDownload	Boolean	Dateiübertragung	Zugelassen
Dateien auf Desktop hochladen	AllowFileUpload	Boolean	Dateiübertragung	Zugelassen
Sitzungsverbindung trennen	EnableSessionIdleTimer	Boolean	Session Timers	Aktiviert (1)
Sitzungsverbindung trennen - Timerintervall	SessionIdleTimerInterval	Integer	Session Timers	1440 Minuten
Timer für getrennte Sitzung	EnableSessionDisconnectTimer	Boolean	Session Timers	Deaktiviert (0)

Studio-Richtlinie	Schlüsselname	Typ	Modul	Standardwert
Getrennte Sitzungen - Timerintervall	SessionDisconnectTimerInterval	User	TimeoutTimers	1440 Minuten
Browserinhaltsumleitung	WebBrowserRedirection	UserOrComputer	ICA\Multimedia	Zulässig
ACL-Konfiguration für die Browserinhaltsumleitung	WebBrowserRedirectionAclConfiguration	UserOrComputer	ICA\Multimedia	`https://www.youtube.com/*`
Sperrlistenkonfiguration für die Browserinhaltsumleitung	WebBrowserRedirectionBlocklistConfiguration	UserOrComputer	ICA\Multimedia	
Proxykonfiguration für die Browserinhaltsumleitung	WebBrowserRedirectionProxyConfiguration	UserOrComputer	ICA\Multimedia	

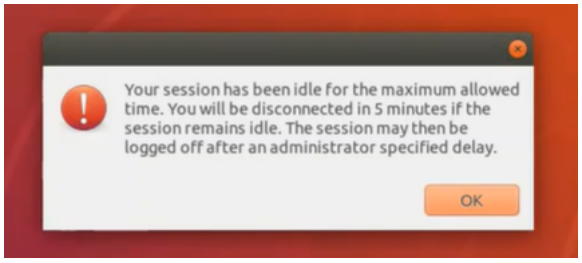
> **Hinweis:**
>
> Nur der Windows Virtual Delivery Agent (VDA) unterstützt Audio über UDP (User Datagram Protocol). Der Linux VDA unterstützt dies nicht. Weitere Informationen finden Sie unter Audio über User Datagram Protocol (UDP) –Echtzeitübertragung.

Sie können mit den folgenden Citrix Richtlinieneinstellungen Sitzungsverbindungstimer in Citrix Studio konfigurieren:

- **Sitzungsleerlauftimer**: Bestimmt, ob ein Zeitlimit für Sitzungen im Leerlauf erzwungen werden soll.
- **Sitzungsleerlauf - Timerintervall**: Legt ein Zeitlimit für Sitzungen im Leerlauf fest. Wenn der **Sitzungsleerlauftimer Aktiviert** ist und in einer aktiven Sitzung während der festgelegten Zeit keine Benutzereingabe erfolgt, wird die Sitzung getrennt.
- **Timer für getrennte Sitzung**: Bestimmt, ob ein Zeitlimit für getrennte Sitzungen erzwungen werden soll.
- **Getrennte Sitzungen - Timerintervall**: Legt ein Intervall fest, bevor eine getrennte Sitzung abgemeldet wird.

Wenn Sie eine der Richtlinieneinstellungen aktualisieren, achten Sie darauf, dass sie in der ganzen Bereitstellung konsistent sind.

A warning message appears when your time limit for idle sessions expires. Ein Beispiel sehen Sie im folgenden Screenshot. Pressing **OK** closes the warning message but cannot keep your session active. To keep your session active, provide user input to reset the idle timer.



Die folgenden Richtlinien können in Citrix Studio Version 7.12 und höher konfiguriert werden.

- MaxSpeexQuality

  Wert (Ganzzahl): [0–10]

  Standardwert: 5

  Details:

  Die Audioumleitung codiert Audiodaten mit dem Speex-Codec, wenn die Audioqualität mittelmäßig oder niedrig ist (siehe Richtlinie "Audioqualität"). Speex ist ein verlustbehafteter Codec, d. h. die Komprimierung geht auf Kosten der Genauigkeit des Eingabesprachsignals.

Im Gegensatz zu anderen Sprachencodecs kann das Verhältnis zwischen Qualität und Bitrate gesteuert werden. Der Speex-Codierungsprozess wird meist über einen Qualitätsparameter mit einem Wertebereich von 0 bis 10 gesteuert. Je höher die Qualität, desto höher ist die Bitrate.

Die maximale Speex-Qualität wählt die beste Speex-Qualität für die Audiodatencodierung gemäß Audioqualität und Bandbreitenlimit (siehe Richtlinie "Bandbreitenlimit für die Audioumleitung"). Bei mittlerer Audioqualität erfolgt die Codierung im Breitbandmodus mit einer höheren Samplingrate. Bei niedriger Audioqualität erfolgt die Codierung im Schmalbandmodus mit einer niedrigeren Samplingrate. Bei gleicher Speex-Qualität ist die Bitrate in verschiedenen Modi unterschiedlich. Die beste Speex-Qualität wird erreicht, wenn für den höchsten Wert folgende Bedingungen zutreffen:

- Es ist kleiner oder gleich der maximalen Speex-Qualität.
- Die Bitrate ist kleiner oder gleich dem Bandbreitenlimit.

Verwandte Einstellungen: Audioqualität, Bandbreitenlimit für die Audioumleitung

- PrimarySelectionUpdateMode

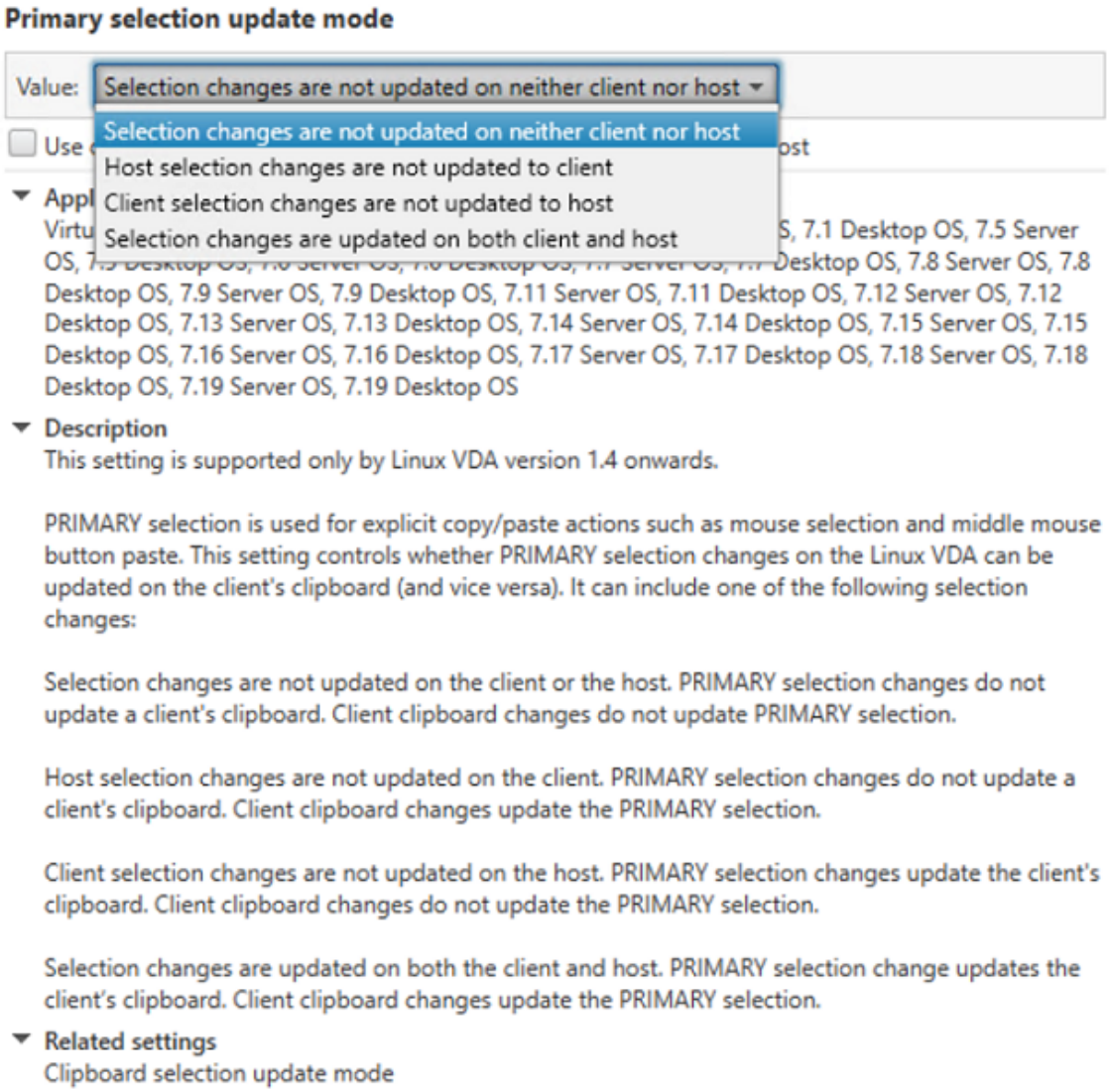
  Wert (Aufzählung): [0, 1, 2, 3]

  Standardwert: 3

  Details:

  Mit der Primärauswahl können Sie ausgewählte Daten durch Drücken der mittleren Maustaste einfügen.

  Diese Richtlinie steuert, ob bei einer Änderung der Primärauswahl auf dem Linux VDA bzw. Client die Zwischenablage des jeweils anderen aktualisiert werden kann. Es gibt vier mögliche Werte:



- **Auswahländerungen werden weder auf Client noch auf Host aktualisiert**
  Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.
- **Auswahländerungen auf dem Host werden nicht auf dem Client aktualisiert**
  Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert.
- **Auswahländerungen auf dem Client werden nicht auf dem Host aktualisiert**
  Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.

- **Auswahländerungen werden auf Client und Host aktualisiert**
  Bei Änderungen der Primärauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Primärauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert. Diese Option ist der Standardwert.

Verwandte Einstellung: Aktualisierungsmodus für die Zwischenablageauswahl

- ClipboardSelectionUpdateMode

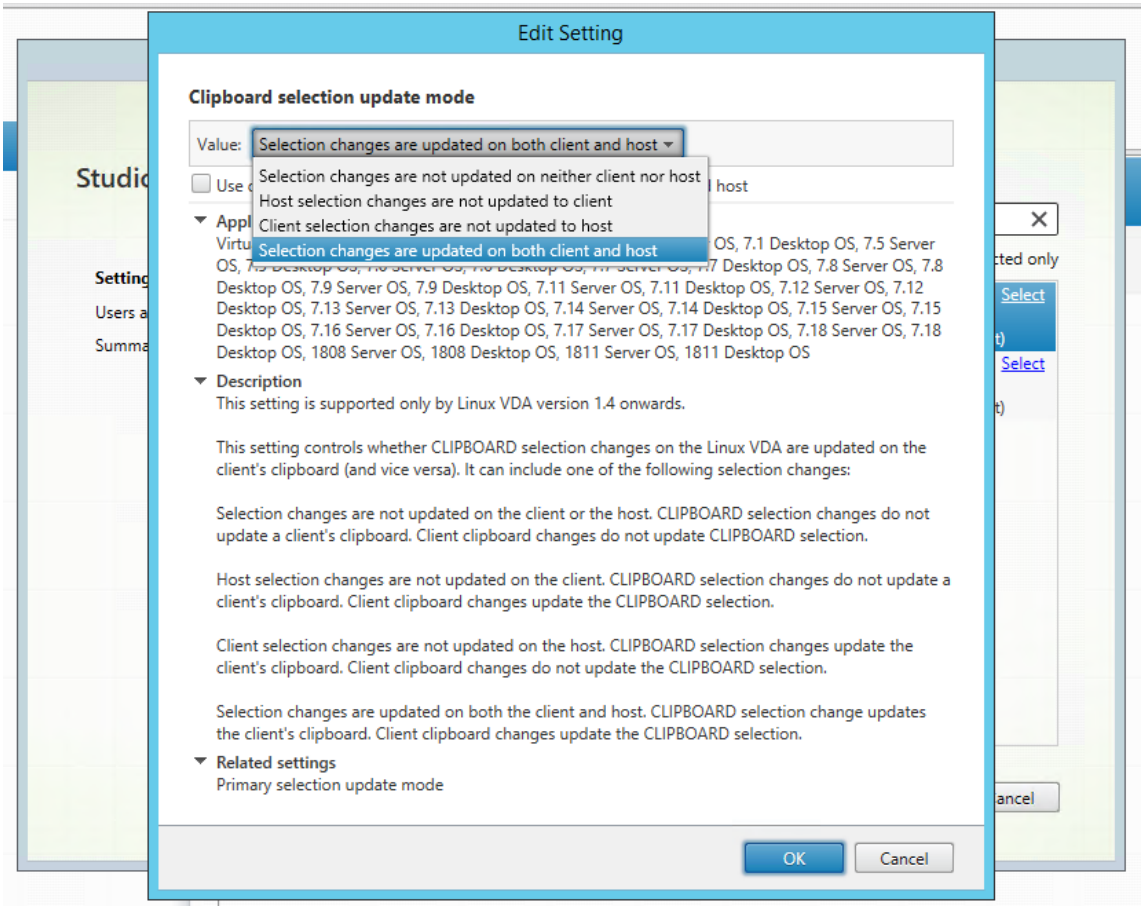
  Wert (Aufzählung): [0, 1, 2, 3]

  Standardwert: 3

  Details:

  Die Zwischenablageauswahl wird verwendet, um ausgewählte Daten explizit in die Zwischenablage zu kopieren (z. B. durch Auswahl von "Kopieren"aus dem Kontextmenü). Die Zwischenablageauswahl wird vor allem mit der Zwischenablage in Microsoft Windows verwendet, während die Primärauswahl nur in Linux genutzt werden kann.

  Diese Richtlinie steuert, ob bei Zwischenablageänderungen auf dem Linux VDA bzw. Client die Zwischenablage des jeweils anderen aktualisiert werden kann. Es gibt vier mögliche Werte:



- **Auswahländerungen werden weder auf Client noch auf Host aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.
- **Auswahländerungen auf dem Host werden nicht auf dem Client aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client nicht aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert.
- **Auswahländerungen auf dem Client werden nicht auf dem Host aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA nicht aktualisiert.
- **Auswahländerungen werden auf Client und Host aktualisiert**
  Bei Änderungen der Zwischenablageauswahl auf dem Linux VDA wird die Zwischenablage auf dem Client aktualisiert. Bei Änderungen der Zwischenablageauswahl auf dem Client wird die Zwischenablage auf dem Linux VDA aktualisiert. Diese Option ist der Standardwert.

Verwandte Einstellung: Aktualisierungsmodus für die Primärauswahl

> **Hinweis:**
>
> Der Linux VDA unterstützt die Zwischenablageauswahl und die Primärauswahl. Um das Kopier- und Einfügeverhalten zwischen Linux VDA und Client zu steuern, empfehlen wir, dass Sie den Aktualisierungsmodus für Zwischenablage- und Primärauswahl auf denselben Wert festzulegen.

Drucken

January 8, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Bewährte Methoden beim Drucken
- PDF-Druck

Bewährte Methoden beim Drucken

January 8, 2024

Dieser Artikel enthält Informationen zu bewährten Druckmethoden.

Installation

Der Linux VDA benötigt die Filter **cups** und **foomatic**. Die Filter werden im Rahmen der VDA-Installation installiert. Sie können die Filter gemäß Ihrer Distribution auch manuell installieren. Beispiel:

Auf RHEL 7:

```
sudo yum –y install cups

sudo yum -y install foomatic-filters
<!--NeedCopy-->
```

Drucken - Richtlinieneinstellungen

Clientdruckerumleitung

Mit dieser Einstellung legen Sie fest, ob Clientdrucker einer VDA-Sitzung zugeordnet werden. Standardmäßig ist die Clientdruckerzuordnung zugelassen.

Clientdrucker automatisch erstellen

Mit dieser Einstellung wird angegeben, welche Clientdrucker den VDA-Sitzungen zugeordnet werden können. Die Standardeinstellung ist **Alle Clientdrucker automatisch erstellen**. Dies bedeutet, dass alle Clientdrucker den VDA-Sitzungen zugeordnet werden. Weitere Informationen zu dieser Einstellung finden Sie unter Clientdrucker automatisch erstellen in der Dokumentation zu Citrix Virtual Apps and Desktops.

Universellen PDF-Drucker automatisch erstellen

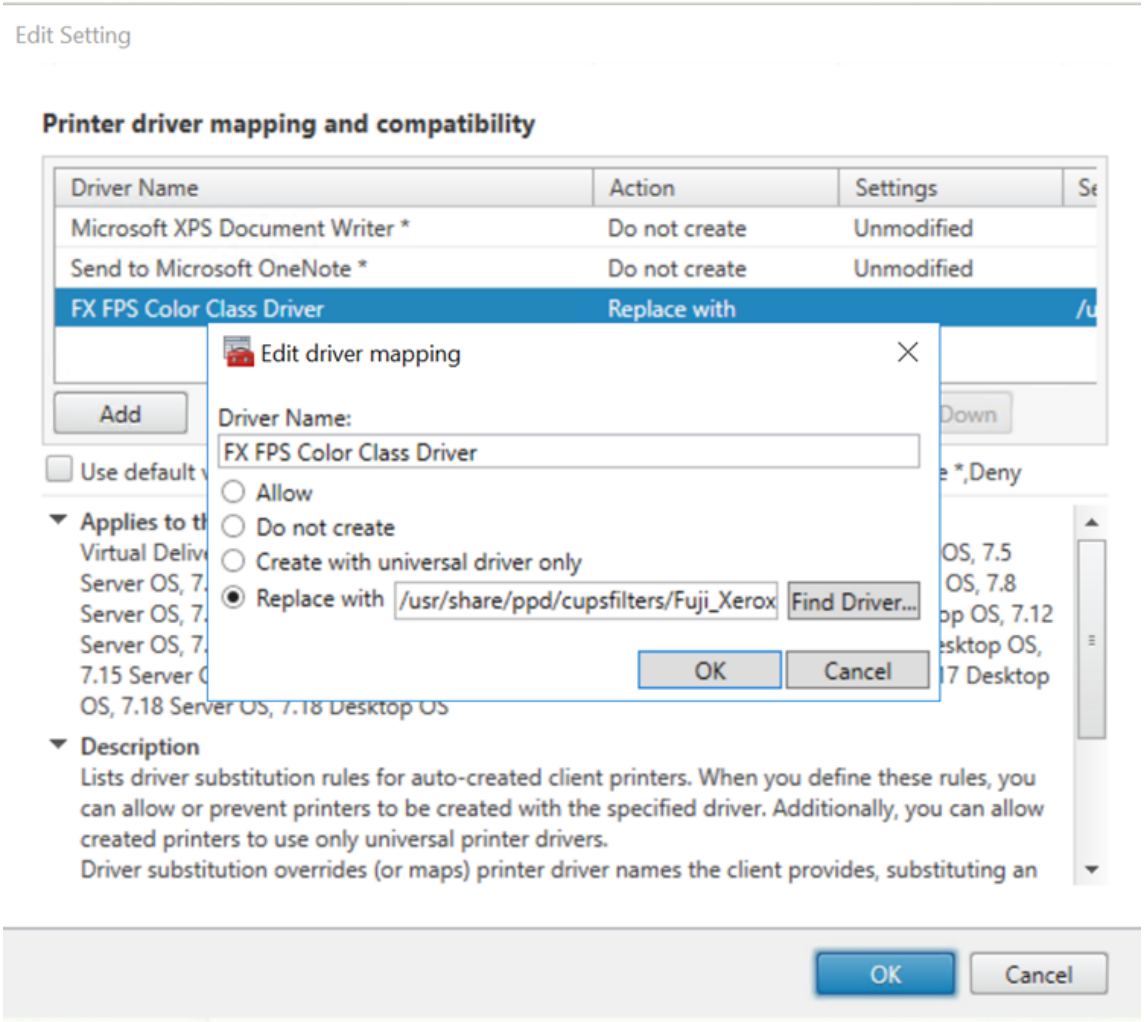
Um die PDF-Druckfunktion zu verwenden, setzen Sie diese Richtlinie auf **Aktiviert**.

Druckertreiberzuordnung und -kompatibilität

Citrix bietet drei universelle Druckertreibertypen: postscript, pcl5 und pcl6. Der universelle Druckertreiber ist unter Umständen nicht mit dem Clientdrucker kompatibel. In diesem Fall bestand in früheren Versionen die einzige Option darin, die Konfigurationsdatei ~/.CtxlpProfile$CLIENT_NAME zu bearbeiten. Ab Version 1906 können Sie stattdessen auch die Richtlinie **Druckertreiberzuordnung und -kompatibilität** in Citrix Studio konfigurieren.

Konfigurieren der Richtlinie **Druckertreiberzuordnung und -kompatibilität** in Citrix Studio:

1. Wählen Sie die Richtlinie **Druckertreiberzuordnung und -kompatibilität** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie unter **Treibername** den Treibernamen des Clientdruckers ein. Bei Verwendung der Citrix Workspace-App für Linux geben Sie stattdessen den Druckernamen ein.
4. Wählen Sie **Ersetzen durch** und geben Sie den absoluten Pfad der Treiberdatei auf dem VDA ein.



> **Hinweis:**
>
> - Es werden nur PPD-Treiberdateien unterstützt.
> - Andere Optionen der Richtlinie **Druckertreiberzuordnung und -kompatibilität** werden nicht unterstützt. Es wird nur **Ersetzen durch** wirksam.

Verwendung

Sie können aus veröffentlichten Desktops und veröffentlichten Anwendungen drucken. Alle Clientdrucker können einer VDA-Sitzung zugeordnet werden Die Druckernamen müssen für Desktops und Anwendungen unterschiedlich sein.

- Veröffentlichte Desktops:
  `<client printer name>:$CLIENT_NAME:dsk$SESSION_ID`
- Veröffentlichte Anwendungen
  `<client printer name>:$CLIENT_NAME:app$SESSION_ID`

> **Hinweis:**
>
> Wenn ein Benutzer einen veröffentlichten Desktop und eine veröffentlichte Anwendung öffnet, stehen in der Sitzung beide Drucker zur Verfügung. Das Drucken auf einem Desktopdrucker in einer veröffentlichten Anwendung oder auf einem Anwendungsdrucker über einen veröffentlichten Desktop schlägt fehl.

Problembehandlung

Fehler beim Drucken

Wenn das Drucken nicht ordnungsgemäß funktioniert, sollten Sie den Druckdaemon **ctxlpmngt** und das **CUPs-Framework** überprüfen.

Der Druckdaemon **ctxlpmngt** ist ein pro Sitzung ausgeführter Vorgang, der für die gesamte Sitzungsdauer ausgeführt werden muss. Mit dem folgenden Befehl prüfen Sie, ob der Druckdaemon ausgeführt wird. Wenn der Prozess **ctxlpmngt** nicht ausgeführt wird, starten Sie **ctxlpmngt** manuell über eine Befehlszeile.

```
1 ps –ef | grep ctxlpmngt
2 <!--NeedCopy-->
```

Wenn der Druck immer noch nicht funktioniert, überprüfen Sie das **CUPS**-Framework. Der Dienst **ctxcups** dient zur Druckerverwaltung und kommuniziert mit dem Linux CUPS-Framework. Es gibt jeweils einen Prozess pro Maschine, der mit folgendem Befehl überprüft werden kann:


```
service ctxcups status
<!--NeedCopy-->
```

Zusätzliche Schritte zum Sammeln von CUPS-Protokollen

Führen Sie die folgenden Befehle aus, um die CUPS-Dienstdatei für das Sammeln von CUPS-Protokollen zu konfigurieren. Andernfalls können CUPS-Protokolle nicht in **hdx.log**aufgezeichnet werden:

```
sudo service cups stop

sudo vi /etc/systemd/system/printer.target.wants/cups.service

PrivateTmp=false

sudo service cups start

sudo systemctl daemon-reload
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das vollständige Druckprotokoll sollte mit dieser Konfiguration nur bei einem Problem abgerufen werden. Normalerweise wird diese Konfiguration nicht empfohlen, da sie die CUPS-Sicherheit verletzt.

Druckausgabe ist verzerrt

Eine fehlerhafte Ausgabe kann durch einen nicht kompatiblen Druckertreiber verursacht werden. Pro Benutzer ist eine Treiberkonfiguration verfügbar und kann durch das Bearbeiten der Konfigurationsdatei **~/.CtxlpProfile$CLIENT_NAME** konfiguriert werden:

```
[DEFAULT_PRINTER]

printername=

model=

ppdpath=

drivertype=
<!--NeedCopy-->
```

> **Wichtig:**
>
> Das Feld **printername** enthält den Namen des aktuellen Clientstandarddruckers. Dieser Wert ist

> schreibgeschützt. Bearbeiten Sie ihn nicht.
>
> Nehmen Sie nicht gleichzeitig Eingaben in den Feldern **ppdpath**, **model** und **drivertype** vor, da nur eines für den **zugeordneten Drucker** wirksam ist.

- Wenn der universelle Druckertreiber mit dem Clientdrucker nicht kompatibel ist, konfigurieren Sie das Modell des nativen Druckertreibers mit der Option **model=**. Sie finden den aktuellen Modellnamen des Druckers mit dem Befehl **lpinfo**:

```
lpinfo –m

...

xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

<!--NeedCopy-->
```

  Sie können dann das Modell gemäß dem Drucker festlegen:

```
model=xerox/ph3115.ppd.gz
<!--NeedCopy-->
```

- Wenn der universelle Druckertreiber nicht mit dem Clientdrucker kompatibel ist, konfigurieren Sie den PPD-Dateipfad für den nativen Druckertreiber. Der Wert von **ppdpath** ist der absolute Pfad der nativen Druckertreiberdatei.

  Beispielsweise ist ein **ppd-Treiber** unter /home/tester/NATIVE_PRINTER_DRIVER.ppd vorhanden.

```
ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
<!--NeedCopy-->
```

- Citrix bietet drei universelle Druckertreibertypen: postscript, pcl5 und pcl6. Sie können den Treibertyp gemäß Ihren Druckereigenschaften konfigurieren.

  Wenn der Standarddruckertreibertyp des Client beispielsweise PCL5 ist, definieren Sie **drivertype** wie folgt:

```
drivertype=pcl5
<!--NeedCopy-->
```

Ausgabegröße ist Null

Versuchen Sie es mit anderen Druckertypen. Versuchen Sie es auch mit einem virtuellen Drucker wie CutePDF oder PDFCreator, um zu ermitteln, ob das Problem mit dem Druckertreiber zusammenhängt.

Der Druckauftrag hängt vom Druckertreiber und dem Standarddrucker des Clients ab. Es ist wichtig, den Typ des aktuell aktiven Treibers zu identifizieren. Wenn der Clientdrucker einen PCL5-Treiber verwendet, der Linux VDA jedoch einen PostScript-Treiber auswählt, kann ein Problem auftreten.

Wenn der Druckertreibertyp richtig ist, können Sie das Problem mit folgenden Schritten finden:

1. Melden Sie sich bei einer veröffentlichten Desktopsitzung an.
2. Führen Sie folgenden Befehl aus: **vi ~/.CtxlpProfile$CLIENT_NAME**.
3. Fügen Sie das folgende Feld hinzu, um die Spooldatei auf dem Linux VDA zu speichern:

   ```
   deletespoolfile=no
   <!--NeedCopy-->
   ```

4. Melden Sie sich ab und wieder an, um die Konfigurationsänderungen zu laden.
5. Drucken Sie das Dokument zum Reproduzieren des Problems. Nach dem Drucken wird eine Spool-Datei unter `/var/spool/cups-ctx/$logon_user/$spool_file` gespeichert.
6. Prüfen Sie, ob die Spooldatei leer ist. Wenn die Spooldatei NULL ist, liegt ein Problem vor. Wenden Sie sich mit dem Druckprotokoll an den Citrix Support.
7. Wenn die Spooldatei nicht NULL ist, kopieren Sie die Datei auf den Client. Der Inhalt der Spooldatei hängt vom Druckertreibertyp und dem Standarddrucker des Clients ab. Wenn der **zugeordnete (native) Druckertreiber** ein PostScript-Treiber ist, kann die Spooldatei direkt im Linux-Betriebssystem geöffnet werden. Prüfen Sie den Inhalt auf Korrektheit.

   Bei einer PCL-Spooldatei oder einem Windows-Betriebssystem auf dem Client kopieren Sie die Spooldatei auf den Client und drucken Sie sie auf dem clientseitigen Drucker mit einem anderen Druckertreiber.
8. Wechseln Sie den **zugeordneten Drucker**, um einen anderen Druckertreiber zu verwenden. Im folgenden Beispiel wird beispielsweise der PostScript-Clientdrucker verwendet:

   a) Melden Sie sich bei einer aktiven Sitzung an und öffnen Sie einen Browser auf dem Clientdesktop.

   b) Öffnen Sie das Druckverwaltungsportal:

      ```
      localhost:631
      <!--NeedCopy-->
      ```

   c) Wählen Sie den **zugewiesenen Drucker** `CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID` und **ändern Sie den Drucker**. Hierfür sind Administratorprivilegien erforderlich.

   d) Behalten Sie die **cups-ctx**-Verbindung bei und klicken Sie auf **Continue**, um den Druckertreiber zu ändern.

e) Wählen Sie in den Feldern **Make** und **Model** einen anderen Druckertreiber als den Citrix UPD-Treiber aus. Wenn beispielsweise der virtuelle CUPS-PDF-Drucker installiert ist, wählen Sie den Druckertreiber "Generic CUPS-PDF Printer". Speichern Sie die Änderung.

f) Wenn der Vorgang Erfolg hat, konfigurieren Sie den PPD-Dateipfad des Treibers in `.CtxlpProfile$CLIENT_NAME` so, dass der zugeordnete Drucker den neu ausgewählten Treiber verwenden darf.

Bekannte Probleme

Die folgenden Probleme beim Drucken mit dem Linux VDA sind bekannt:

CTXPS-Treiber ist mit einigen PLC-Druckern nicht kompatibel

Wenn Sie Druckausgabestörungen bemerken, legen Sie als Druckertreiber den nativen Druckertreiber des Herstellers fest.

Langsame Druckleistung bei großen Dokumenten

Wenn Sie ein großes Dokument auf einem lokalen Clientdrucker drucken, wird das Dokument über die Serververbindung übertragen. Bei langsamen Verbindungen kann die Übertragung sehr lange dauern.

Drucker- und Druckauftragsbenachrichtigungen aus anderen Sitzungen werden angezeigt

Linux hat nicht das gleiche Sitzungskonzept wie das Windows-Betriebssystem. Daher erhalten alle Benutzer systemweite Benachrichtigungen. Durch Ändern der CUPS-Konfigurationsdatei **/etc/cups/cupsd.conf** können Sie diese Benachrichtigungen deaktivieren.

Suchen Sie den aktuellen, in der Datei konfigurierten Richtliniennamen:

```
DefaultPolicy default
```

Wenn der Richtlinienname *default* lautet, fügen Sie dem XML-Block der Standardrichtlinie die folgenden Zeilen hinzu:

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default
```



```
8
9       SubscriptionPrivateAccess default
10
11      SubscriptionPrivateValues default
12
13      ... ...
14
15      <Limit Create-Printer-Subscription>
16
17           Require user @OWNER
18
19           Order deny,allow
20
21      </Limit>
22
23      <Limit All>
24
25           Order deny,allow
26
27      </Limit>
28
29  </Policy>
30  <!--NeedCopy-->
```

PDF-Druck

January 8, 2024

Mit einer Version der Citrix Workspace-App, die PDF-Druck unterstützt, können Sie PDF-Dateien aus Linux VDA-Sitzungen heraus drucken. Druckaufträge aus der Sitzung werden an den lokalen Computer gesendet, auf dem die Citrix Workspace-App installiert ist. Auf dem lokalen Computer können Sie PDFs mit Ihrem bevorzugten PDF-Viewer öffnen und auf dem Drucker Ihrer Wahl ausdrucken.

Der Linux VDA unterstützt den PDF-Druck auf folgenden Versionen der Citrix Workspace-App:

- Citrix Receiver für HTML5 Versionen 2.4 bis 2.6.9, Citrix Workspace-App 1808 für HTML5 und höher
- Citrix Receiver für Chrome Versionen 2.4 bis 2.6.9, Citrix Workspace-App 1808 für Chrome und höher
- Citrix Workspace-App 1905 für Windows und höher

Konfiguration

Sie müssen eine Version der Citrix Workspace-App verwenden, die den PDF-Druck unterstützt, und die folgenden Richtlinien in Citrix Studio einrichten:

- Wählen Sie für **Clientdruckerumleitung** den Wert **Zugelassen** (Standardeinstellung: **Zugelassen**).
- Wählen Sie für **Universellen PDF-Drucker automatisch erstellen** den Wert **Aktiviert** (Standardeinstellung: **Deaktiviert**).
- Wählen Sie für **Clientdrucker automatisch erstellen** den Wert **Alle Clientdrucker automatisch erstellen**.

Wenn diese Richtlinien aktiviert sind und Sie in einer aktiven Sitzung auf **Drucken** klicken, wird auf der lokalen Maschine eine Druckvorschau angezeigt, sodass Sie einen Drucker auswählen können. Informationen zum Festlegen von Standarddruckern finden Sie in der Dokumentation für die Citrix Workspace-App.

Remote-PC-Zugriff

February 9, 2024

Übersicht

Remote-PC-Zugriff ist eine Erweiterung von Citrix Virtual Apps and Desktops. Damit können Unternehmen einfach und sicher den Remotezugriff auf ihre physischen Büro-PCs ermöglichen. Wenn Benutzer auf ihre Büro-PCs zugreifen können, können sie auf alle Anwendungen, Daten und Ressourcen zugreifen, die sie für ihre Arbeit benötigen.

Remote-PC-Zugriff verwendet dieselben Citrix Virtual Apps and Desktops-Komponenten zum Bereitstellen von virtuellen Desktops und Anwendungen. Die Anforderungen und der Prozess für die Bereitstellung und Konfiguration des Remote-PC-Zugriffs sind mit den Anforderungen und dem Prozess für die Bereitstellung von Citrix Virtual Apps and Desktops identisch. Diese Einheitlichkeit bietet eine konsistente und gemeinsame administrative Erfahrung. Benutzer erhalten die beste Benutzererfahrung, wenn sie Citrix HDX für die Bereitstellung ihrer Büro-PC-Remotesitzungen verwenden.

Weitere Informationen finden Sie unter Remote-PC-Zugriff in der Citrix Virtual Apps and Desktops-Dokumentation.

Überlegungen

Diese Überlegungen gelten speziell für den Linux-VDA:

- Verwenden Sie auf physischen Maschinen den Linux VDA nur im Nicht-3D-Modus. Aufgrund von Einschränkungen des NVIDIA-Treibers kann der lokale Bildschirm des PCs nicht ausgeblendet

werden, wenn der HDX 3D-Modus aktiviert ist. Das Anzeigen dieses Bildschirms ist ein potenzielles Sicherheitsrisiko.

- Verwenden Sie Maschinenkataloge des Typs "Einzelsitzungs-OS"für physische Linux-Maschinen.
- Die automatische Benutzerzuweisung ist für Linux-Maschinen nicht verfügbar. Bei automatischer Benutzerzuweisung werden Benutzer automatisch ihren Maschinen zugewiesen, wenn sie sich lokal an den PCs anmelden. Die Anmeldung erfolgt ohne Administratoreingriff. Die Citrix Workspace-App auf dem Client erleichtert Benutzern den Zugriff auf Anwendungen und Daten auf dem Büro-PC von der Remote-PC-Zugriff-Desktopsitzung aus.
- Wenn Benutzer bereits lokal an ihren PCs angemeldet sind, schlagen Versuche, die PCs über StoreFront zu starten, fehl.
- Energiesparoptionen sind für Linux-Maschinen nicht verfügbar.

Konfiguration

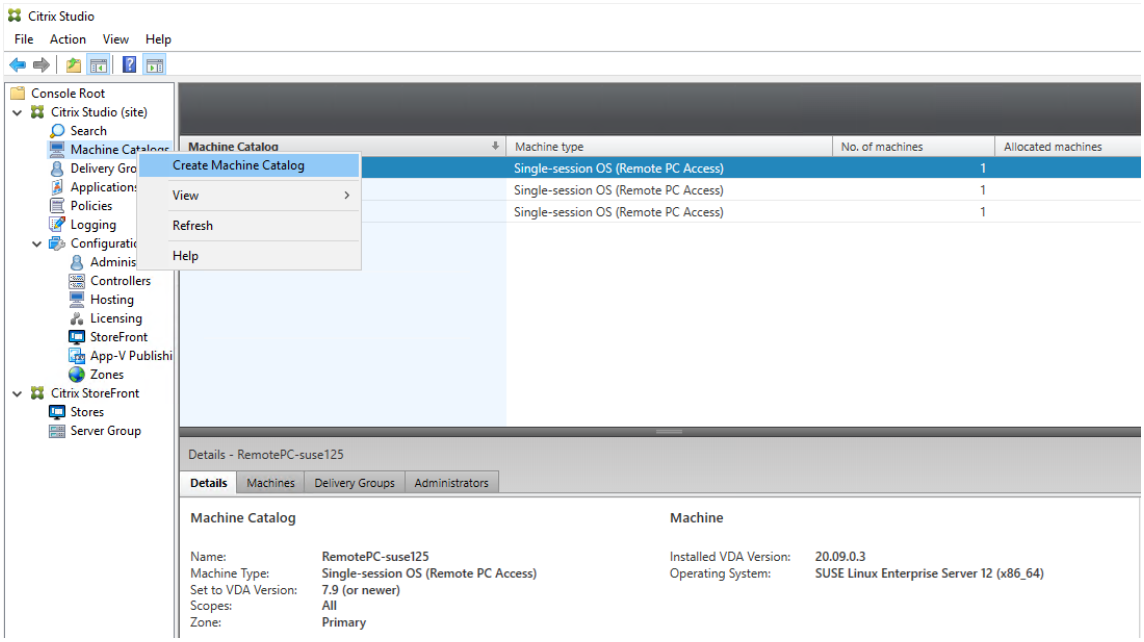
Um Linux-PC-Sitzungen bereitzustellen, installieren Sie den Linux VDA auf Ziel-PCs, erstellen Sie einen Maschinenkatalog vom Typ **Remote-PC-Zugriff** und erstellen Sie eine Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern. Im folgenden Abschnitt wird das Verfahren beschrieben:

Schritt 1 –Installieren des Linux VDA auf Ziel-PCs

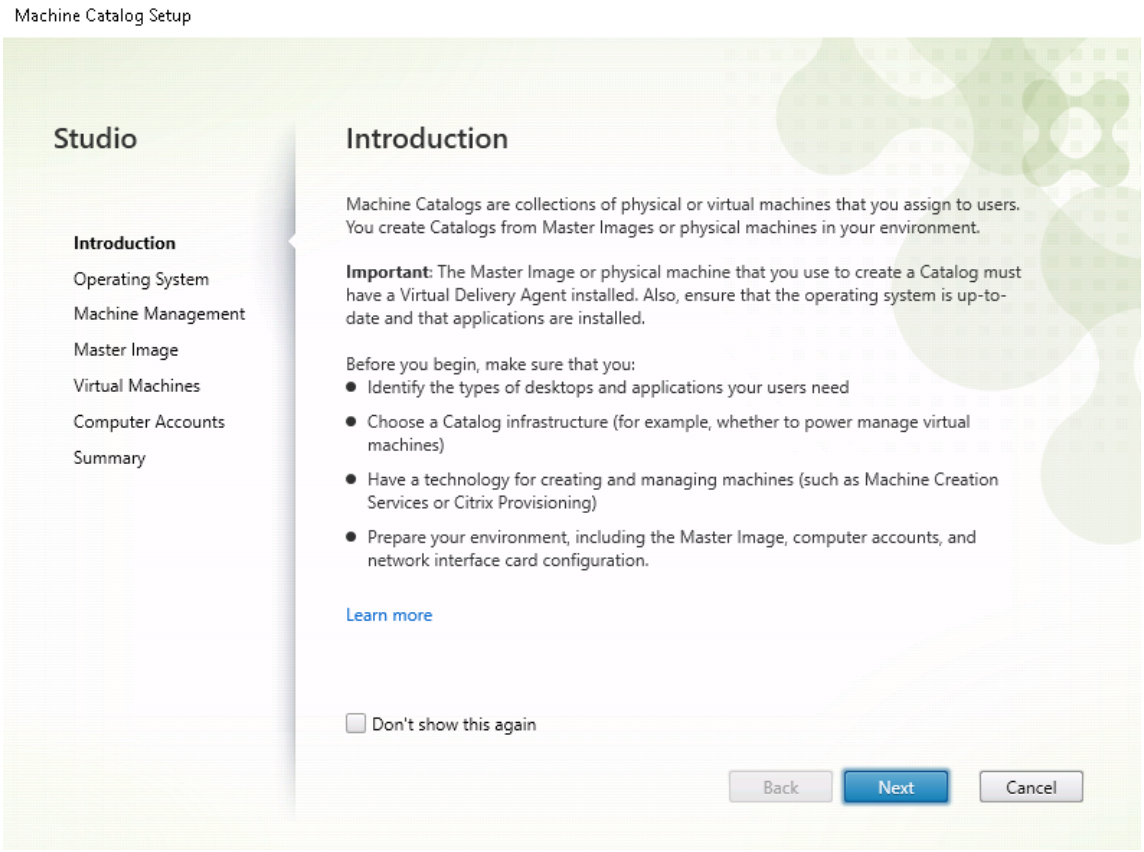
Es wird empfohlen, den Linux VDA mit Easy Install zu installieren. Legen Sie während der Installation für die Variable `CTX_XDL_VDI_MODE` den Wert `Y` fest.

Schritt 2 –Erstellen eines Maschinenkatalogs vom Typ Remote-PC-Zugriff

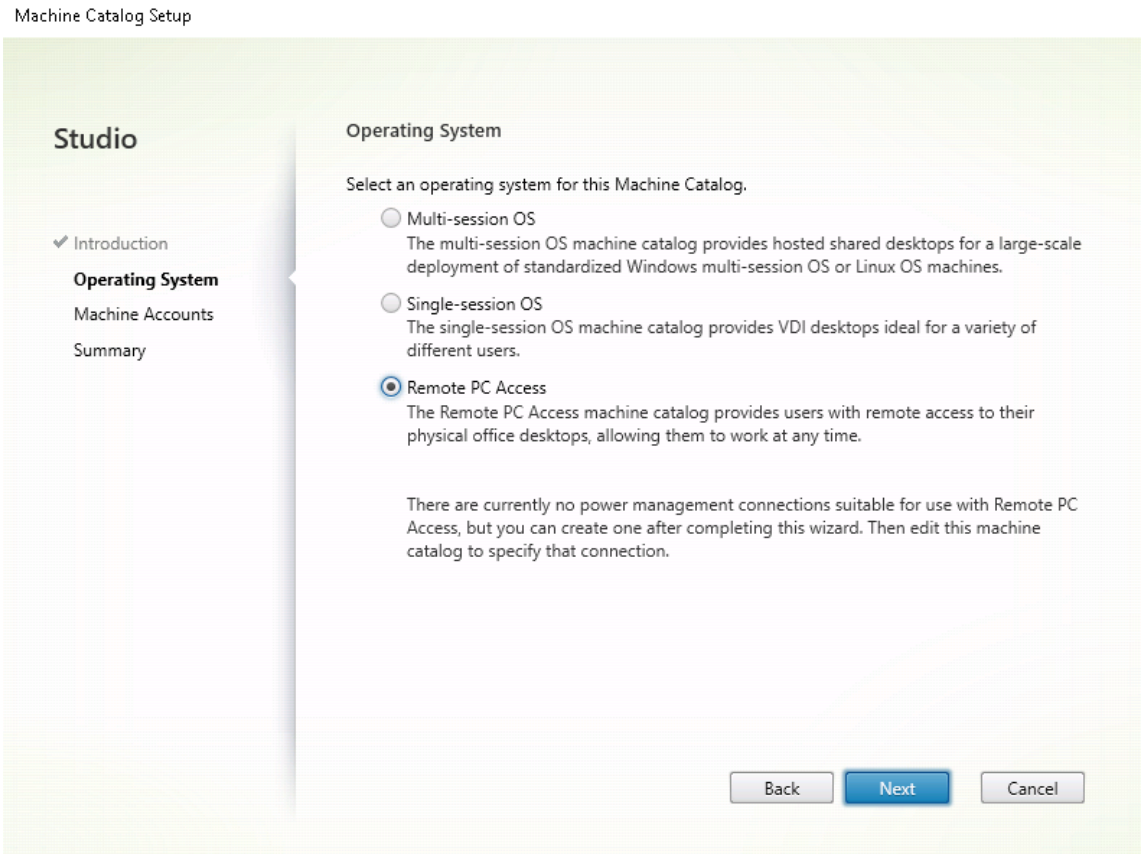
1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Maschinenkataloge** und wählen Sie im Kontextmenü **Maschinenkatalog erstellen** aus.



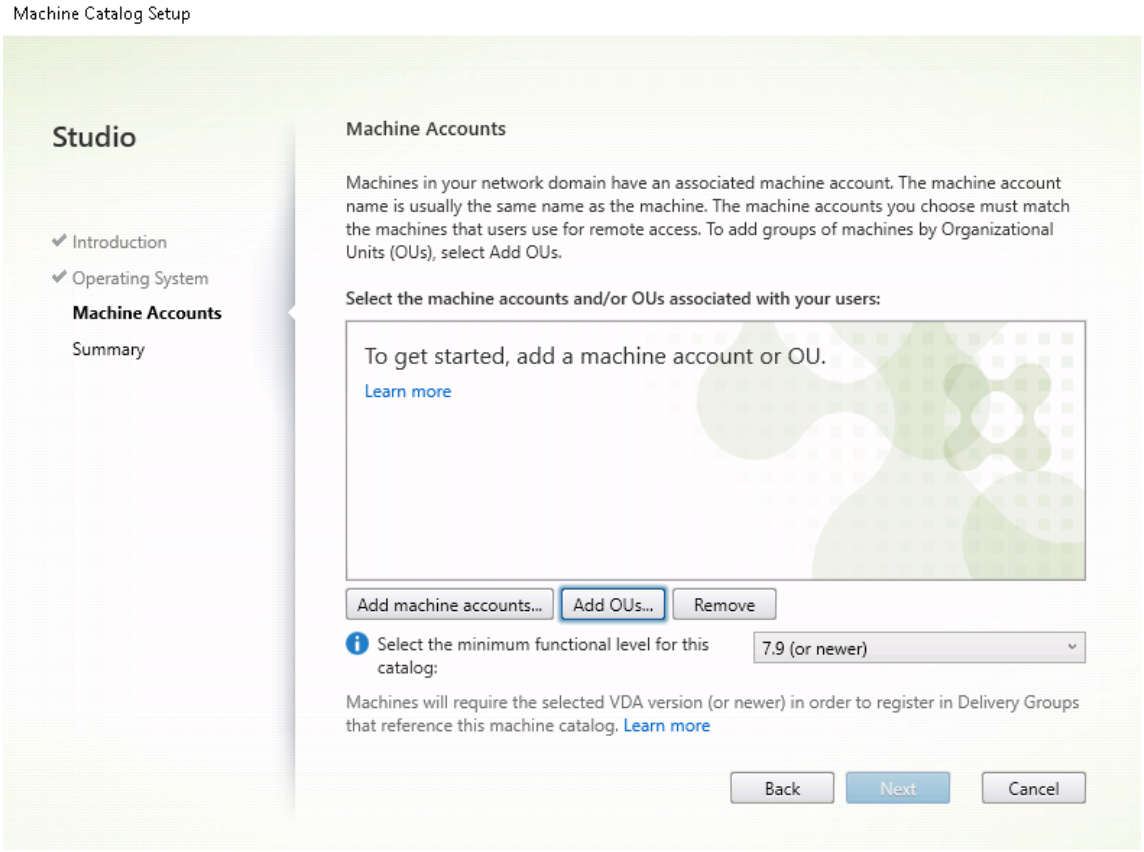
2. Klicken Sie auf der Seite **Einführung** auf **Weiter**.



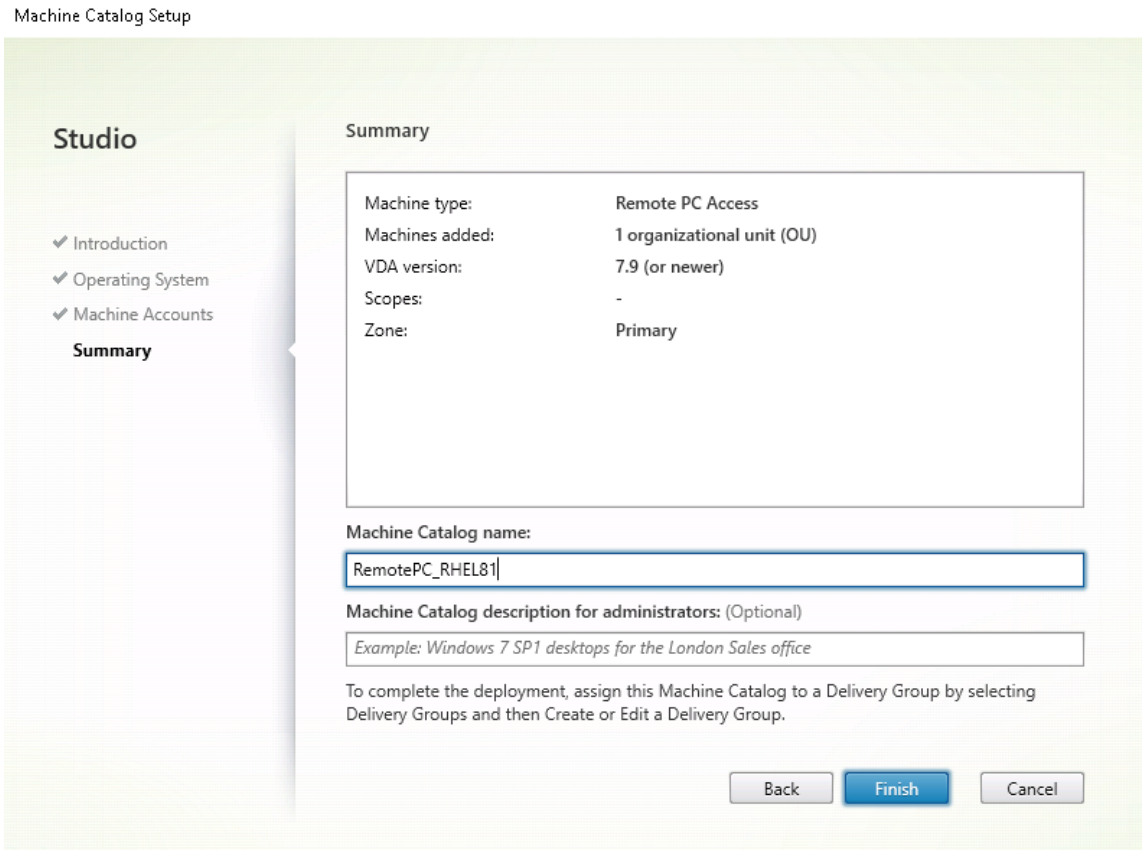
3. Wählen Sie auf der Seite **Betriebssystem** die Option **Remote-PC-Zugriff** aus.



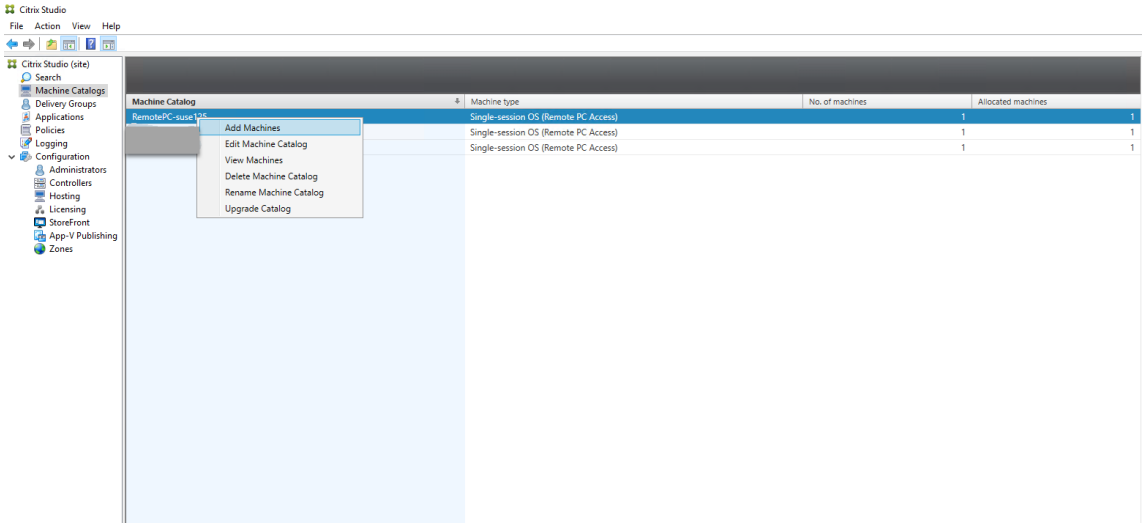
4. Klicken Sie auf **Organisationseinheiten hinzufügen**, um Organisationseinheiten auszuwählen, die die Ziel-PCs enthalten, oder klicken Sie auf **Maschinenkonten hinzufügen**, um dem Maschinenkatalog einzelne Maschinen hinzuzufügen.



5. Benennen Sie den Maschinenkatalog.

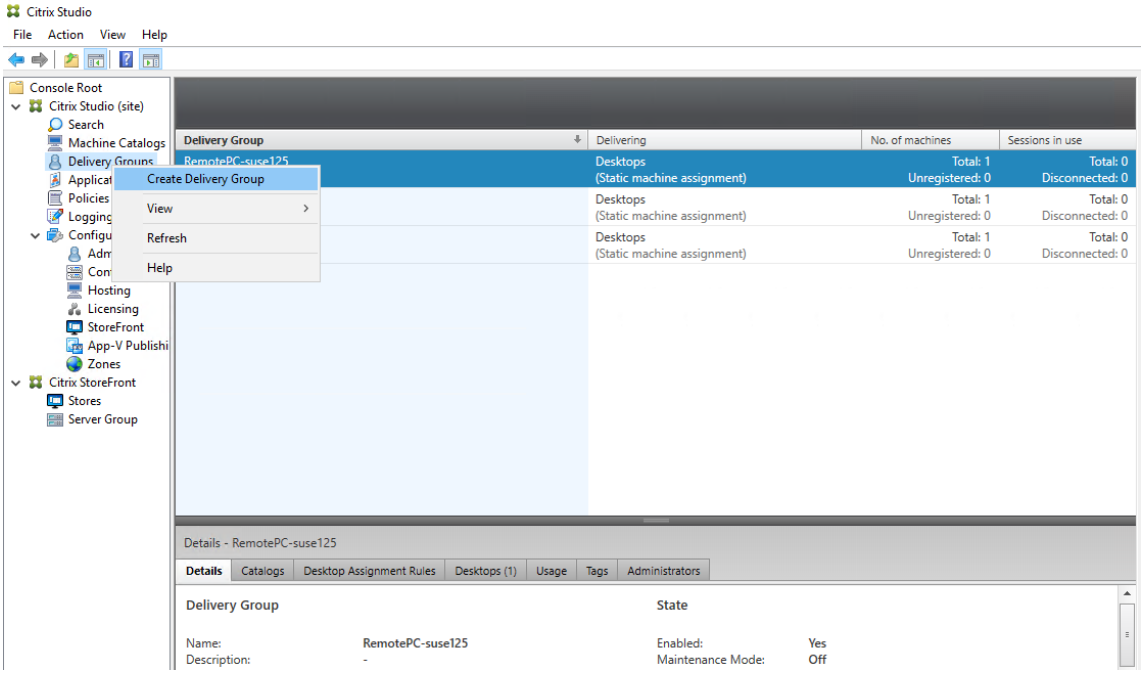


6. (Optional) Klicken Sie mit der rechten Maustaste auf den Maschinenkatalog, um relevante Vorgänge auszuführen.

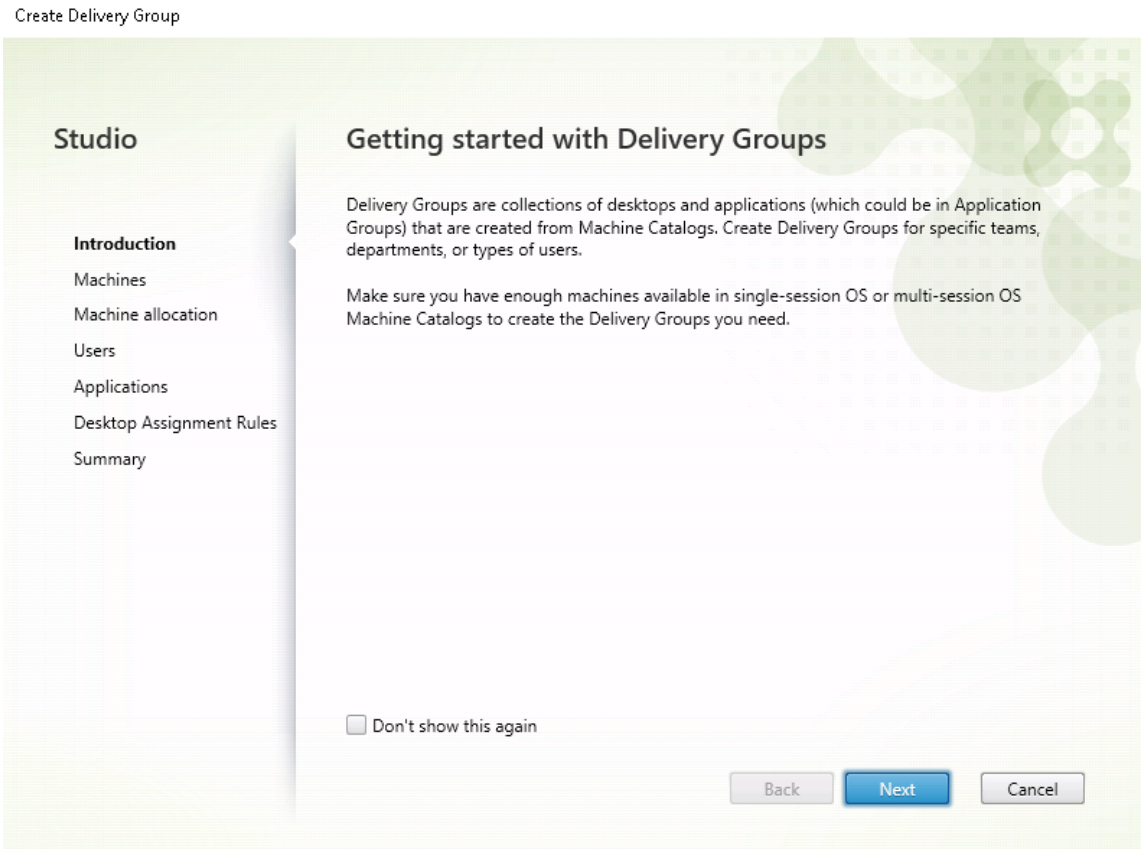


Schritt 3 –Erstellen einer Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern

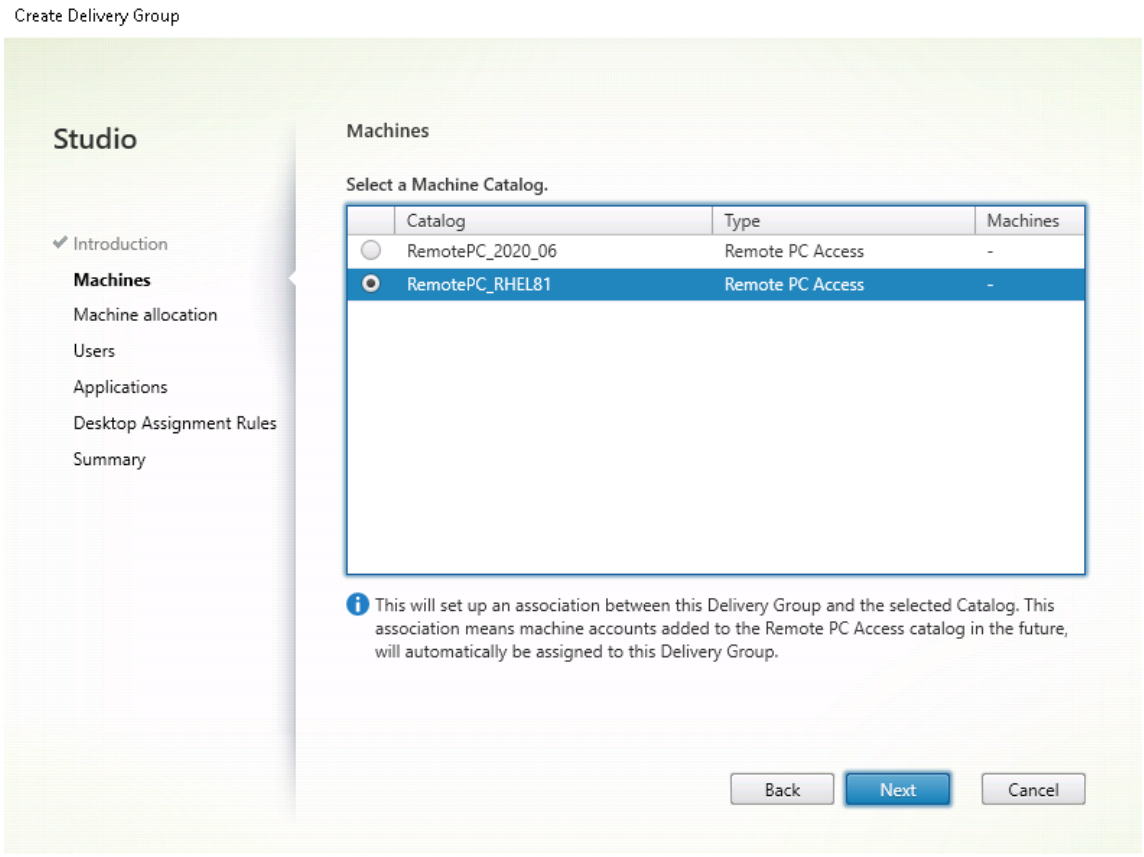
1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Bereitstellungsgruppen** und wählen Sie im Kontextmenü **Bereitstellungsgruppe erstellen** aus.



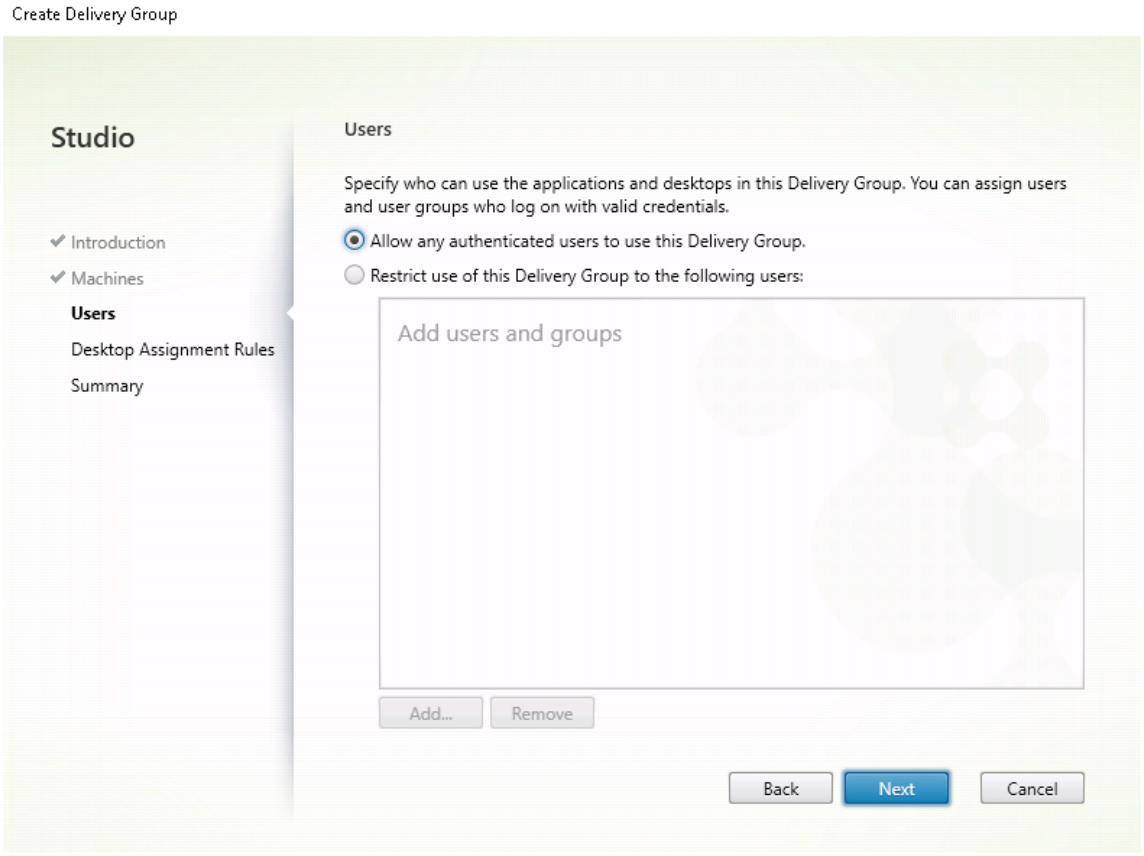
2. Klicken Sie auf der Seite **Erste Schritte für Bereitstellungsgruppen** auf **Weiter**.



3. Wählen Sie den in Schritt 2 erstellten Maschinenkatalog aus, um ihn der Bereitstellungsgruppe zuzuordnen.



4. Fügen Sie Benutzer hinzu, die auf die PCs im Maschinenkatalog zugreifen können. Die von Ihnen hinzugefügten Benutzer können mit der Citrix Workspace App auf einem Clientgerät remote auf die PCs zugreifen.



Wake-On-LAN

Remote-PC-Zugriff unterstützt Wake-On-LAN, sodass physische PCs remote eingeschaltet werden können. Dieses Feature ermöglicht es Benutzern, ihre Büro-PCs ausgeschaltet zu lassen, wenn diese nicht verwendet werden, um Energiekosten zu sparen. Außerdem ist ein Remotezugriff möglich, wenn Maschinen unabsichtlich ausgeschaltet wurden.

Mit dem Wake-On-LAN-Feature werden die Magic Packets auf Befehl des Delivery Controllers direkt vom VDA, der auf dem PC ausgeführt wird, an das Subnetz gesendet, in dem sich der PC befindet. Dadurch kann das Feature ohne Abhängigkeiten von zusätzlichen Infrastrukturkomponenten oder Drittanbieterlösungen für die Bereitstellung von Magic Packets funktionieren.

Das Wake-On-LAN-Feature unterscheidet sich vom älteren SCCM-basierten Wake-On-LAN-Feature. Weitere Informationen zu SCCM-basiertem Wake-on-LAN finden Sie unter Wake-On-LAN –SCCM-integriert.

Systemanforderungen

Folgende Systemanforderungen gelten für die Verwendung des Wake-On-LAN-Feature:

- Steuerungsebene:
  - Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops 2012 oder höher
- Physische PCs:
  - VDA-Version 2012 oder höher
  - Wake-On-LAN, aktiviert im BIOS und auf der Netzwerkkarte

Konfigurieren von Wake-On-LAN

Derzeit kann integriertes Wake-On-LAN nur mit PowerShell konfiguriert werden.

Konfigurieren von Wake-On-LAN:

1. Erstellen Sie den Maschinenkatalog für den Remote-PC-Zugriff (falls noch nicht vorhanden).
2. Erstellen Sie die Wake-On-LAN-Hostverbindung (falls noch nicht vorhanden).

   > **Hinweis:**
   >
   > Wenn Sie über eine Hostverbindung vom Typ "Microsoft Configuration Manager Wake-On-LAN"verfügen, erstellen Sie eine Hostverbindung, um das Wake-On-LAN-Feature zu verwenden.

3. Rufen Sie den eindeutigen Bezeichner der Wake-On-LAN-Hostverbindung ab.
4. Ordnen Sie die Wake-On-LAN-Hostverbindung einem Maschinenkatalog zu.

   Erstellen der Wake-On-LAN-Hostverbindung:

```
# 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
 }

<!--NeedCopy-->
```

Wenn die Hostverbindung bereit ist, führen Sie die folgenden Befehle aus, um den eindeutigen Bezeichner der Hostverbindung abzurufen:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>
    "
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Nachdem Sie den eindeutigen Bezeichner der Verbindung abgerufen haben, führen Sie die folgenden Befehle aus, um die Verbindung dem Remote-PC-Zugriff-Maschinenkatalog zuzuordnen:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
    RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

5. Aktivieren Sie Wake-On-LAN im BIOS und auf der Netzwerkkarte auf jeder VM im Maschinenkatalog.

   Hinweis: Die Methode zum Aktivieren von Wake-On-LAN variiert je nach Maschinenkonfiguration.

   - Aktivieren von Wake-On-LAN im BIOS:
     a) Öffnen Sie das BIOS und aktivieren Sie das Wake-On-LAN-Feature.
     Die Methode für den Zugriff auf das BIOS hängt vom Hersteller der Hauptplatine und dem von ihm gewählten BIOS-Anbieter ab.
     b) Speichern Sie Ihre Einstellungen und starten Sie die Maschine neu.
   - Aktivieren von Wake-On-LAN auf der Netzwerkkarte:
     a) Prüfen Sie mit dem Befehl `sudo ethtool <NIC>`, ob Ihre Netzwerkkarte Magic Packets unterstützt.
     <NIC> ist der Gerätename Ihrer Netzwerkkarte, also beispielsweise `eth0`. Der Befehl `sudo ethtool <NIC>` liefert Angaben zu den Fähigkeiten Ihrer Netzwerkkarte:

- Wenn die Befehlsausgabe eine Zeile wie `Supports Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` enthält, unterstützt Ihre Netzwerkkarte die Wake-On-LAN-Methode mit Magic Packets.
- Wenn die Befehlsausgabe eine Zeile wie `Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` und nicht den Buchstaben `d` enthält, ist die Wake-On-LAN-Methode mit Magic Packets aktiviert. Wenn `<letters>` jedoch den Buchstaben `d` enthält, ist das Wake-On-LAN-Feature deaktiviert. Führen Sie in diesem Fall den Befehl `sudo ethtool -s <NIC> wol g` aus, um Wake-On-LAN zu aktivieren.

b) Bei den meisten Distributionen ist der Befehl `sudo ethtool -s <NIC> wol g` nach jedem Start erforderlich. Um die Option dauerhaft festzulegen, führen Sie die folgenden Schritte basierend auf Ihren Distributionen aus:

Ubuntu:

Fügen Sie in der Schnittstellenkonfigurationsdatei `/etc/network/interfaces` die Zeile `up ethtool -s <NIC> wol g` hinzu. Beispiel:

```
# ifupdown has been replaced by netplan(5) on this system.
    See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
# sudo apt install ifupdown
auto eth0
iface eth0 inet static
           address 10.0.0.1
           netmask 255.255.240.0
           gateway 10.0.0.1
           up ethtool -s eth0 wol g
<!--NeedCopy-->
```

RHEL/SUSE:

Fügen Sie der Schnittstellenkonfigurationsdatei `/etc/sysconfig/network-scripts/ifcfg-<NIC>` den Parameter `ETHTOOL_OPTS` hinzu :

```
ETHTOOL_OPTS="-s ${
 DEVICE }
  wol g"
<!--NeedCopy-->
```

Designüberlegungen

Wenn Sie planen, Wake-On-LAN mit Remote-PC-Zugriff zu verwenden, sollten Sie Folgendes beachten:

- Mehrere Maschinenkataloge können dieselbe Wake-On-LAN-Hostverbindung verwenden.
- Damit ein PC einen anderen PC reaktivieren kann, müssen beide PCs sich im gleichen Subnetz

befinden und dieselbe Wake-On-LAN-Hostverbindung verwenden. Die PCs können sich im gleichen oder in unterschiedlichen Maschinenkatalogen befinden.
- Hostverbindungen werden bestimmten Zonen zugewiesen. Wenn Ihre Bereitstellung mehr als eine Zone enthält, benötigen Sie in jeder Zone eine Wake-On-LAN-Hostverbindung. Gleiches gilt für Maschinenkataloge.
- Magic Packets werden mit der globalen Broadcast-Adresse 255.255.255.255 übertragen. Stellen Sie sicher, dass diese Adresse nicht blockiert ist.
- Um Maschinen in einem Subnetz zu reaktivieren, muss in diesem Subnetz (für jede Wake-On-LAN-Verbindung) mindestens ein PC aktiviert sein.

Operative Überlegungen

Berücksichtigen Sie Folgendes bei der Verwendung des Wake-On-LAN-Features:

- Der VDA muss sich mindestens einmal registrieren, bevor der PC über die integrierte Wake-On-LAN-Funktion reaktiviert werden kann.
- Wake-on-LAN kann nur zum Reaktivieren von PCs verwendet werden. Andere Energieaktionen wie Neustart oder Herunterfahren werden nicht unterstützt.
- Nachdem die Wake-On-LAN-Verbindung erstellt wurde, ist sie in Studio sichtbar. Das Bearbeiten ihrer Eigenschaften in Studio wird jedoch nicht unterstützt.
- Es gibt zwei Situationen, in denen ein Magic Packet gesendet wird:
  - Ein Benutzer versucht, eine Sitzung auf dem PC zu starten und der VDA ist nicht registriert.
  - Ein Administrator sendet manuell einen Einschaltbefehl über Studio oder PowerShell.
- Da der Delivery Controller den Energiezustand eines PCs nicht kennt, wird in Studio unter "Energiezustand"**Nicht unterstützt** angezeigt. Der Delivery Controller ermittelt anhand des VDAs -Registrierungsstatus, ob ein PC ein- oder ausgeschaltet ist.

Weitere Ressourcen

Im Folgenden finden Sie weitere Ressourcen für Remote-PC-Zugriff:

- Solution design guidance: Remote PC Access Design Decisions.
- Remote-PC-Zugriff-Musterarchitekturen: Referenzarchitektur für Citrix Remote-PC-Zugriff-Lösung.

Sitzung

January 8, 2024

Dieser Abschnitt behandelt die folgenden Themen:

- Adaptiver Transport
- Anmeldung mit einem temporären Basisverzeichnis
- Anwendungen veröffentlichen
- Sitzungszuverlässigkeit
- Rendezvous V1
- Rendezvous V2
- Sichere Benutzersitzungen mit TLS
- Sichere Benutzersitzungen mit DTLS

Adaptiver Transport

January 8, 2024

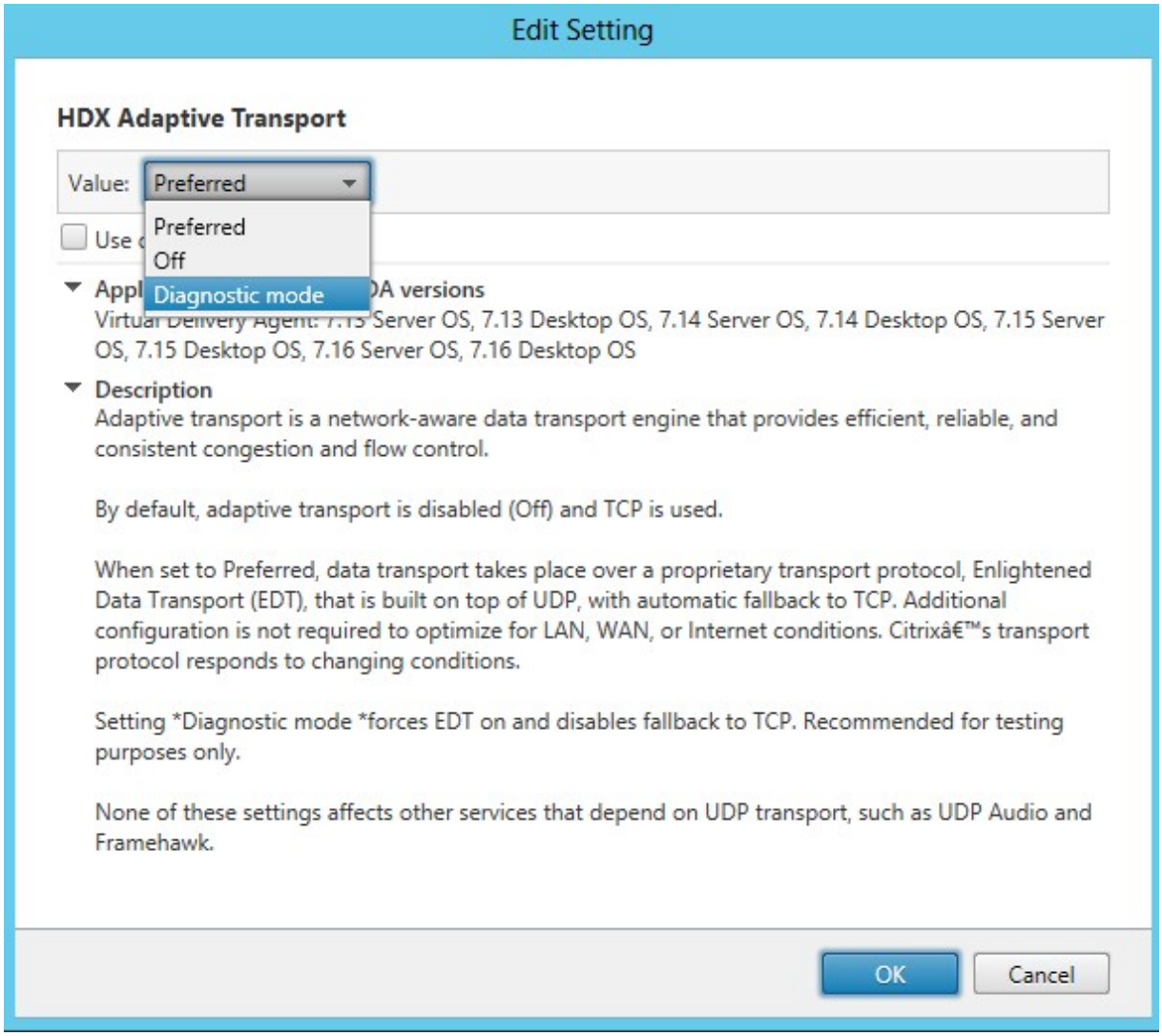
Adaptiver Transport ist ein Verfahren in Citrix Virtual Apps and Desktops, mit dem Enlightened Data Transport (EDT) als Transportprotokoll für ICA-Verbindungen verwendet werden kann. Wenn EDT nicht verfügbar ist, wechselt der adaptive Transport zu TCP.

EDT ist ein Citrix-eigenes Transportprotokoll, das auf UDP (User Datagram Protocol) basiert. Es liefert eine überlegene Benutzererfahrung bei schwierigen Langstreckenverbindungen, ohne Abstriche bei der Serverskalierbarkeit. EDT verbessert den Datendurchsatz für alle virtuellen ICA-Kanäle in instabilen Netzwerken und bietet so einen verlässlicheren Service.

Weitere Informationen finden Sie unter Adaptiver Transport in der Dokumentation zu Citrix Virtual Apps and Desktops.

Adaptiven Transport aktivieren oder deaktivieren

Der adaptive Transport ist standardmäßig aktiviert. Sie können die folgenden Optionen mit der Richtlinieneinstellung **Adaptiver HDX-Transport** konfigurieren:



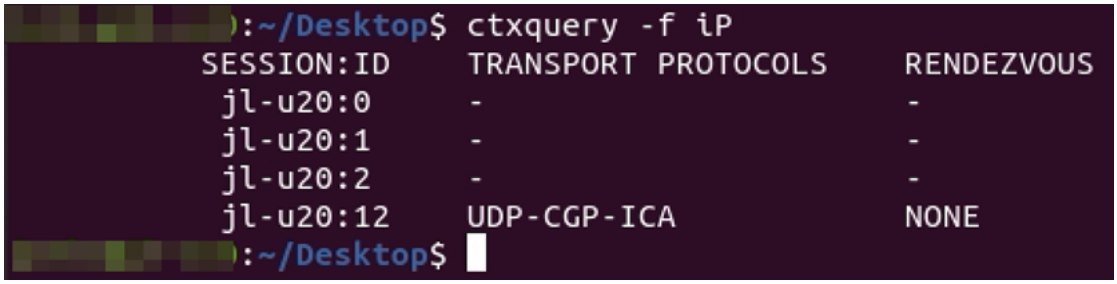
- **Bevorzugt:** Der adaptive Transport ist aktiviert und verwendet EDT (Enlightened Data Transport) als bevorzugtes Transportprotokoll sowie TCP als Fallback.
- **Diagnosemodus**: Der adaptive Transport ist aktiviert und erzwingt den Einsatz von EDT. Der Fallback auf TCP ist deaktiviert. Diese Einstellung wird nur zum Testen und zur Fehlerbehebung empfohlen.
- **Aus**. Der adaptive Transport ist deaktiviert, und es wird nur TCP für den Transport verwendet.

Überprüfen, ob der adaptive Transport verwendet wird

Mit dem folgenden Befehl überprüfen Sie, ob EDT als Transportprotokoll für die aktuelle Sitzung verwendet wird.

```
/opt/Citrix/VDA/bin/ctxquery -f iP
<!--NeedCopy-->
```


Wenn EDT verwendet wird, wird UDP in den Transportprotokollen angezeigt, zum Beispiel:



MTU-Discovery durch EDT

Mit MTU-Discovery kann EDT beim Einrichten einer Sitzung automatisch die maximale Übertragungseinheit (MTU) ermitteln. Dadurch wird eine EDT-Paketfragmentierung verhindert, die zu einer Leistungsminderung oder einem Fehler beim Einrichten der Sitzung führen kann.

Systemanforderungen:

- Linux VDA ab 2012 (Mindestversion)
- Citrix Workspace-App:
  - Windows: 1911 oder höher
- Citrix ADC:
  - 13.0.52.24 oder höher
  - 12.1.56.22 oder höher
- Sitzungszuverlässigkeit muss aktiviert sein.

Bei Verwendung von Clientplattformen oder Versionen, die dieses Feature nicht unterstützen, finden Sie unter CTX231821 weitere Informationen zum Konfigurieren einer benutzerdefinierten EDT-MTU, die für Ihre Umgebung geeignet ist.

Steuern der MTU-Discovery durch EDT auf dem VDA

Die MTU-Discovery durch EDT ist standardmäßig deaktiviert.

- Um die MTU-Discovery durch EDT zu aktivieren, setzen Sie mit folgendem Befehl den Registrierungsschlüssel `MtuDiscovery`, starten den VDA neu und warten, bis der VDA registriert ist:

```
1  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
       CurrentControlSet\Control\Terminal Server\Wds\icawd" -t "
       REG_DWORD" -v "MtuDiscovery" -d "0x00000001" --force
2  <!--NeedCopy-->
```


- Zum Deaktivieren der MTU-Discovery durch EDT löschen Sie den Registrierungswert `MtuDiscovery`.

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des **Registrierungseditors** zurückzuführen sind, behoben werden können. Die Verwendung des **Registrierungseditors** geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Steuern der MTU-Discovery durch EDT auf dem Client

Sie können die MTU-Discovery durch EDT selektiv auf Clients steuern, indem Sie den Parameter `MtuDiscovery` in der ICA-Datei hinzufügen. Um das Feature zu deaktivieren, legen Sie im Abschnitt `Application` Folgendes fest:

```
MtuDiscovery=Off
```

Um das Feature wieder zu aktivieren, löschen Sie den Parameter `MtuDiscovery` aus der ICA-Datei.

> **Wichtig:**
>
> Dieser Parameter in der ICA-Datei funktioniert nur, wenn Sie die MTU-Discovery durch EDT auf dem VDA aktivieren. Ist die MTU-Discovery durch EDT auf dem VDA nicht aktiviert, zeigt der Parameter in der ICA-Datei keine Wirkung.

Verbesserte EDT-Überlastungssteuerung

Zur Optimierung des EDT-Protokolls wird ein Algorithmus zur Überlastungssteuerung eingeführt. Damit kann EDT höhere Durchsätze erzielen und die Latenz reduzieren, wodurch das Benutzererlebnis verbessert wird. Das Feature ist in der Standardeinstellung deaktiviert. Führen Sie zur Aktivierung den folgenden Befehl aus und starten Sie den Dienst `ctxhdx` neu:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters" -t "
     REG_DWORD" -v "edtBBR" -d "0x00000001" --force
2 <!--NeedCopy-->
```


Benutzerdefinierte Hintergründe und Bannermeldungen auf Anmeldebildschirmen

February 9, 2024

Benutzerdefinierten Hintergrund oder Bannermeldung auf Anmeldebildschirm hinzufügen

> **Tipp:**
>
> Um das Feature in SUSE 15.4 zu verwenden, installieren Sie `imlib2` von http://download.opensuse.org/distribution/leap/15.3/repo/oss/.

Mit den folgenden Befehlen können Sie auf dem **Anmeldebildschirm** einer Sitzung einen benutzerdefinierten Hintergrund oder eine Bannermeldung hinzufügen. Um beides (Hintergrund und Bannermeldung) zum **Anmeldebildschirm** einer Sitzung hinzuzufügen, können Sie die Bannermeldung in das Hintergrundbild einbetten. Wenn Sie eine Sitzung öffnen, wird zuerst die Bannernachricht und anschließend das Authentifizierungsdialogfeld angezeigt.

Um den Titel einer Bannernachricht festzulegen, führen Sie folgenden Befehl aus:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix" -t "REG_SZ" -v "LogonDisplayStringTitle" -d "<Banner
      message title>" --force
2 <!--NeedCopy-->
```

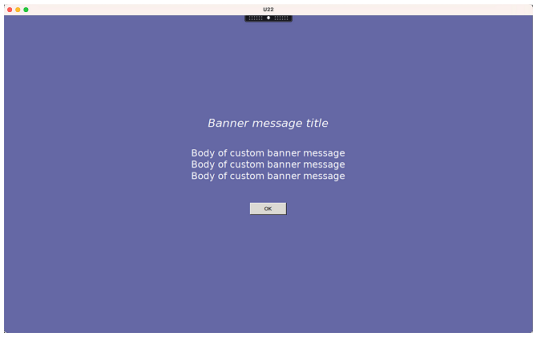
Die maximale Länge des Titels einer Bannernachricht beträgt 64 Byte.

Um den Haupttext einer Bannernachricht festzulegen, führen Sie folgenden Befehl aus:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix" -t "REG_SZ" -v "LogonDisplayString" -d "Body of
     custom banner message\nBody of custom banner message\nBody of custom
      banner message\n" --force
2 <!--NeedCopy-->
```

Die maximale Länge eines Bannernachrichtentexts beträgt 1.024 Byte.

> **Tipp:**
>
> Das Element `\n` erzeugt einen Zeilenumbruch. In diesem Beispiel sieht die Bannernachricht wie folgt aus:

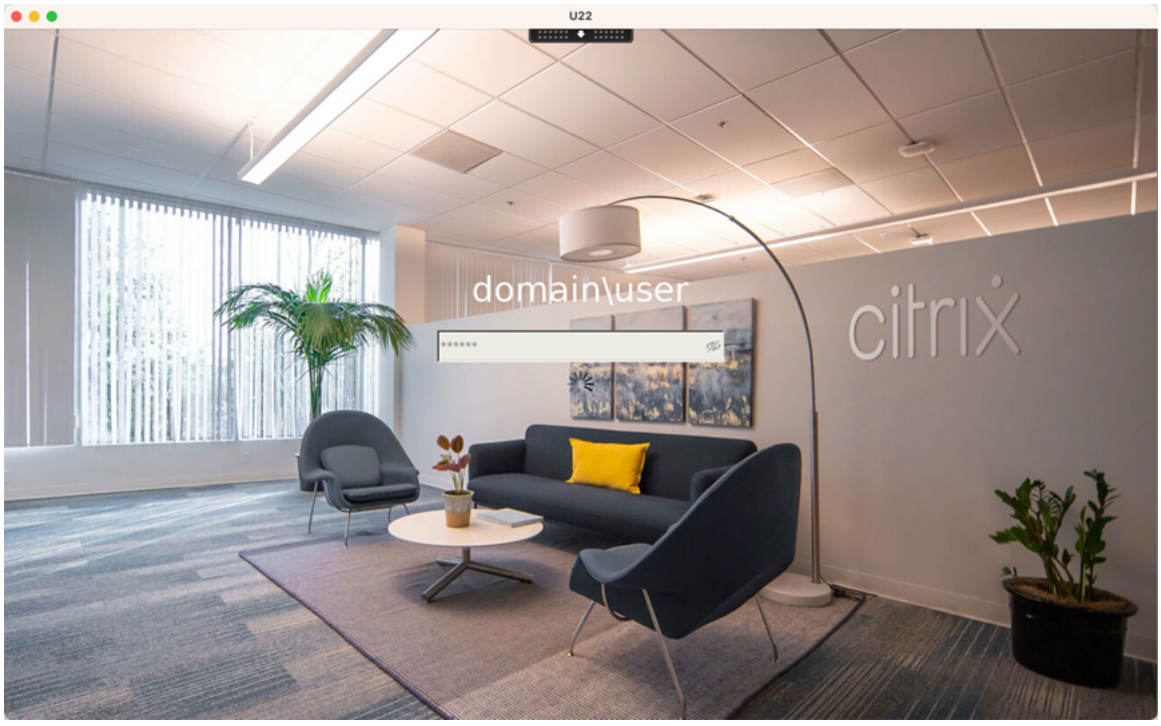


Führen Sie folgenden Befehl aus, um den **Sitzungsanmeldebildschirmen** einen benutzerdefinierten Hintergrund hinzuzufügen:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
   Control\Citrix" -t "REG_SZ" -v "BackgroundImagePath" -d "<path to
   the background image>" --force
<!--NeedCopy-->
```

Um den benutzerdefinierten Hintergrund zu sehen, müssen Sitzungsbenutzer Zugriff auf den Pfad zum Hintergrundbild haben.

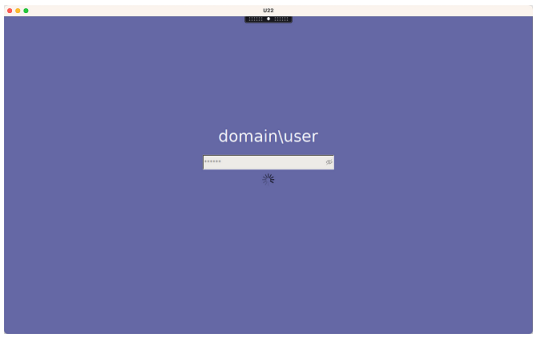
Beispiel:



Beispiele für Sitzungsanmeldebildschirme

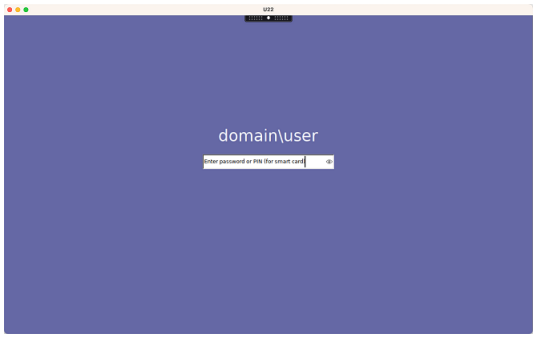
Im Folgenden finden Sie Beispiele für Sitzungsanmeldebildschirme in verschiedenen Szenarien:

- **Sitzungsanmeldung** bei Single-Sign-On:



  Der **Anmeldevorgang** wird angezeigt.

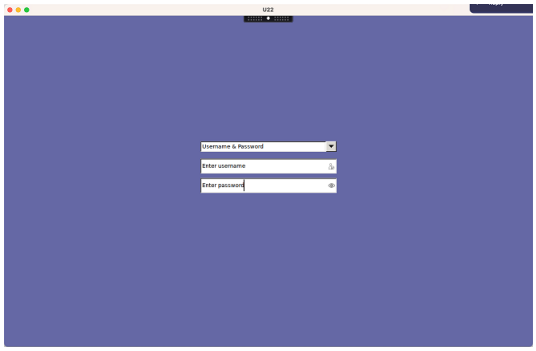
- **Sitzungsanmeldung** in typischen Szenarien ohne Single Sign-On:



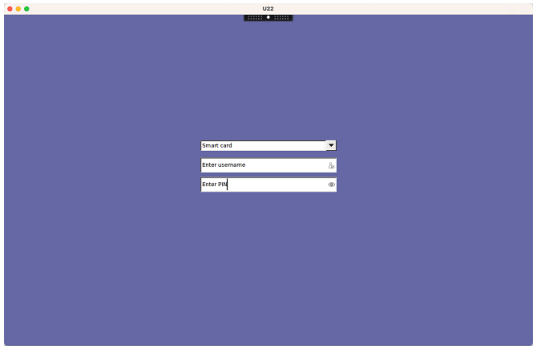
  - In Szenarien ohne Single Sign-On ist ein Kennwort oder ein PIN-Code erforderlich.
  - Die Benutzer können die Anzeige von Kennwörtern und PIN-Codes ein- und ausschalten, um falsche Eingaben leichter zu sehen.

- Sitzungsanmeldung ohne Single Sign-On, wenn sich ein Benutzer bei VDA-Sitzungen mit anderen Anmeldeinformationen anmeldet als bei der Citrix Workspace-App:

  Benutzername und Kennwort für die Sitzungsanmeldung:



  Smartcard für die Sitzungsanmeldung:



Informationen zu den in Szenarien ohne Single Sign-On unterstützten Kombinationen von Benutzerauthentifizierungsmethoden finden Sie unter Authentifizierung ohne Single Sign-On.

Benutzerdefinierte Desktopumgebungen für Sitzungsbenutzer

February 9, 2024

Sie können mit der Variable **CTX_XDL_DESKTOP_ENVIRONMENT** eine Desktopumgebung für Sitzungsbenutzer angeben. Ab Release 2209 können Sitzungsbenutzer ihre Desktopumgebung anpassen. Damit Sitzungsbenutzer dieses Feature verwenden können, müssen Sie Desktopumgebungen vorher auf dem VDA installieren.

Die folgende Tabelle zeigt eine Matrix der Linux-Distributionen und Desktopumgebungen, die benutzerdefinierte Desktopumgebungen für Sitzungsbenutzer unterstützen.

Linux-Distribution	Unterstützter Desktop
Debian11.3	MATE, GNOME, GNOME-Classic, KDE
RHEL 8.8, RHEL 8.6	MATE, GNOME, GNOME-Classic
RHEL 7.9	MATE, GNOME, GNOME-Classic, KDE
Rocky Linux 8.8, Rocky Linux 8.6	MATE, GNOME, GNOME-Classic, KDE
SUSE 15.4	MATE, GNOME, GNOME-Classic
Ubuntu 22.04, Ubuntu 20.04	MATE, GNOME, GNOME-Classic, KDE

Befehle für den Desktopwechsel

> **Hinweis:**
>
> Sie können sowohl vom Terminal aus als auch im Infobereich zwischen Desktop-Umgebungen wechseln.

Um vom Terminal zu einer anderen Desktopumgebung zu wechseln, führen Sie den entsprechenden Befehl in der Sitzung aus:

Zieldesktopumgebung	Führen Sie diesen Befehl aus
GNOME	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME`
GNOME Classic	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh GNOME-CLASSIC`
MATE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh MATE`
KDE	`/opt/Citrix/VDA/bin/ctxdesktopswitch.sh KDE`

KDE-Tipps

- Magnus kann beim Start in KDE geladen werden. Als Workaround können Sie das Magnus-Paket mit dem Befehl `sudo apt remove magnus` entfernen.
- Um QT-Warnungen während des KDE-Starts zu deaktivieren, bearbeiten Sie `/usr/share/qt5/qtlogging.ini` als Root-Benutzer, indem Sie die folgenden Einträge hinzufügen:

```
1  qt.qpa.xcb.xcberror.error=false
2  qt.qpa.xcb.warning=false
3  qt.qpa.xcb.error=false
4  <!--NeedCopy-->
```

- Das Entsperren des Bildschirms kann bei KDE fehlschlagen. Als Workaround empfehlen wir, die automatische Bildschirmsperre des Desktops zu deaktivieren.

Anmeldung mit einem temporären Basisverzeichnis

January 8, 2024

Sie können ein temporäres Basisverzeichnis angeben, das verwendet wird, wenn der Bereitstellungspunkt auf dem Linux VDA fehlschlägt. Wenn ein temporäres Basisverzeichnis angegeben ist, wird bei der Sitzungsanmeldung eine Eingabeaufforderung angezeigt, wenn der Bereitstellungspunkt fehlschlägt. Benutzerdaten werden dann im temporären Basisverzeichnis gespeichert.

Die folgende Tabelle enthält Registrierungsschlüssel, die das Festlegen der Einstellungen für Ihr Basisverzeichnis erleichtern.

Registrierungsschlüssel	Beschreibung	Befehl
`LogNoHome`	Legt fest, ob Benutzer sich an Sitzungen ohne Basisverzeichnis anmelden können. Der Standardwert ist 1 und bedeutet "Ja". Wenn der Wert auf 0 gesetzt ist, werden Sitzungsanmeldungen ohne Basisverzeichnis deaktiviert.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "LogNoHome"-d "0x00000001"--force`
`HomeMountPoint`	Richtet einen lokalen Bereitstellungspunkt auf dem Linux VDA ein. Wenn der Bereitstellungspunkt beispielsweise `/mnt/home` ist, ist das Basisverzeichnis eines Benutzers `/mnt/home/domain/<user_name>`. Stellen Sie sicher, dass der Bereitstellungspunkt mit dem Basisverzeichnis des Benutzers in Ihrer Umgebung übereinstimmt. Diese Einstellung ist nur wirksam, wenn `CheckUserHomeMountPoint` auf 0 gesetzt ist.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "HomeMountPoint"-d "<A directory where the NFS share is to be mounted>"--force`

Registrierungsschlüssel	Beschreibung	Befehl
CheckUserHomeMountPoint	Steuert, ob benutzerspezifische Basisverzeichnisse als Bereitstellungspunkt auf dem Linux VDA festgelegt werden. Wenn Sie benutzerspezifische Basisverzeichnisse als Bereitstellungspunkt festlegen möchten, legen Sie den Wert auf **1** fest. Der Standardwert ist **0**.	`ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "CheckUserHomeMountPoint"-d "0x00000001"--force`
TempHomeDirectoryPath	Richtet ein temporäres Basisverzeichnis auf dem Linux VDA ein für den Fall, dass der Bereitstellungspunkt fehlschlägt. Der Standardwert ist /tmp. Die Einstellung für das temporäre Basisverzeichnis wird nur wirksam, wenn der mit HomeMountPoint und CheckUserHomeMountPoint festgelegte Bereitstellungspunkt nicht verfügbar ist. Ein temporäres Basisverzeichnis für einen Benutzer ist /tmp/CTXSmf_user_id.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_SZ"-v "TempHomeDirectoryPath"-d "</tmp by default>"--force`
CheckMountPointRetryTime	Legt mit einer Frequenz von einmal pro Sekunde fest, wie viele Prüfungen durchgeführt werden, um festzustellen, ob die Bereitstellung erfolgreich war. Der Standardwert ist 5.	`ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "CheckMountPointRetryTime"-d "0x000000010"--force`

Registrierungsschlüssel	Beschreibung	Befehl
RemoveHomeOnLogoff	Legt fest, ob temporäre Basisverzeichnisse nach der Abmeldung des Benutzers zu entfernen sind. 1 bedeutet “Ja” . 0 bedeutet “Nein”.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix"-t "REG_DWORD"-v "RemoveHomeOnLogoff"-d "0x00000000"--force`

Anwendungen veröffentlichen

January 8, 2024

Mit Linux VDA-Version 7.13 hat Citrix das Feature Seamlessanwendungen auf allen unterstützten Linux-Plattformen hinzugefügt. Zum Verwenden dieses Features sind keine besonderen Installationsmaßnahmen erforderlich.

> **Tipp:**
>
> Für Version 1.4 des Linux VDA hat Citrix die Unterstützung für veröffentlichte Nicht-Seamlessanwendungen und die Sitzungsfreigabe hinzugefügt.

Veröffentlichen von Anwendungen mit Citrix Studio

Sie können die auf einem Linux VDA installierten Anwendungen beim Erstellen einer Bereitstellungsgruppe veröffentlichen oder einer vorhandenen Bereitstellungsgruppe hinzufügen. Dies ist vergleichbar mit dem Veröffentlichen von auf einem Windows VDA installierten Anwendungen. Weitere Informationen finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation(basierend auf der verwendeten Version von Citrix Virtual Apps and Desktops).

> **Hinweis:**
>
> - Achten Sie beim Konfigurieren von Bereitstellungsgruppen darauf, als Bereitstellungstyp **Desktop und Anwendungen** oder **Anwendungen** festzulegen.
> - Die Veröffentlichung von Anwendungen wird unter Linux VDA-Version 1.4 und höher unterstützt. Der Linux VDA unterstützt jedoch keine Bereitstellung von Desktops und Anwendungen für dieselbe Maschine. Um dieses Problem zu lösen, empfehlen wir, für App- und

> Desktop-Bereitstellungen separate Bereitstellungsgruppen zu erstellen.
>
> - Um Seamlessanwendungen zu verwenden, deaktivieren Sie den Seamlessmodus nicht auf StoreFront. Der Seamlessmodus ist standardmäßig aktiviert. Wenn Sie den Modus durch "TWIMode=Off"bereits deaktiviert haben, entfernen Sie diese Einstellung, statt sie in "TWIMode=On"zu ändern. Andernfalls können Sie u. U. keine veröffentlichten Desktops starten.

Einschränkung

Der Linux VDA unterstützt keinen Start mehrerer Instanzen einer Anwendung durch einen Benutzer.

In App-Sitzungen funktionieren nur App-spezifische Verknüpfungen einwandfrei.

Bekannte Probleme

Beim Veröffentlichen von Anwendungen sind folgende Probleme bekannt:

- Nicht-rechteckige Fenster werden nicht unterstützt. Die Ecken eines Fensters zeigen möglicherweise den serverseitigen Hintergrund an.
- Die Vorschau des Inhalts eines Fensters aus einer veröffentlichten Anwendung wird nicht unterstützt.
- Wenn Sie mehrere LibreOffice-Anwendungen ausführen, wird nur die zuerst gestartete in Citrix Studio angezeigt, da diese Anwendungen denselben Prozess verwenden.
- Veröffentlichte, auf Qt5 basierende Anwendungen wie "Dolphin"zeigen u. U. keine Symbole an. Um das Problem zu beheben, lesen Sie den Artikel unter https://wiki.archlinux.org/title/Qt.

Rendezvous V1

January 8, 2024

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerebene herzustellen.

Es sind zwei Arten von Datenverkehr zu berücksichtigen: 1) Steuerungsdatenverkehr für die VDA-Registrierung und die Sitzungsvermittlung; 2) HDX-Sitzungsdatenverkehr.

Rendezvous V1 ermöglicht es, dass HDX-Sitzungsdatenverkehr Cloud Connectors umgeht. Cloud Connectors sind jedoch weiterhin erforderlich, um als Proxy für den gesamten Steuerungsdatenverkehr für die VDA-Registrierung und das Sitzungsbrokering zu fungieren.

Anforderungen

- Zugriff auf die Umgebung mit Citrix Workspace und Citrix Gateway Service.
- Steuerungsebene: Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- Linux VDA Version 2112 oder höher.
  - Version 2112 ist die erforderliche Mindestversion für nicht transparente HTTP-Proxys.
  - Version 2204 ist die erforderliche Mindestversion für transparente Proxys und SOCKS5-Proxys.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix Richtlinie. Weitere Informationen finden Sie unter Richtlinieneinstellung für Rendezvous-Protokoll.
- Die VDAs müssen Zugriff auf `https://*.nssvc.net` einschließlich aller Unterdomänen haben. Wenn Sie nicht alle Unterdomänen auf diese Weise auf die Positivliste setzen können, verwenden Sie stattdessen `https://*.c.nssvc.net` und `https://*.g.nssvc.net`. Weitere Informationen finden Sie im Abschnitt Anforderungen an die Internetkonnektivität der Citrix Cloud-Dokumentation (unter "Virtual Apps and Desktops Service") und im Knowledge Center-Artikel CTX270584.
- Cloud Connectors müssen beim Brokering einer Sitzung die FQDNs der VDAs abrufen. Um dieses Ziel zu erreichen, aktivieren Sie die DNS-Auflösung für die Site: Führen Sie mit dem Remote PowerShell SDK von Citrix DaaS den Befehl `Set-BrokerSite -DnsResolutionEnabled $true` aus. Weitere Informationen zum Remote PowerShell SDK von Citrix DaaS finden Sie unter SDKs und APIs.

Proxykonfiguration

Der VDA unterstützt Rendezvous-Verbindungen über HTTP- und SOCKS5-Proxys.

Überlegungen zum Proxy

Berücksichtigen Sie Folgendes, wenn Sie Proxys mit Rendezvous verwenden:

- Nicht transparente HTTP-Proxys und SOCKS5-Proxys werden unterstützt.
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der ICA-Datenverkehr zwischen dem VDA und Gateway Service nicht abgefangen, entschlüsselt oder überprüft wird. Ansonsten bricht die Verbindung ab.
- HTTP-Proxys unterstützen die maschinenbasierte Authentifizierung über Aushandlungs- und Kerberos-Authentifizierungsprotokolle. Wenn Sie eine Verbindung mit dem Proxyserver herstellen, wählt das Aushandlungsauthentifizierungsschema automatisch das Kerberos-Protokoll aus. Kerberos ist das einzige Schema, das vom Linux VDA unterstützt wird.

> **Hinweis:**
>
> Um Kerberos zu verwenden, müssen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver erstellen und ihn mit dem Active Directory-Konto des Proxys verknüpfen. Der VDA generiert den Dienstprinzipalnamen (SPN) im Format `HTTP/<proxyURL>` beim Einrichten einer Sitzung, wobei die Proxy-URL aus der Richtlinieneinstellung **Rendezvousproxy** abgerufen wird. Wenn Sie keinen Dienstprinzipalnamen erstellen, schlägt die Authentifizierung fehl.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Bei Verwendung eines SOCKS5-Proxy müssen Sie eine Ausnahme konfigurieren, damit Datenverkehr an die in den Anforderungen angegebenen Gateway Service-Adressen die Authentifizierung umgehen kann.
- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Verwenden Sie für einen HTTP-Proxy TCP als Transportprotokoll für ICA.

Transparenter Proxy

Rendezvous-Verbindungen über transparente HTTP-Proxys werden unterstützt. Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist auf dem VDA keine zusätzliche Konfiguration erforderlich.

Nicht transparenter Proxy

Wenn Sie einen nicht transparenten Proxy in Ihrem Netzwerk verwenden, konfigurieren Sie die Einstellung Rendezvousproxykonfiguration. Wenn die Einstellung aktiviert ist, geben Sie die HTTP- oder SOCKS5-Proxyadresse an, damit der VDA weiß, welcher Proxy zu verwenden ist. Beispiel:

- Proxyadresse: `http://<URL or IP>:<port>` oder `socks5://<URL or IP>:<port>`

Rendezvous-Validierung

Wenn alle Anforderungen erfüllt sind, überprüfen Sie folgendermaßen, ob Rendezvous verwendet wird:

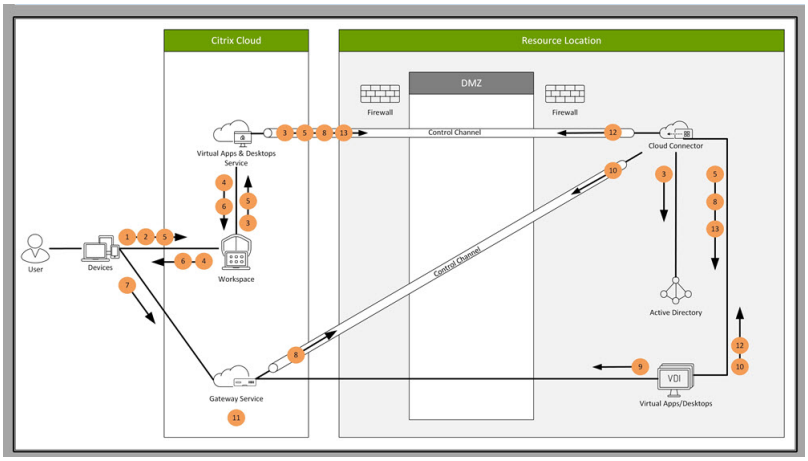
1. Starten Sie ein Terminal auf dem VDA.
2. Führen Sie `/opt/Citrix/VDA/bin/ctxquery -f iP` aus.
3. Die verwendeten TRANSPORTPROTOKOLLE geben die Art der Verbindung an:

- TCP-Rendezvous: TCP - TLS - CGP - ICA
- EDT-Rendezvous: UDP - DTLS - CGP - ICA
- Proxy über Cloud Connector: TCP - PROXY - SSL - CGP - ICA oder UDP - PROXY - DTLS - CGP - ICA

> **Tipp:**
>
> Wenn der VDA bei aktiviertem Rendezvous den Citrix Gateway Service nicht direkt erreichen kann, greift der VDA auf eine Proxyumleitung der HDX-Sitzung über den Cloud Connector zurück.

Funktionsweise von Rendezvous

Diese Abbildung bietet eine Übersicht über den Rendezvous-Verbindungsfluss.



Folgen Sie den Schritten, um den Fluss zu verstehen.

1. Navigieren Sie zu Citrix Workspace.
2. Geben Sie die Anmeldeinformationen in Citrix Workspace ein.
3. Wenn Sie Active Directory on-premises verwenden, authentifiziert Citrix DaaS die Anmeldeinformationen mit Active Directory über den Cloud Connector-Kanal.
4. Citrix Workspace zeigt enumerierte Ressourcen aus Citrix DaaS an.
5. Wählen Sie Ressourcen aus Citrix Workspace aus. Citrix DaaS sendet eine Nachricht an den VDA zur Vorbereitung auf eine eingehende Sitzung.
6. Citrix Workspace sendet eine ICA-Datei an den Endpunkt, der ein von Citrix Cloud generiertes STA-Ticket enthält.
7. Der Endpunkt stellt eine Verbindung mit Citrix Gateway Service her und stellt das Ticket zur Verbindung mit dem VDA bereit. Citrix Cloud validiert das Ticket.
8. Citrix Gateway Service sendet Verbindungsinformationen an den Cloud Connector. Der Cloud Connector bestimmt, ob die Verbindung eine Rendezvous-Verbindung ist, und sendet die Informationen an den VDA.
9. Der VDA stellt eine direkte Verbindung zu Citrix Gateway Service her.

10. Wenn eine direkte Verbindung zwischen VDA und Citrix Gateway Service nicht möglich ist, erstellt der VDA eine Proxyverbindung über den Cloud Connector.
11. Citrix Gateway Service stellt eine Verbindung zwischen Endpunktgerät und VDA her.
12. Der VDA überprüft seine Lizenz mit Citrix DaaS über den Cloud Connector.
13. Citrix DaaS sendet Sitzungsrichtlinien über den Cloud Connector an den VDA. Diese Richtlinien werden angewendet.

Rendezvous V2

January 8, 2024

Wenn Sie Citrix Gateway Service verwenden, ermöglicht das Rendezvous-Protokoll die Citrix Cloud Connectors zu umgehen, um eine direkte und sichere Verbindung mit der Citrix Cloud-Steuerebene herzustellen.

Es sind zwei Arten von Datenverkehr zu berücksichtigen: 1) Steuerungsdatenverkehr für die VDA-Registrierung und die Sitzungsvermittlung; 2) HDX-Sitzungsdatenverkehr.

Rendezvous V1 ermöglicht es, dass HDX-Sitzungsdatenverkehr Cloud Connectors umgeht. Cloud Connectors sind jedoch weiterhin erforderlich, um als Proxy für den gesamten Steuerungsdatenverkehr für die VDA-Registrierung und das Sitzungsbrokering zu fungieren.

Für reguläre mit AD-Domänen verbundene Maschinen und für nicht mit Domänen verbundene Maschinen wird Rendezvous V2 mit Einzelsitzungs- und Multisitzungs-Linux-VDAs unterstützt. Bei Maschinen, die nicht mit der Domäne verbunden sind, ermöglicht Rendezvous V2 sowohl dem HDX-Datenverkehr als auch dem Steuerungsdatenverkehr die Cloud Connectors zu umgehen.

Anforderungen

Anforderungen für die Verwendung von Rendezvous V2:

- Zugriff auf die Umgebung mit Citrix Workspace und Citrix Gateway Service.
- Steuerungsebene: Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- VDA Version 2201 oder höher.
  - Version 2204 ist die erforderliche Mindestversion für HTTP- und SOCKS5-Proxys.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix Richtlinie. Weitere Informationen finden Sie unter Richtlinieneinstellung für Rendezvous-Protokoll.
- Die VDAs müssen Zugriff auf `https://*.nssvc.net` einschließlich aller Unterdomänen haben. Wenn Sie nicht alle Unterdomänen auf diese Weise auf die Positivliste setzen können,

verwenden Sie stattdessen `https://*.c.nssvc.net` und `https://*.g.nssvc.net`. Weitere Informationen finden Sie im Abschnitt Anforderungen an die Internetkonnektivität der Citrix Cloud-Dokumentation (unter "Virtual Apps and Desktops Service") und im Knowledge Center-Artikel CTX270584.

- Die VDAs müssen eine Verbindung zu den zuvor genannten Adressen herstellen können:
  - An TCP 443 für TCP Rendezvous.
  - An UDP 443 für EDT Rendezvous.

Proxykonfiguration

Der VDA unterstützt die Verbindung über Proxys für Steuerungsverkehr und HDX-Sitzungsverkehr bei Verwendung von Rendezvous. Die Anforderungen und Richtlinien für beide Arten von Datenverkehr sind unterschiedlich. Überprüfen Sie sie daher sorgfältig.

Richtlinien für Proxys für den Steuerungsverkehr

- Es werden nur HTTP-Proxys unterstützt.
- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der Steuerungsdatenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder überprüft wird. Andernfalls schlägt die Verbindung fehl.
- Proxyauthentifizierung wird nicht unterstützt.
- Um einen Proxy zur Steuerung des Datenverkehrs zu konfigurieren, bearbeiten Sie die Registrierung wie folgt:

```
1  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
       VirtualDesktopAgent" -t "REG_SZ" -v "ProxySettings" -d "http
       ://<URL or IP>:<port>" --force
2  <!--NeedCopy-->
```

Richtlinien für Proxys für den HDX-Datenverkehr

- HTTP- und SOCKS5-Proxys werden unterstützt.
- EDT kann nur mit SOCKS5-Proxys verwendet werden.
- Um einen Proxy für den HDX-Datenverkehr zu konfigurieren, wählen Sie die Richtlinieneinstellung Rendezvous-Proxykonfiguration.

- Die Entschlüsselung und Inspektion von Paketen wird nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der HDX-Datenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder überprüft wird. Andernfalls schlägt die Verbindung fehl.
- HTTP-Proxys unterstützen die maschinenbasierte Authentifizierung über Aushandlungs- und Kerberos-Authentifizierungsprotokolle. Wenn Sie eine Verbindung mit dem Proxyserver herstellen, wählt das Aushandlungsauthentifizierungsschema automatisch das Kerberos-Protokoll aus. Kerberos ist das einzige Schema, das vom Linux VDA unterstützt wird.

  > **Hinweis:**
  >
  > Um Kerberos zu verwenden, müssen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver erstellen und ihn mit dem Active Directory-Konto des Proxys verknüpfen. Der VDA generiert den Dienstprinzipalnamen (SPN) im Format `HTTP/<proxyURL>` beim Einrichten einer Sitzung, wobei die Proxy-URL aus der Richtlinieneinstellung **Rendezvousproxy** abgerufen wird. Wenn Sie keinen Dienstprinzipalnamen erstellen, schlägt die Authentifizierung fehl.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Bei Verwendung eines SOCKS5-Proxy müssen Sie eine Ausnahme konfigurieren, damit Datenverkehr an die in den Anforderungen angegebenen Gateway Service-Adressen die Authentifizierung umgehen kann.
- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Verwenden Sie für einen HTTP-Proxy TCP als Transportprotokoll für ICA.

Transparenter Proxy

Rendezvous-Verbindungen über transparente HTTP-Proxys werden unterstützt. Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist auf dem VDA keine zusätzliche Konfiguration erforderlich.

Konfigurieren von Rendezvous V2

Im Folgenden werden die Schritte zum Konfigurieren von Rendezvous aufgeführt:

1. Achten Sie darauf, dass alle Anforderungen erfüllt sind.
2. Nachdem der VDA installiert wurde, führen Sie den folgenden Befehl aus, um den erforderlichen Registrierungsschlüssel festzulegen:


```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
   VirtualDesktopAgent" -t "REG_DWORD" -v "GctRegistration" -d "0
   x00000001" --force
<!--NeedCopy-->
```

3. Starten Sie die VDA-Maschine neu.
4. Erstellen Sie eine Citrix Richtlinie oder bearbeiten Sie eine vorhandene:
   - Legen Sie die Einstellung Rendezvous-Protokoll auf **Zugelassen** fest.
   - Stellen Sie sicher, dass die Citrix Richtlinienfilter richtig eingestellt sind. Die Richtlinie gilt für die Maschinen, für die Rendezvous aktiviert sein muss.
   - Stellen Sie sicher, dass die Citrix Richtlinie die richtige Priorität hat, damit sie keine weitere außer Kraft setzt.

Rendezvous-Validierung

Um zu überprüfen, ob eine Sitzung das Rendezvous-Protokoll verwendet, führen Sie den Befehl `/opt/Citrix/VDA/bin/ctxquery -f iP` im Terminal aus.

Die angezeigten Transportprotokolle geben die Art der Verbindung an:

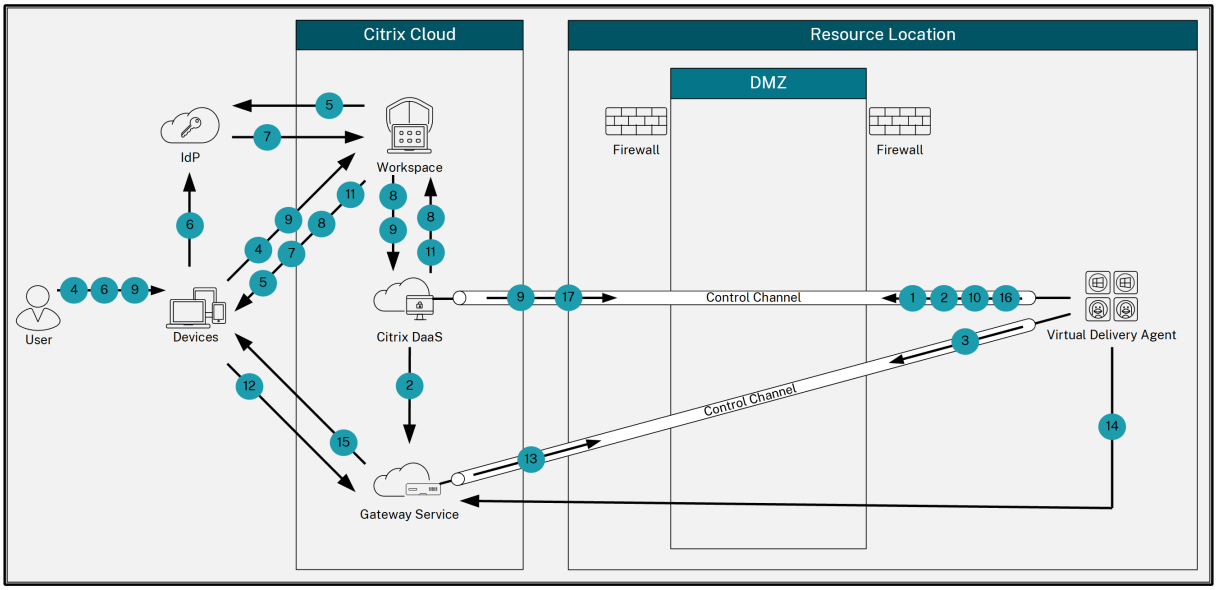
- TCP-Rendezvous: TCP - TLS - CGP - ICA
- EDT-Rendezvous: UDP - DTLS - CGP - ICA
- Proxy über Cloud Connector: TCP - PROXY - SSL - CGP - ICA oder UDP - PROXY - DTLS - CGP - ICA

Wenn Rendezvous V2 verwendet wird, wird für die Protokollversion 2.0 angezeigt.

> **Tipp:**
>
> Wenn der VDA bei aktiviertem Rendezvous den Citrix Gateway Service nicht direkt erreichen kann, greift der VDA auf eine Proxyumleitung der HDX-Sitzung über den Cloud Connector zurück.

Rendezvous-Verkehrsfluss

Das folgende Diagramm zeigt die Abfolge der Schritte zum Rendezvous-Verkehrsfluss.



1. Der VDA stellt eine WebSocket-Verbindung mit Citrix Cloud her und registriert sich.
2. Der VDA registriert sich beim Citrix Gateway Service und erhält einen dedizierten Token.
3. Der VDA stellt eine persistente Steuerungsverbindung mit Gateway Service her.
4. Der Benutzer navigiert zu Citrix Workspace.
5. Workspace wertet die Authentifizierungskonfiguration aus und leitet Benutzer zur Authentifizierung an den entsprechenden IdP weiter.
6. Der Benutzer gibt die Anmeldeinformationen ein.
7. Nach erfolgreicher Überprüfung der Benutzeranmeldeinformationen wird der Benutzer zu Workspace umgeleitet.
8. Workspace zählt Ressourcen für den Benutzer und zeigt sie an.
9. Der Benutzer wählt einen Desktop oder eine Anwendung in Workspace aus. Workspace sendet die Anfrage an Citrix DaaS, das die Verbindung vermittelt und den VDA anweist, sich auf die Sitzung vorzubereiten.
10. Der VDA reagiert mit der Rendezvous-Funktion und seiner Identität.
11. Citrix DaaS generiert ein Startticket und sendet es über Workspace an das Benutzergerät.
12. Der Endpunkt des Benutzers stellt eine Verbindung zu Gateway Service her und stellt das Startticket zur Authentifizierung und Identifizierung der Ressource bereit, mit der eine Verbindung hergestellt werden soll.
13. Gateway Service sendet die Verbindungsinformationen an den VDA.
14. Der VDA stellt für die Sitzung eine direkte Verbindung mit Gateway Service her.
15. Gateway Service stellt die Verbindung zwischen dem Endpunkt und dem VDA her.
16. Der VDA überprüft die Lizenzierung für die Sitzung.
17. Citrix DaaS sendet die entsprechenden Richtlinien an den VDA.

Sichere Benutzersitzungen mit DTLS

January 8, 2024

Die DTLS-Verschlüsselung ist ab Release 7.18 ein vollständig unterstütztes Feature. Dieses Feature ist standardmäßig im Linux VDA aktiviert. Weitere Informationen finden Sie unter TLS (Transport Layer Security).

Aktivieren der DTLS-Verschlüsselung

Überprüfen der Aktivierung des adaptiven Transports

Vergewissern Sie sich in Citrix Studio, dass die Richtlinie **Adaptiver HDX-Transport** auf den Modus **Bevorzugt** oder **Diagnose** festgelegt ist.

Aktivieren der SSL-Verschlüsselung auf dem Linux VDA

Verwenden Sie auf dem Linux VDA das Tool **enable_vdassl.sh** im Verzeichnis **/opt/Citrix/VDA/sbin**, um die SSL-Verschlüsselung zu aktivieren oder zu deaktivieren. Informationen zu den Optionen des Tools können Sie über den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh –h` aufrufen.

> **Hinweis:**
>
> Der Linux VDA unterstützt sowohl DTLS 1.0 als auch DTLS 1.2 und verwendet standardmäßig DTLS 1.2. Prüfen Sie, welche Version von DTLS in Ihrer Citrix Workspace-App verwendet wird. Stellen Sie sicher, dass dieselbe Version von DTLS sowohl auf dem Linux VDA als auch auf Ihrer Citrix Workspace-App verwendet wird. Wenn Ihre Citrix Workspace-App nur DTLS 1.0 unterstützt (z. B. Citrix Receiver für Windows 4.11), setzen Sie **SSLMinVersion** auf **TLS_1.0** und **SSLCipherSuite** auf **COM** oder **ALL**, indem Sie das Tool **enable_vdassl.sh** verwenden.

Sichere Benutzersitzungen mit TLS

January 8, 2024

Ab Version 7.16 unterstützt der Linux VDA die TLS-Verschlüsselung für sichere Benutzersitzungen. Die TLS-Verschlüsselung ist standardmäßig deaktiviert.

TLS-Verschlüsselung aktivieren

Zum Aktivieren der TLS-Verschlüsselung für sichere Benutzersitzungen installieren Sie Zertifikate und aktivieren Sie die TLS-Verschlüsselung auf Linux VDA und auf dem Delivery Controller (dem Controller).

Installieren von Zertifikaten auf dem Linux VDA

Beschaffen Sie Serverzertifikate im PEM-Format und Stammzertifikate im CRT-Format. Serverzertifikate enthalten die folgenden Abschnitte:

- Zertifikat
- Nicht verschlüsselter privater Schlüssel
- Zwischenzertifikate (optional)

Ein Beispiel eines Serverzertifikats:


```
-----BEGIN CERTIFICATE-----
MIIDTTCCAragAwIBAgIJALluncpiqGXCMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNTk1M1oXDTI4MDkyNTEwNTk1M1owgYoxCzAJBgNVBAYTAlVL
MRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEUMBIGA1UE
ChMLQ2l0cml4IFRlc3QxGzAZBgNVBAsTElNlcnZlciBDZXJ0aWZpY2F0ZTEgMB4G
A1UEAxMXY2EwMDEtc2MwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALCTTOdxcivbIOLOF66xgO5gkNeIGKVP+37pSKV8B66lWCVzr6p9
t72Fa+9oCcf2x/ue274NXFcg4fqGRDsrEwl3YxM6COyBf7L6psrsCDNnBPlq8TJH
4xoPIXUeaW4MVk/3PVyfhHKs4fz8yy1I4VDnXVHhw+OFQ2Bq3NhwsRhnAgMBAAGj
gdwwgdkwCQYDVR0TBAIwADAdBgNVHQ4EFgQUrLidzYot+CUXSh9xMfp1M+/O8yOw
gZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQwGsKha6RpMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
ggkAy8nC8dcB32EwEQYJYIZIAYb4QgEBBAQDAgVgMA0GCSqGSIb3DQEBBQUAA4GB
AD5axBYHwIxJCJzNt2zdXnbp2O0yUToWElBwQe/9cGaP6CpjoxJ7FJa2/8IpaT68
Vel8u1SEYY1GKCGCw93pc7sPKqb8pGBRI5/dygb+geFk1Q7KyVbuOIjOtr3pkxAe
b6CFJtNLudHUrwF6lOrB72zbyz3PiIx+HEwt1jOj8z4K
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCwk0zncXIr2yNC9BeusYDuYJDXiBilT/t+6UilfAeupVglc6+q
fbe9hWvvaAnH9sf7ntu+DVxXIOH6hkQ7KxMNd2MTOgjsgX+y+qbK7AgzZwT9avEy
R+MaDyFlHmluDFZP9z1cn4RyrOH8/MstSOFQ511R4cPtBUNgatzYcLEYZwIDAQAB
AoGBAKwBgZu/bkl8edgB8YPyU7diiBX89IOs4b/aPjM+JDmjxb8N96RsPO24p9Ea
FtUc9+iL8mEroLUbSicCXjsJFc+cxg9vVaNa6EEkkBj735oCUERqSxOYb/lAdck/
FXzU0tqytUe/KHgcSgjtjrSeqLJqMm+yxzBAatVRTTzGdwAhAkEA3l1kRZjIN5uz
Enmi2RTI3ngBhBP/S3GEbvJfKsD5n2Ri9O+OoEPxclvvp5ne8QOzUpshbjFEPbOC
ykZ6UassFwJBAMtI5yPnV9ewPzJoaNjZIJcMtNXDchSlxXiJiyzv+Qmr8RuQz9Pv
fIenmTrfZ+Wo4DaKg+8ar2OvOnKFOHFAmDECQQDEWRlH6cE3WyCfN1u942M9XkhR
GvSpR7+b///vL6Nwwv3CwPV9n8DTpL+wuDkJZ9nCvRteil9MlaMTYjs3alNvAkEA
qy5JzZcbBnrYzMbVO32jju7ZPISnhTGO1xDjzMSLLpTGpNLN34b0k3sTclr8L42E
uQjtTqRm+wdsrVF3lFazkQJANudmsUVv3gZKhMGaV2hzIdXIfHyOIYv+3leZhQY6
h5eEmxSZS5OTvyNGt2e6m2ZgaZmjTagH59TCBHvR5nof2g==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDGTCCAoKgAwIBAgIJAMvJwvHXAd9hMA0GCSqGSIb3DQEBBQUAMGcxCzAJBgNV
BAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNVBAcTCUNhbWJvdXJuZTEU
MBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNhMDAxLmNpdHJpdGUubmV0
MB4XDTA4MDkzMDEwNDExMVoXDTI4MDkyNTEwNDExMVowZzELMAkGA1UEBhMCVUsx
EjAQBgNVBAgTCUNhbWJyaWRnZTESMBAGA1UEBxMJQ2FtYm9lcmSlMRQwEgYDVQQK
EwtDaXRyaXggVGVzdDEaMBgGA1UEAxMRY2EwMDEuY2l0cml0ZS5uZXQwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKVZmF7Uj7uOnvO3QwdfiOnr3QkNH2DXpWrZ
Zh8cI9Vv+UFRUiC6oB7izLtBMFn3fOUP7i2CfkHN3ZGJ17p89pdyjket1MslVeJw
acOqrYvD+fNNSvJjunTbaCywVtALjmFSfMHeZJXVSckrpEhnk0nkMS16tcrya/K/
osSlzvI3AgMBAAGjgcwwgckwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQU85kN1EPJ
OcVhcOss1slseDQwGsIwgZkGA1UdIwSBkTCBjoAU85kN1EPJOcVhcOss1slseDQw
GsKha6RpMGcxCzAJBgNVBAYTAlVLMRIwEAYDVQQIEwlDYW1icmlkZ2UxEjAQBgNV
BAcTCUNhbWJvdXJuZTEUMBIGA1UEChMLQ2l0cml4IFRlc3QxGjAYBgNVBAMTEWNh
MDAxLmNpdHJpdGUubmV0ggkAy8nC8dcB32EwDQYJKoZIhvcNAQEFBQADgYEAIZ4Z
gXLLXf12RNqh/awtSbd41Ugv8BIKAsg5zhNAiTiXbzz8Cl3ec53Fb6nigMWc5Tli
UNCLXwnxRUiD4O0tESLX9ACUNH3I94yxOgujkSOSBni21jjZTvfBB32Rmr5DByJg
UmKORn/hdqMlcqpe5wO6as6+HN4WUOi+hEtUMME=
-----END CERTIFICATE-----
```


TLS-Verschlüsselung aktivieren

Aktivieren der TLS-Verschlüsselung auf dem Linux VDA Verwenden Sie auf dem Linux VDA das Skript `enable_vdassl.sh` im Verzeichnis **/opt/Citrix/VDA/sbin**, um die TLS-Verschlüsselung zu aktivieren (oder zu deaktivieren). Informationen zu den Optionen des Skripts können Sie über den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help` aufrufen.

```
root@lxu1804:~# /opt/Citrix/VDA/sbin/enable_vdassl.sh
===Enable/Disable SSL on Linux VDA===
To enable SSL, a certificate file must be specified, otherwise the local certificate file under
/etc/xdl/.sslkeystore/ is used, If the local certificate file does not exist, the command
fails. You can specify the SSL port number, version and cipher suite, otherwise, their default
values are used!

Usage: enable_vdassl.sh -Disable
       Disable Linux VDA SSL.

Usage: enable_vdassl.sh -Enable [-Certificate <CERT-FILE>] [-SSLPort <SSL-PORT-NUMBER>]
       [-SSLMinVersion <SSL-MIN-VERSION>] [-SSLCipherSuite <SSL-CIPHER-SUITE>]
       Enable Linux VDA SSL.

Options:
       -Certificate <CERT-FILE>
       Specify a certificate file, where <CERT-FILE> must include the full file path. Only one format
       is currently supported, that is PEM.

       -RootCertificate <ROOT-CERT-FILE>
       Specify a root certificate file, where <ROOT-CERT-FILE> must include the full file path, The root certificate will be put in the local keystore(under /etc/xdl/.sslkeystore/cacerts).

       -SSLPort <SSL-PORT-NUMBER>
       Specify an SSL port number. Unless otherwise specified, the default port 443 used.

       -SSLMinVersion <TLS_1.0|TLS_1.1|TLS_1.2|TLS_1.3>
       Specify SSL version. Unless otherwise specified, the default value TLS_1.2 is used.

       -SSLCipherSuite <GOV|COM|ALL>
       Specify an SSL Cipher suite. Unless otherwise specified, the default value GOV is used.

Examples:
       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem"
       Enable Linux VDA SSL using Certificate cert001.pem.

       enable-vdassl.sh -Enable -RootCertificate "/home/rootCR.cer"
       Enable Linux VDA SSL using Root Certificate rootCR.cer with local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -SSLPort 445
       Enable Linux VDA SSL on port 445 using local certificate(under /etc/xdl/.sslkeystore).

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445
       Enable Linux VDA SSL using Certificate cert001.pem on port 445, with default SSLMinVersion and SSLCipherSuite.

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and default SSLCipherSuite..

       enable-vdassl.sh -Enable -Certificate "/home/cert001.pem" -SSLPort 445 -SSLMinVersion "TLS_1.2" -SSLCipherSuite "GOV"
       Enable Linux VDA SSL using Certificate cert001.pem on port 445 with SSLMinVersion TLS_1.2 and SSLCipherSuite GOV.
```

Tipp: Auf jedem Linux VDA-Server muss ein Serverzertifikat installiert sein und auf jedem Linux VDA-Server und -Client müssen Stammzertifikate installiert sein.

Enable TLS encryption on the Controller

> **Hinweis:**
>
> Sie können die TLS-Verschlüsselung nur für ganze Bereitstellungsgruppen aktivieren. Für einzelne Anwendungen können Sie die TLS-Verschlüsselung nicht aktivieren.

Führen Sie in einem PowerShell-Fenster auf dem Controller die folgenden Befehle nacheinander aus, um die TLS-Verschlüsselung für die gewünschte Bereitstellungsgruppe zu aktivieren.

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME'| Set-BrokerAccessPolicyRule –HdxSslEnabled $true`

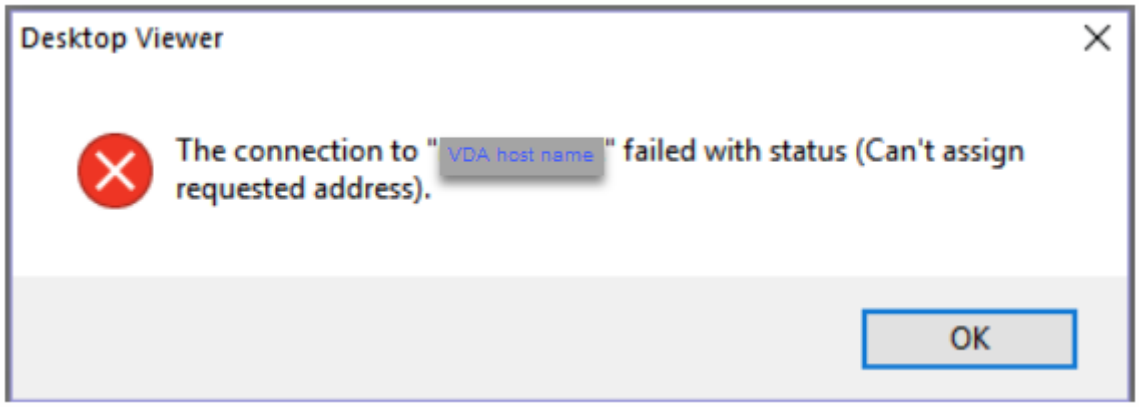
> **Hinweis:**
>
> Um sicherzustellen, dass nur VDA-FQDNs in einer ICA-Sitzungsdatei enthalten sind, können Sie auch den Befehl `Set-BrokerSite –DnsResolutionEnabled $true` ausführen. Der Befehl aktiviert die DNS-Auflösung. Wenn Sie die DNS-Auflösung deaktivieren, legt eine ICA-Sitzungsdatei VDA-IP-Adressen offen und stellt FQDNs nur für TLS-bezogene Elemente wie `SSLProxyHost` und `UDPDTLSPort` bereit.

Zum Deaktivieren der TLS-Verschlüsselung auf dem Controller führen Sie die folgenden Befehle nacheinander aus:

1. `Add-PSSnapin citrix.*`
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME'| Set-BrokerAccessPolicyRule –HdxSslEnabled $false`
3. `Set-BrokerSite –DnsResolutionEnabled $false`

Problembehandlung

Der folgende Fehler “Angeforderte Adresse kann nicht zugewiesen werden”kann in Citrix Workspace-App für Windows auftreten, wenn Sie versuchen, auf eine veröffentlichte Desktopsitzung zuzugreifen:



Fügen Sie als Workaround der Datei **hosts** einen Eintrag hinzu, der folgendem Beispiel folgt:

`<IP address of the Linux VDA>  <FQDN of the Linux VDA>`

Auf Windows-Computern ist die **Hosts**-Datei normalerweise unter `C:\Windows\System32\drivers\etc\hosts`.

Sitzungszuverlässigkeit

January 8, 2024

Citrix führt die Sitzungszuverlässigkeit für alle unterstützten Linux-Plattformen ein. Die Sitzungszuverlässigkeit ist standardmäßig aktiviert.

Die Sitzungszuverlässigkeit gewährleistet eine nahtlose Wiederverbindung von ICA-Sitzungen bei Netzwerkunterbrechungen. Weitere Informationen zur Sitzungszuverlässigkeit finden Sie unter Automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit.

Hinweis: Daten, die über eine Verbindung zur Sitzungszuverlässigkeit übertragen werden, sind standardmäßig im Nur-Text-Format. Aus Sicherheitsgründen empfehlen wir, die TLS-Verschlüsselung zu aktivieren. Weitere Informationen zur TLS-Verschlüsselung finden Sie unter Schützen von Benutzersitzungen mit TLS.

Konfiguration

Richtlinieneinstellungen in Citrix Studio

Sie können die folgenden Richtlinien für die Sitzungszuverlässigkeit in Citrix Studio festlegen:

- Sitzungszuverlässigkeit - Verbindungen
- Sitzungszuverlässigkeit - Timeout
- Sitzungszuverlässigkeit - Portnummer
- UI-Transparenzstufe während Wiederverbindung

Weitere Informationen finden Sie unter Richtlinieneinstellungen für die Sitzungszuverlässigkeit und Richtlinieneinstellungen für die automatische Wiederverbindung von Clients.

Hinweis: Nach dem Festlegen des Parameters **Sitzungszuverlässigkeit - Verbindungen** oder **Sitzungszuverlässigkeit - Portnummer** starten Sie erst den VDA-Service und anschließend den HDX-Service neu, damit die Einstellungen wirksam werden.

Einstellungen auf dem Linux VDA

- **Aktivieren oder Deaktivieren des TCP-Listeners der Sitzungszuverlässigkeit**

Standardmäßig ist der TCP-Listener der Sitzungszuverlässigkeit aktiviert und überwacht Port 2598. Führen Sie folgenden Befehl aus, um den Listener zu deaktivieren:


```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
    fEnableWinStation" -d "0x00000000"
<!--NeedCopy-->
```

Hinweis: Starten Sie den HDX-Service neu, damit die Einstellungen wirksam werden. Durch das Deaktivieren des TCP-Listeners wird die Sitzungszuverlässigkeit selbst nicht deaktiviert. Die Sitzungszuverlässigkeit ist weiterhin über andere Listener (z. B. SSL) verfügbar, wenn das Feature über die Richtlinie **Sitzungszuverlässigkeit - Verbindungen** aktiviert ist.

- **Sitzungszuverlässigkeit - Portnummer**

Sie können die Portnummer für die Sitzungszuverlässigkeit auch mit dem folgenden Befehl festlegen (als Beispiel dient Portnummer 2599):

```
/opt/Citrix/VDA/bin/ctxreg update -k  "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "PortNumber"
     -d  "2599"
<!--NeedCopy-->
```

Hinweis: Starten Sie den HDX-Service neu, damit die Einstellung wirksam wird. Wenn die Portnummer über die Richtlinieneinstellung in **Citrix Studio** festgelegt wurde, wird die Einstellung auf dem Linux VDA ignoriert. Stellen Sie sicher, dass die Firewall auf dem VDA so konfiguriert ist, dass Netzwerkverkehr über den festgelegten Port nicht verhindert wird.

- **Server-zu-Client-Keep-Alive-Intervall**

Keep-Alive-Meldungen werden zwischen dem Linux VDA und dem Client übertragen, wenn in einer Sitzung keine Aktivität stattfindet (keine Mausbewegung, keine Bildschirmaktualisierung o. Ä.). Die Keep-Alive-Meldungen testen, ob der Client noch antworten kann. Wenn der Client nicht antwortet, wird die Sitzung angehalten, bis der Client die Verbindung wieder herstellt. Mit dieser Einstellung geben Sie die Anzahl der Sekunden zwischen aufeinanderfolgenden Keep-Alive-Meldungen an. Standardmäßig ist diese Einstellung nicht konfiguriert. Führen Sie zum Konfigurieren folgenden Befehl aus (Beispielintervall = 10 Sekunden):

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    Citrix\XTEConfig"  -t "REG_DWORD"  -v  "CgpServerToClientKeepAlive"
     -d  "10"  --force
```

- **Client-zu-Server-Keep-Alive-Intervall**

Mit dieser Einstellung geben Sie die Anzahl der Sekunden zwischen aufeinanderfolgenden ICA-Keep-Alive-Meldungen an, die vom ICA-Client an den Linux VDA gesendet werden. Standardmäßig ist diese Einstellung nicht konfiguriert. Führen Sie zum Konfigurieren folgenden Befehl aus (Beispielintervall = 10 Sekunden):


```
/opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
   Citrix\XTEConfig"  -t "REG_DWORD"  -v  "CgpClientToServerKeepAlive"
    -d  "10"  --force
<!--NeedCopy-->
```

Problembehandlung

Nach dem Aktivieren der Sitzungszuverlässigkeit über die Richtlinieneinstellung können Sitzungen nicht gestartet werden.

Sie umgehen das Problem wie folgt:

1. Stellen Sie sicher, dass Sie nach dem Aktivieren der Sitzungszuverlässigkeit über die Richtlinieneinstellung in Citrix Studio zunächst den VDA-Service und dann den HDX-Service neu starten.
2. Prüfen Sie auf dem VDA mit folgendem Befehl, ob der TCP-Listener der Sitzungszuverlässigkeit ausgeführt wird (Beispielport = 2598):

   ```
   netstat -an | grep 2598
   <!--NeedCopy-->
   ```

   Wenn am Port für die Sitzungszuverlässigkeit kein TCP-Listener vorhanden ist, aktivieren Sie den Listener mit dem folgenden Befehl:

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k  "HKEY_LOCAL_MACHINE\SYSTEM\
      CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
      fEnableWinStation" -d "0x00000001"
   <!--NeedCopy-->
   ```

Sitzungsaufzeichnung (Preview)

January 8, 2024

Sie können auf einem Linux VDA gehostete Sitzungen aufzeichnen und wiedergeben.

> **Hinweis:**
>
> Dieses Feature ist als Preview verfügbar. Als Preview verfügbare Features sind möglicherweise nicht vollständig lokalisiert und werden für die Verwendung in Nicht-Produktionsumgebungen empfohlen. Probleme mit Preview-Features werden vom technischen Support von Citrix nicht unterstützt.

Aktivieren oder Deaktivieren der Sitzungsaufzeichnung

Um die Sitzungsaufzeichnung für einen Linux VDA zu aktivieren oder zu deaktivieren, setzen Sie **SmAudAllowed** auf **1** bzw. **0**. Sie können die folgenden Befehle verwenden:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    SmAudAllowed" -d "0x00000001" --force
<!--NeedCopy-->
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    SmAudAllowed" -d "0x00000000" --force
<!--NeedCopy-->
```

> **Hinweis:**
>
> Nachdem Sie die Sitzungsaufzeichnung auf einem Linux VDA aktiviert haben, werden Benutzer darüber informiert, dass ihre Sitzungen aufgezeichnet werden, wenn sie sich bei ihren Sitzungen anmelden.

Dateigröße für Aufzeichnungen angeben

Wenn die Größe der Aufzeichnungsdateien zunimmt, dauert ihr Download länger und die Reaktionszeit verlangsamt sich, wenn Sie mit dem Schieberegler durch die Wiedergabe navigieren. Sie können die Dateigröße durch Festlegen eines Schwellenwerts für eine Datei steuern. Wenn die Aufzeichnung dieses Limit erreicht, wird die aktuelle Datei geschlossen und es wird eine weitere Datei erstellt, um die Aufzeichnung fortzusetzen. Dies wird Rollover genannt.

Mit den folgenden Befehlen können Sie zwei Schwellenwerte für ein Rollover angeben:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    RolloverFileSizeInMB" -d "0x00000032" --force

sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD" -v "
    RolloverTimeInHours" -d "0x0000000c" --force
<!--NeedCopy-->
```

- **RolloverFileSizeInMB**. Die aktuelle Datei wird geschlossen, wenn sie die Größe erreicht, und eine neue Datei wird geöffnet. Standardmäßig erfolgt der Rollover, wenn die Größe 50 MB überschreitet. Unterstützte Werte: 10–300.
- **RolloverTimeInHours**. Wenn die Dauer erreicht ist, wird die aktuelle Datei geschlossen und eine neue Datei wird geöffnet. Standardmäßig erfolgt der Rollover nach 12 Stunden Aufzeichnung einer Sitzung. Unterstützte Werte: 1–24.

Ein Rollover erfolgt, sobald eine der beiden obigen Bedingungen erfüllt ist. Nehmen wir als Beispiel an, dass Sie 17 MB für die Dateigröße und 6 Stunden für die Dauer eingeben. Wenn die Aufzeichnung nach 3 Stunden 17 MB erreicht, schließt die Sitzungsaufzeichnung die Datei und öffnet eine neue.

Unabhängig vom eingegebenen Wert für die Dateigröße wird das Rollover frühestens nach einer Stunde durchgeführt, um das Erstellen von zu vielen kleinen Dateien zu vermeiden. Diese Regel gilt nicht, wenn die Dateigröße 300 MB übersteigt.

Speicherort für Aufzeichnungen festlegen

Aufzeichnungsdateien werden standardmäßig unter `/var/xdl/session_recordings` gespeichert. Führen Sie den folgenden Befehl aus, um einen anderen Pfad anzugeben:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\
    CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_SZ" -v "Path"
     -d "<your custom storage path>" --force
<!--NeedCopy-->
```

Sie können Aufzeichnungen auf einem lokalen Laufwerk oder einem Bereitstellungspunkt speichern, der auf einen Netzwerkpfad verweist. Konfigurieren Sie die richtigen Zugriffsberechtigungen für den von Ihnen festgelegten Speicherpfad und gewähren Sie dem Benutzer `ctxsrvr` die Schreibberechtigung für den Pfad.

Aufzeichnungen anzeigen

Zum Anzeigen von Aufzeichnungen führen Sie die folgenden Schritte aus, um den Sitzungsaufzeichnungsplayer oder den Webplayer für die Sitzungsaufzeichnung zu installieren:

1. Geben Sie die Anmeldeinformationen Ihres Citrix-Kontos an, um die Citrix Virtual Apps and Desktops-Downloadseite aufzurufen, und laden Sie die Produktdatei herunter. Entpacken Sie die Datei.
2. Doppelklicken Sie auf SessionRecordingPlayer.msi und SessionRecordingWebPlayer.msi und folgen Sie den Anweisungen, um die Installation abzuschließen.

> **Tipp:**
>
> Um den Webplayer für die Sitzungsaufzeichnung zu verwenden, installieren Sie ihn nur auf dem Sitzungsaufzeichnungsserver und stellen Sie sicher, dass die Aufzeichnungen auf dem Sitzungsaufzeichnungsserver verfügbar sind. Weitere Informationen finden Sie in der Dokumentation zur Citrix Sitzungsaufzeichnung.

Einschränkungen

- Bei virtuellen App-Sitzungen sind die Aufzeichnungsbenachrichtigungen möglicherweise nicht zentriert.

Virtual Channel SDK (Preview)

January 8, 2024

Mit dem Virtual Channel SDK für den Linux VDA können Sie serverseitige Anwendungen schreiben, die auf dem VDA ausgeführt werden. Weitere Informationen finden Sie in der Dokumentation zum Citrix Virtual Channel SDK für den Linux VDA.

Das Citrix Virtual Channel SDK für den Linux VDA ist auf der Citrix Virtual Apps and Desktops-Downloadseite zum Download verfügbar. Erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um den Linux VDA-Download auszuwählen.

> **Hinweis:**
>
> Dieses Feature ist als Preview verfügbar. Als Preview verfügbare Features sind möglicherweise nicht vollständig lokalisiert und werden für die Verwendung in Nicht-Produktionsumgebungen empfohlen. Der technische Support von Citrix bietet keine Unterstützung bei Problemen mit als Preview verfügbaren Features.

Wayland (Preview)

January 8, 2024

Der Linux VDA unterstützt das Wayland-Protokoll in GNOME unter RHEL 9.2/9.0, Rocky Linux 9.2/9.0 und Ubuntu 22.04. Die folgenden Funktionen wurden in Wayland vollständig getestet:

- Audio
- Zwischenablage
- Clientlaufwerkzuordnung (CDM)
- Drucken
- USB-Geräteumleitung

> **Hinweis:**
>
> - Dieses Feature ist als Preview verfügbar. Als Preview verfügbare Features sind möglicherweise nicht vollständig lokalisiert und werden für die Verwendung in Nicht-Produktionsumgebungen empfohlen. Probleme mit Preview-Features werden vom technischen Support von Citrix **nicht unterstützt**.
> - HDX 3D Pro wird nicht unterstützt.
> - Virtuelle Linux-App-Sitzungen werden nicht unterstützt.

Wayland aktivieren

Um Wayland zu verwenden, führen Sie den folgenden Befehl aus, um den Registrierungsschlüssel **EnableWayland** auf **1** zu setzen:

```
1 /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet\
     Control\Citrix\Wayland" -t "REG_DWORD" -v "EnableWayland" -d "0
     x00000001" --force
2 <!--NeedCopy-->
```

Die Standardeinstellung für den Registrierungsschlüssel **EnableWayland** ist **0**. Dies bedeutet, dass X11 verwendet wird.

Aktivierung von Wayland überprüfen

1. Öffnen Sie ein Terminalfenster in Linux.
2. Führen Sie den Befehl **echo $XDG_SESSION_TYPE** aus.

Wenn Wayland verwendet wird, wird '**wayland**' ausgegeben.

Einschränkungen

Bei der Verwendung von Wayland wurden folgende Einschränkungen festgestellt:

- Das Tastaturlayout des Clientgeräts ist nicht mit dem Tastaturlayout des VDAs synchronisiert.
- Das Abmelden von einer Sitzung unter RHEL 9.1/9.0 oder Rocky Linux 9.1/9.0 dauert etwa 20 Sekunden.