Linux Virtual Delivery Agent 2308

Wichtig:

Die Produktlebenszyklusstrategie für Current Releases (CR) und Long Term Service Releases (LTSR) wird in Lifecycle Milestones beschrieben.

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

Sie können virtuelle Anwendungen und Desktops basierend auf unterstützten Linux-Distributionen bereitstellen. Installieren Sie die VDA-Software auf Ihren virtuellen Linux-Maschinen (VMs), konfigurieren Sie den Delivery Controller und verwenden Sie dann Citrix Studio, um die Anwendungen und Desktops für Benutzer verfügbar zu machen.

Was ist neu

Neuerungen in 2308

Version 2308 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

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

Der Linux VDA unterstützt jetzt die folgenden Linux-Distributionen:

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

Weitere Informationen finden Sie unter Systemanforderungen.

Gemeinsame GPU-Beschleunigung auf einem Multi-Session-Linux-VDA

Sie können jetzt die gemeinsame GPU-Beschleunigung auf einem Multi-Session-Linux-VDA aktivieren, um OpenGL-3D-Anwendungen zu beschleunigen. Weitere Informationen finden Sie unter Gemeinsame GPU-Beschleunigung auf einem Multi-Session-Linux-VDA.

Spezifische Datenformate können zwischen Sitzung und Client kopiert und eingefügt werden

Sie können jetzt zulassen, dass spezifische Datenformate zwischen der VDA-Sitzung und dem Clientgerät kopiert und eingefügt werden. Diese Funktion wird durch Citrix-Richtlinien realisiert. Weitere Informationen finden Sie unter Zwischenablageumleitung.

Erweiterte Quest-Unterstützung

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 im Abschnitt **Active Directory-Integrationspakete** unter Systemanforderungen.

Server-Abruf und Client-Rendering für die Browserinhaltsumleitung

Wir haben die Browserinhaltsumleitung erweitert, um das Szenario „Server-Abruf und Client-Rendering“ zu unterstützen. In diesem Szenario kontaktiert die Citrix Workspace-App (der Client) den Webserver und ruft Inhalte über den VDA mithilfe eines virtuellen Kanals (**CTXPFWD**) ab. Diese Option ist nützlich, wenn der Client keinen Zugriff auf den Webserver hat (z. B. Thin Clients). Sie senkt den CPU- und RAM-Verbrauch auf dem VDA, aber Bandbreite wird auf dem virtuellen ICA-Kanal verbraucht. Weitere Informationen finden Sie unter Browserinhaltsumleitung.

Erweiterte EDT-Überlastungssteuerung (Vorschau)

Ein neuer Überlastungssteuerungsalgorithmus wurde eingeführt, um das Enlightened Data Transport (EDT)-Protokoll zu optimieren. Diese Implementierung ermöglicht EDT einen höheren Durchsatz und eine geringere Latenz für eine verbesserte Benutzererfahrung. Diese Funktion ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter Adaptiver Transport.

Weitere Menüelemente im Infobereich

Wir haben das System-Tray-Tool für die Bildschirmfreigabe erweitert, um mehr Menüelemente aufzunehmen. Derzeit können Sitzungsbenutzer auf das System-Tray-Symbol klicken, um auf alle folgenden Menüelemente zuzugreifen und entsprechende Aktionen auszuführen:

- Bildschirmfreigabe
- Wechsel der Desktop-Umgebung
- Schieberegler für Grafikqualität
- Echtzeit-CQI

Weitere Informationen finden Sie unter Infobereich.

Erweiterte H.265-Hardwarekodierung

Wir haben die H.265-Hardwarekodierung erweitert, um eine verlustfreie Komprimierung für den gesamten Bildschirm und einen verlustbehafteten H.265-Hardware-Codec für sich aktiv ändernde Bereiche zu ermöglichen. Weitere Informationen finden Sie unter Grafikkonfiguration und Feinabstimmung.

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

Wir haben den Umfang der einzelnen Tests und der VDA-Registrierungsstatusprüfungen, die das Linux-Tool **XDPing** durchführen kann, erweitert, um SQLite-Tests bzw. RC4-Problemprüfungen einzuschließen. Weitere Informationen finden Sie unter **XDPing**.

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

Die Verwendung von **realm** zum Beitreten einer Linux-VM zu einer Active Directory-Domäne wurde nun gründlich für Amazon Linux 2, RHEL 7.9 und CentOS 7.9 getestet. Sie können weiterhin den Befehl **net ads** verwenden, um die auf Amazon Linux 2, RHEL 7.9 und CentOS 7.9 ausgeführten Linux-VMs einer Active Directory-Domäne beizutreten.

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

Neuerungen in früheren Releases

Informationen zu neuen Features, die in den Releases enthalten sind, die nach dem 1912 LTSR bis zum 2305 CR ausgeliefert wurden, finden Sie unter Verlauf der Neuerungen.

Behobene Probleme

Der Linux Virtual Delivery Agent 2308 enthält die folgenden behobenen Probleme:

- Versuche, App-Sitzungen von einem Linux-VDA zu starten, der auf RHEL 8.x oder Rocky Linux 8.x installiert ist, schlagen fehl. Das Problem tritt auf, wenn der VDA über den System Security Services Daemon (SSSD) mit der Domäne verbunden ist und die **default_shell** in der Datei **/etc/sssd/sssd.conf** auf **/bin/csh** gesetzt ist.
- Wenn Sie die Sitzung in den Vollbildmodus versetzen, während HDX™ 3D Pro auf einem Linux-VDA aktiviert ist, kann die Sitzung unerwartet beendet werden.

Bekannte Probleme

Die folgenden Probleme wurden in dieser Version identifiziert:

- Wenn Sie über ein 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 die Citrix Workspace™-App für Mac oder die Citrix Workspace-App für Linux

verwenden, um auf dieselbe Sitzung zuzugreifen, die Sie zuvor mit einem Clientgerät mit Akku geöffnet haben.

- Wenn Sie den Linux VDA auf Version 2308 aktualisieren und ctxinstall.sh erneut ausführen, wird Ihr Home-Ordner geändert. Das Problem tritt auf, wenn der Kerberos-Realm-Name in Großbuchstaben festgelegt ist und SSSD als Domänenbeitrittsmethode verwendet wird. Um das Problem zu beheben, nehmen Sie die folgenden Änderungen an ctxinstall.sh vor:
  - Ändern Sie in der Skriptfunktion **get_realm** `realm=$(tr '[:upper:]' '[:lower:]' <<<"${CTX_EASYINSTALL_REALM}")` in `realm="${CTX_EASYINSTALL_REALM}"` und `realm=$(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"`
- Wenn HDX™ 3D Pro aktiviert ist, werden Sitzungen auf den erweiterten Monitoren schwarz angezeigt, und nur der primäre Monitor zeigt die Sitzungen korrekt an. Um das Problem zu beheben, öffnen Sie ein Terminal auf dem VDA und führen Sie bei Bedarf die folgenden Befehle aus:
  - Für zwei Monitore führen Sie aus:

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

  - Für drei Monitore führen Sie aus:

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

  - Für vier Monitore führen Sie aus:

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

- Sitzungsstartfehler treten auf, wenn die in PostgreSQL festgelegten maximalen Verbindungen nicht ausreichen, um gleichzeitige Sitzungen zu verarbeiten. Um das Problem zu umgehen,

erhöhen Sie die maximalen Verbindungen, indem Sie die Einstellung **max_connections** in der Datei **postgresql.conf** ändern.

- Die VDA-Registrierung kann aufgrund der folgenden LDAP-Ausnahme fehlschlagen, die in **/var/log/xdl/jproxy.log** ausgegeben wird:

  ```
  javax.naming.NamingException: LDAP response read timed out, timeout
  used: 10000 ms.
  ```

  Um das Problem zu umgehen, gehen Sie wie folgt vor:

  - Ändern Sie den LDAP-Timeout-Wert. Ändern Sie beispielsweise den LDAP-Timeout-Wert mit dem folgenden Befehl auf 60 s:

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

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

    ```
    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
    ```

- Microsoft hat im November 2022 die kumulativen Updates KB5019966 und KB5019964 für Windows 10 veröffentlicht. Die Updates führen zu Fehlern beim Domänenbeitritt und bei der Registrierung. Informationen zur Umgehung des Problems finden Sie im Knowledge Center-Artikel CTX474888.
- Mit dem für Kerberos zugelassenen Verschlüsselungstyp **RC4_HMAC_MD5** kann die Registrierung des Linux VDA beim Controller fehlschlagen, und die folgende Fehlermeldung wird angezeigt:

  Fehler: Fehler nicht spezifiziert auf GSS-API-Ebene (Mechanismus-Ebene: Verschlüsselungstyp RC4 mit HMAC wird nicht unterstützt/ist nicht aktiviert)

  Um dieses Problem zu beheben, deaktivieren Sie **RC4_HMAC_MD5** global in Ihrer Active Directory-Domäne (*oder speziell in einer OU*) oder erlauben Sie schwache

Verschlüsselungstypen auf dem Linux VDA. Löschen Sie danach 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.

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

a. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
b. Suchen Sie die Zieldomäne, und wählen Sie dann **Standarddomänenrichtlinie** aus.
c. Klicken Sie mit der rechten Maustaste auf **Standarddomänenrichtlinie** und wählen Sie **Bearbeiten**. Der Gruppenrichtlinienverwaltungs-Editor wird geöffnet.
d. Wählen Sie **Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen**.
e. Doppelklicken Sie auf **Netzwerksicherheit: Verschlüsselungstypen für Kerberos konfigurieren**.
f. Deaktivieren Sie die Kontrollkästchen **DES_CBC_CRC**, **DES_CBC_MD5** und **RC4_HMAC_MD5**, und wählen Sie **AES128_HMAC_SHA1**, **AES256_HMAC_SHA1** und **Zukünftige Verschlüsselungstypen** aus.

Um schwache Verschlüsselungstypen auf dem Linux VDA zuzulassen, führen Sie die folgenden Schritte aus:

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

a. Öffnen Sie die Datei /etc/krb5.conf auf dem Linux VDA.
b. Fügen Sie den folgenden Eintrag unter dem Abschnitt hinzu:

```
allow_weak_crypto= TRUE
```

- Der Linux VDA unterstützt SecureICA 1.0 für die Verschlüsselung nicht. Das Aktivieren von SecureICA 1.0 auf dem Linux VDA führt zu einem Fehler beim Starten der Sitzung.
- Während des Dateidownloads wird ein unerwartetes Fenster angezeigt. Das Fenster beeinträchtigt die Dateidownload-Funktionalität nicht und verschwindet nach einer Weile automatisch.

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

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

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

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

Dieser Befehl löscht alle Diensttickets im LSA-Cache, die vom Prinzipal des Netzwerkdienstes gehalten werden, unter dem der Citrix Broker Service ausgeführt wird. Er entfernt Diensttickets für andere VDAs und potenziell andere Dienste. Dies ist jedoch harmlos – diese Diensttickets können bei Bedarf erneut vom KDC abgerufen werden.

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

Hinweise von Drittanbietern

Linux Virtual Delivery Agent Version 2308 (PDF-Download)

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

Einstellung

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

Einstellungen und Entfernungen

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

FUNKTION	EINSTELLUNG ANGEKÜNDIGT IN	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

FUNKTION	EINSTELLUNG ANGEKÜNDIGT IN	ENTFERNT IN
Unterstützung für RHEL 6.10, CentOS 6.10	2003	2003
Unterstützung für RHEL 6.9, CentOS 6.9	1909	1909
Unterstützung für RHEL 7.5, CentOS 7.5	1903	1903
Unterstützung für RHEL 7.4, CentOS 7.4	1811	1811
Unterstützung für RHEL 6.8, CentOS 6.8	1811	1811
Unterstützung für RHEL 7.3, CentOS 7.3	7.18	7.18
Unterstützung für RHEL 6.6, CentOS 6.6	7.16	7.16
SUSE 11.4	7.16	7.16

Verlauf der Neuerungen

Dieser Artikel enthält Informationen zu neuen Funktionen, die in den Versionen enthalten sind, die nach dem 1912 LTSR bis zum 2305 CR veröffentlicht wurden.

Neuerungen in 2305

Version 2305 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für SQLite

SQLite wird jetzt vollständig unterstützt. Sie können SQLite oder PostgreSQL zur Verwendung angeben, indem Sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Weitere Informationen zum Angeben einer zu verwendenden Datenbank finden Sie in den Artikeln zur einfachen Installation und zur manuellen Installation.

> **Hinweis:**
>
> Das Linux-Tool **XDPing** führt keine SQLite-Tests durch.

Verbesserungen bei der Sitzungsanmeldung

Diese Version verbessert die Sitzungsanmeldung in den folgenden Aspekten:

- Ermöglicht Benutzern, die Sichtbarkeit von Passwörtern und PIN-Codes umzuschalten, wodurch es für Benutzer einfacher wird, falsche Eingaben zu erkennen.
- Zeigt die Anmeldebanner-Nachricht und den Authentifizierungsdialog auf separaten Bildschirmen an.
- Zeigt den Sitzungsanmeldevorgang an und erfordert Passwörter oder PIN-Codes für Sitzungswiederverbindungen in Nicht-SSO-Szenarien.
- Wenn Benutzer sich mit anderen Anmeldeinformationen bei VDA-Sitzungen anmelden als denen, die für die Anmeldung bei der Citrix Workspace™-App verwendet wurden, werden die Authentifizierungsdialoge separat angezeigt. Benutzer können leicht erkennen, wann Anmeldeinformationen fehlerhaft eingegeben wurden.
- Fügt Unterstützung für die folgenden Kombinationen von Benutzerauthentifizierungsmethoden in Nicht-SSO-Szenarien hinzu:

CITRIX WORKSPACE-APP	VDA-SITZUNG
FAS	Benutzername
FAS	Smartcard

Weitere Informationen finden Sie unter Benutzerdefinierte Hintergründe und Bannernachrichten auf Anmeldebildschirmen und Authentifizierung ohne SSO.

Weitere Registrierungsschlüssel für temporäre Home-Verzeichnis-Einstellungen verfügbar

Diese Version führt zwei weitere Registrierungsschlüssel ein, die bei den Einstellungen für temporäre Home-Verzeichnisse helfen:

- CheckUserHomeMountPoint
- CheckMountPointRetryTime

Weitere Informationen finden Sie unter Anmeldung mit einem temporären Home-Verzeichnis.

Unterstützung für Fast Identity Online (FIDO2)-Authentifizierung (Vorschau)

Sie können jetzt die FIDO2-Authentifizierung einrichten, um auf Websites zuzugreifen, die Google Chrome auf dem Linux VDA hosten. Weitere Informationen finden Sie unter FIDO2 (Vorschau).

> **Hinweis:**
>
> Diese Funktion befindet sich in der Vorschauphase. Vorschaufunktionen sind möglicherweise nicht vollständig lokalisiert und werden für die Verwendung in Nicht-Produktionsumgebungen empfohlen. Probleme, die bei Vorschaufunktionen auftreten, werden vom technischen Support von Citrix nicht unterstützt.

H.264-Unterstützung für verlustfreie Komprimierung für HDX 3D PRO

Die H.264-Unterstützung für verlustfreie Komprimierung ist jetzt für die HDX 3D PRO-Hardwarebeschleunigung durch NVIDIA-GPUs verfügbar. Weitere Informationen finden Sie unter Grafikkonfiguration und Feinabstimmung.

Erweiterte Platzhalterunterstützung für die Angabe von umzuleitenden URLs

Beim Angeben von URLs, deren Inhalt an den Client umgeleitet werden kann, können Sie jetzt den Platzhalter `*` verwenden, um alle URL-Komponenten außer dem Protokoll darzustellen. Weitere Informationen finden Sie unter Browserinhaltsumleitung.

Unterstützung für VDA-Datensicherung und -Vergleich mithilfe von XDPing

Zu Fehlerbehebungszwecken haben wir dem Tool **XDPing** ein VDA-Sicherungsmodul hinzugefügt. Mit diesem Modul können Sie die Schlüsseldaten eines VDA jederzeit sichern, z. B. die Konfiguration, die Datenbank und die binären Berechtigungsdaten. Sie können die Schlüsseldaten des VDA sichern, wenn er 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. Weitere Informationen finden Sie unter **XDPing**.

SSSD-Unterstützung für die Verwendung von MCS zur Erstellung von RHEL 8.x/9.x und Rocky Linux 8.x/9.x VDAs

Sie können jetzt den System Security Services Daemon (SSSD) verwenden, um Active Directory-Domänen beizutreten, wenn Sie MCS zur Erstellung von RHEL 8.x/9.x und Rocky Linux 8.x/9.x VDAs verwenden.

Hinweis:

Um einen aktuell ausgeführten RHEL 8.x/9.x oder Rocky Linux 8.x/9.x VDA, der über SSSD mit der Domäne verbunden ist, als Vorlagen-VM für MCS zu verwenden, stellen Sie sicher, dass:

- Der VDA manuell und nicht über die einfache Installation installiert wird. Die einfache Installation verwendet **Adcli** für RHEL 8.x/9.x und Rocky Linux 8.x/9.x, und die Kombination aus SSSD und **Adcli** wird von MCS nicht unterstützt.
- Ein Samba-Server für die Verwendung von SSSD zur AD-Authentifizierung konfiguriert ist. Weitere Informationen finden Sie im Red Hat-Artikel unter `<https://access.redhat.com/solutions/3802321>`.

Weitere Informationen finden Sie unter Linux-VDAs mit MCS erstellen.

Unterstützung für neue Linux-Streaming-Zielgeräte

Wir haben das Linux-Streaming auf die folgenden Distributionen erweitert:

- RHEL 8.7
- Rocky Linux 8.7
- SUSE 15.4

Weitere Informationen finden Sie unter Linux-VDAs mit Citrix Provisioning erstellen und Streaming von Linux-Zielgeräten in der Citrix Provisioning-Dokumentation.

Neuerungen in 2303

Version 2303 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für RHEL 9.1 und Rocky Linux 9.1

Wir haben RHEL 9.1 und Rocky Linux 9.1 als unterstützte Distributionen hinzugefügt. Weitere Informationen finden Sie unter Systemanforderungen.

Unterstützung für neue Linux-Streaming-Zielgeräte

Wir haben Linux-Streaming auf die folgenden Distributionen erweitert:

- RHEL 9.1
- RHEL 9.0
- Rocky Linux 9.1
- Rocky Linux 9.0

Weitere Informationen finden Sie unter Streaming-Linux-Zielgeräte in der Citrix Provisioning-Dokumentation.

Verbesserungen bei der einfachen Installation

Wir haben die Funktion für die einfache Installation verbessert und die Benutzerfreundlichkeit sowohl für den unbeaufsichtigten als auch für den interaktiven Modus optimiert. Hier ist eine Liste der wichtigsten Verbesserungen, die wir vorgenommen haben:

- **/opt/Citrix/VDA/sbin/ctxinstall.conf** wurde als Konfigurationsdatei für die einfache Installation hinzugefügt, um die Werte aller Umgebungsvariablen, die für GUI und ctxinstall.sh benötigt werden, festzulegen, zu speichern und zu synchronisieren.
- Validierung für Variablenkonfigurationen hinzugefügt, um die Robustheit zu verbessern.
- Befehlsoptionen zum Ausführen von ctxinstall.sh hinzugefügt. Weitere Informationen erhalten Sie mit dem Hilfebefehl **ctxinstall.sh -h**.

Weitere Informationen zur Verwendung der einfachen Installation finden Sie unter Domänenverbundene VDAs mit einfacher Installation erstellen.

XDPing-Verbesserungen

Wir haben ein Analysemodul im **XDPing**-Tool hinzugefügt, um den VDA-Registrierungsstatus zu überprüfen und zu analysieren. Um eine Überprüfung des VDA-Registrierungsstatus durchzuführen, führen Sie den Befehl **sudo /opt/Citrix/VDA/bin/xdping -a** aus.

Wir haben die **XDPing**-Testkategorien auch um Abhängigkeits-, Kerberos- und PAM-Prüfungen erweitert. Um die spezifischen Prüfungen durchzuführen, führen Sie die Befehle **sudo /opt/Citrix/VDA/bin/xdping -T dependency,kerberos,pam** aus.

Weitere Informationen finden Sie unter **XDPing**, Federated Authentication Service und Smartcards.

Neuerungen in Version 2301

Version 2301 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für RHEL 8.7, Rocky Linux 8.7 und SUSE 15.4

Wir haben RHEL 8.7, Rocky Linux 8.7 und SUSE 15.4 als unterstützte Distributionen hinzugefügt. Weitere Informationen finden Sie unter Systemanforderungen.

Hinweis:

SUSE 15.3 wird ab dieser Version nicht mehr unterstützt. Um den Linux VDA unter SUSE 15.4 auszuführen, führen Sie eine Neuinstallation des VDA durch.

Unterstützung für Wayland (Vorschau)

Der Linux VDA unterstützt jetzt Wayland in GNOME unter RHEL 9.0, Rocky Linux 9.0 und Ubuntu 22.04. Weitere Informationen finden Sie unter Wayland (Vorschau).

Hinweis:

Diese Funktion ist eine Vorschau. Vorschaufunktionen sind möglicherweise nicht vollständig lokalisiert und werden für den Einsatz in Nicht-Produktionsumgebungen empfohlen. Probleme, die bei Vorschaufunktionen auftreten, werden vom technischen Support von Citrix nicht unterstützt.

Alle Clientdrucker können jetzt einer Linux VDA-Sitzung zugeordnet werden

Bisher konnte nur der Standarddrucker eines Clientgeräts einer Linux VDA-Sitzung zugeordnet werden. Ab dieser Version können Sie alle Drucker eines Clientgeräts einer Linux VDA-Sitzung zuordnen. Weitere Informationen finden Sie unter Best Practices für den Druck und PDF-Druck.

Dynamische Clientlaufwerkszuordnung und Clientordnerumleitung

Bisher wurden Laufwerke, die nach dem Start einer Sitzung an den Client angeschlossen wurden, nicht der Sitzung zugeordnet. Um diese Laufwerke in der Sitzung zugänglich zu machen, mussten Sie die Sitzung trennen und erneut verbinden. Ab dieser Version können Laufwerke, die jederzeit während einer Sitzung an den Client angeschlossen werden, automatisch zugeordnet werden. Darüber hinaus führt diese Version die Clientordnerumleitung ein, mit der Sie einen benutzerdefinierten Teil eines lokalen Laufwerks auf dem Client dynamisch in die Sitzung umleiten können. Weitere Informationen finden Sie unter Clientlaufwerkszuordnung.

Neuerungen in 2212

Version 2212 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für RHEL 9.0 und Rocky Linux 9.0

Wir haben RHEL 9.0 und Rocky Linux 9.0 als unterstützte Distributionen hinzugefügt. Weitere Informationen finden Sie unter Systemanforderungen.

Verbesserungen bei der USB-Geräteumleitung

Wir haben die folgenden Verbesserungen für die USB-Geräteumleitung vorgenommen:

- Wir verwenden jetzt USB/IP als neuen virtuellen Host-Controller für die USB-Geräteumleitung. Da das USB/IP-Kernelmodul in den meisten Fällen mit Linux-Kernelversion 3.17 und höher veröffentlicht wird, müssen Sie das Kernelmodul standardmäßig nicht erstellen.
- Wir haben Unterstützung für USB 3.0-Ports hinzugefügt. Sie können jetzt USB 3.0-Geräte in USB 3.0-Ports auf einem Clientgerät einstecken.
- Wir haben Massenübertragungen optimiert und die Übertragungsgeschwindigkeit erhöht. Die Leistungssteigerung ist in Umgebungen mit hoher Latenz deutlicher.
- Wir haben die USB-Geräteumleitung auf weitere USB-Geräte erweitert, wie z. B. das **TD-RDF5A Transcend USB-Gerät** und das zusammengesetzte USB-Gerät **Yubico YubiKey OTP+FIDO+CCID**.

Weitere Informationen finden Sie unter USB-Geräteumleitung.

Hardwarebeschleunigung für bestimmte nicht virtualisierte GPUs von NVIDIA

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

- GPUs, die in Remote-PC-Zugriffsszenarien verwendet werden
- GPUs, die von einem Hypervisor durchgereicht werden

Damit HDX 3D Pro-Grafiken mit überragender Leistung gerendert werden können, aktivieren wir jetzt die Hardwarebeschleunigung für bestimmte nicht virtualisierte GPUs von NVIDIA. Die spezifischen nicht virtualisierten GPUs finden Sie im Abschnitt zur unterstützten Hardware der Versionshinweise für NVIDIA Linux Capture SDK.

Weitere Informationen finden Sie unter Nicht virtualisierte GPUs.

Ersetzen von pam_krb5 durch SSSD für Smartcard- und FAS-Authentifizierung

Bisher mussten Sie zur Verwendung der Smartcard- oder Federated Authentication Service (FAS)-Authentifizierung unter RHEL 8 und Rocky Linux 8 das pam_krb5-Modul manuell erstellen. Ab dieser Version ist dieser manuelle Schritt für RHEL 8- und Rocky Linux 8-Maschinen, die im VDI-Modus bereitgestellt werden, nicht mehr erforderlich. Weitere Informationen finden Sie unter Federated Authentication Service und Smartcards.

Erweiterung der Easy Install-GUI um die MCS-Konfiguration

Bisher konnten Sie MCS-Variablen nur durch Bearbeiten der Datei `/etc/xdl/mcs/mcs.conf` konfigurieren. Diese Version erweitert die Easy Install-GUI um die MCS-Konfiguration, sodass Sie MCS-Variablen auch über die GUI konfigurieren können. Nachdem Sie in der GUI auf **Bereitstellen** geklickt haben, überschreiben die in der GUI festgelegten Variablen die in der Datei `/etc/xdl/mcs/mcs.conf` festgelegten Variablen. Weitere Informationen finden Sie unter Schritt 3j: Erstellen eines Masterimages.

Unterstützung für die Aufzeichnung von Linux-Sitzungen (Vorschau)

Sie können jetzt auf einem Linux-VDA gehostete Sitzungen aufzeichnen und wiedergeben. Weitere Informationen finden Sie unter Sitzungsaufzeichnung (Vorschau).

> **Hinweis:**
>
> Diese Funktion ist eine Vorschau. Vorschaufunktionen sind möglicherweise nicht vollständig lokalisiert und werden für den Einsatz in Nicht-Produktionsumgebungen empfohlen. Probleme, die bei Vorschaufunktionen auftreten, werden vom technischen Support von Citrix nicht unterstützt.

Datenbankoptionen jetzt verfügbar (Vorschau)

Sie können jetzt zusätzlich zu PostgreSQL auch SQLite verwenden. Sie können SQLite oder PostgreSQL zur Verwendung angeben, indem Sie `/etc/xdl/db.conf` nach der Installation des Linux VDA-Pakets bearbeiten. Gehen Sie dazu wie folgt vor:

1. Führen Sie `/opt/Citrix/VDA/sbin/ctxcleanup.sh` aus. Überspringen Sie diesen Schritt, wenn es sich um eine Neuinstallation handelt.
2. Bearbeiten Sie `/etc/xdl/db.conf`, um eine zu verwendende Datenbank anzugeben.
3. Führen Sie eines der folgenden Skripte aus, je nach Installationsmethode:

- `/opt/Citrix/VDA/sbin/ctxinstall.sh` oder `/opt/Citrix/VDA/bin/easyinstall`, wenn Sie die einfache Installation verwenden
- `/opt/Citrix/VDA/sbin/ctxsetup.sh`, wenn Sie den Linux VDA manuell installieren
- `/opt/Citrix/VDA/sbin/deploymcs.sh`, wenn Sie MCS zum Erstellen von Linux-VDAs verwenden

Hinweis:

- Wir empfehlen die Verwendung von SQLite nur für den VDI-Modus.
- Bei manuellen Installationen müssen Sie SQLite und PostgreSQL manuell installieren, bevor Sie zwischen ihnen wechseln können. Bei einfacher Installation und MCS können Sie zwischen SQLite und PostgreSQL wechseln, ohne sie manuell installieren zu müssen.
- Sie können auch `/etc/xdl/db.conf` verwenden, um die Portnummer für PostgreSQL zu konfigurieren.

Weitere Informationen finden Sie in den Installationsartikeln.

Neuerungen in 2210

Version 2210 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Verbesserte GPU-Hardwarebeschleunigung für HDX™ 3D Pro

Wir haben die Effizienz der Datenübertragung zwischen der GPU und dem Linux-Systemspeicher verbessert. Außerdem haben wir die Latenz bei der 3D-Grafikwiedergabe und der Hardwarekodierung reduziert. Diese Verbesserungen optimieren die Hardware-Ressourcennutzung und steigern die Leistung der Bilder pro Sekunde (FPS) erheblich. Weitere Informationen finden Sie unter Grafikkonfiguration und Feinabstimmung.

Unterstützung von Größenbeschränkungen für Datenübertragungen über die Zwischenablage

Sie können die maximale Größe (in KB) der Zwischenablagedaten angeben, die Benutzer während eines einzelnen Kopiervorgangs zwischen einem Client und einer virtuellen Linux-Sitzung übertragen können. Verwenden Sie dazu die folgenden Richtlinieneinstellungen:

- Größe der Zwischenablageübertragung vom Client zur Sitzung begrenzen

- Größe der Zwischenablageübertragung von Sitzung zu Client begrenzen

Weitere Informationen zu den Richtlinieneinstellungen finden Sie im Abschnitt Client-Zwischenablagenumleitung der ICA-Richtlinieneinstellungen.

Informationen zu den vom Linux VDA unterstützten Richtlinieneinstellungen finden Sie unter Liste der unterstützten Richtlinien.

Unterstützung für neue Linux-Streaming-Zielgeräte

Wir haben das Linux-Streaming auf die folgenden Distributionen erweitert:

- RHEL 8.6
- Rocky Linux 8.6
- Ubuntu 22.04

Weitere Informationen finden Sie unter Streaming-Linux-Zielgeräte in der Citrix Provisioning-Dokumentation.

Verbesserung von Shell-Skripten

Wir haben Shell-Skripte wartungsfreundlicher gemacht und die folgenden Konfigurationsvorlagen von `/etc/xdl/mcs/` nach `/etc/xdl/ad_join/` verschoben:

- winbind_krb5.conf.tmpl
- winbind_smb.conf.tmpl
- sssd.conf.tmpl
- sssd_krb5.conf.tmpl
- sssd_smb.conf.tmpl
- centrify_krb5.conf.tmpl
- centrify_smb.conf.tmpl

Die einfache Installation verwendet auch die Konfigurationsvorlagen, die für die spezifischen Domänenbeitrittsmethoden relevant sind.

Neuerungen in 2209

Version 2209 des Linux VDA enthält die folgenden neuen Features und Verbesserungen:

Unterstützung für RHEL 8.6, Rocky Linux 8.6 und Ubuntu 22.04

Wir haben RHEL 8.6, Rocky Linux 8.6 und Ubuntu 22.04 als unterstützte Distributionen hinzugefügt.

Unterstützung der föderierten Authentifizierung für SSSD- und PBIS-verbundene Ubuntu- und SUSE-VDAs

Wir haben die Unterstützung des **Federated Authentication Service (FAS)** auf die folgenden VDA-Typen erweitert:

- Ubuntu-VDAs, die über SSSD und PBIS mit der Domäne verbunden sind
- SUSE-VDAs, die über SSSD mit der Domäne verbunden sind.

Sie können FAS jetzt verwenden, um Benutzer zu authentifizieren, die sich bei diesen VDAs anmelden. Weitere Informationen finden Sie unter Federated Authentication Service.

Benutzerdefinierte Desktopumgebungen durch Sitzungsbenutzer

Sitzungsbenutzer können jetzt ihre Desktopumgebungen anpassen. Um diese Funktion zu aktivieren, müssen Sie Desktopumgebungen im Voraus auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen durch Sitzungsbenutzer.

GPG-Signierung

Wir haben das Linux VDA-Paket mit GPG signiert, damit Sie die Integrität des Linux VDA-Pakets mithilfe des öffentlichen Schlüssels überprüfen können.

So erhalten Sie den öffentlichen Schlüssel:

1. Gehen Sie zur Citrix Virtual Apps and Desktops Downloadseite.
2. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. Klicken Sie auf **Komponenten**, um den öffentlichen Schlüssel zu finden und herunterzuladen.

So überprüfen Sie die Integrität des Linux VDA-Pakets mithilfe des öffentlichen Schlüssels:

- Für ein RPM-Paket importieren Sie den öffentlichen Schlüssel in die RPM-Datenbank und führen Sie die folgenden Befehle aus:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

- Für ein DEB-Paket importieren Sie den öffentlichen Schlüssel in die DEB-Datenbank und führen Sie die folgenden Befehle aus:

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

Neuerungen in 2207

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

Unterstützung für weitere Benutzerauthentifizierungsmethoden in Nicht-SSO-Szenarien

Bisher konnten sich Benutzer bei deaktiviertem Single Sign-On (SSO) mit unterschiedlichen Benutzernamen bei der Citrix Workspace-App und bei Sitzungen anmelden. Ab dieser Version können sich Benutzer mit Benutzernamen oder Smartcards anmelden. Weitere Informationen finden Sie unter Nicht-SSO-Authentifizierung.

Zusätzliche Optionen zum Konfigurieren des Sitzungswasserzeichens

Wir haben der Richtlinie **Benutzerdefinierter Wasserzeichentext** neue Optionen hinzugefügt, mit denen Sie Sitzungswasserzeichen weiter anpassen können. Sie können beispielsweise **Benutzerdefinierter Wasserzeichentext** auf **<image=Pfad zu einem PNG-Bild auf dem VDA>** festlegen, um ein PNG-Wasserzeichen zu erstellen. Weitere Informationen finden Sie unter Sitzungswasserzeichen.

KVM-Hypervisor-Unterstützung

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

Dateikopieren und -einfügen für alle unterstützten Linux-Distributionen verfügbar

Bisher war die Funktion **Dateikopieren und -einfügen** nur für Debian 10, RHEL 7.9 und Ubuntu 18.04 verfügbar. Ab dieser Version wird die Funktion auf alle vom Linux VDA unterstützten Linux-Distributionen erweitert. Weitere Informationen finden Sie unter Dateikopieren und -einfügen.

Neuerungen in Version 2206

Version 2206 des Linux VDA enthält die folgenden neuen Features und Verbesserungen:

Unterstützung für Debian 11.3

Wir haben Debian 11.3 als unterstützte Distribution hinzugefügt.

Unterstützung für Benutzerauthentifizierung mit Azure AD-Anmeldeinformationen

Der Linux VDA kann jetzt in Azure Active Directory (AD) integriert werden, um die Benutzerauthentifizierung bereitzustellen. Mit dieser Funktion können sich Benutzer mit ihren Azure AD-Anmeldeinformationen an nicht in die Domäne eingebundenen Linux-Desktops anmelden. Weitere Informationen finden Sie unter Authentifizierung mit Azure Active Directory.

Anzeige des Client-Akkustatus

Der Linux VDA kann jetzt den Akkustatus von Clientgeräten in virtuellen Desktops umleiten und anzeigen. Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Anzeige des Client-Akkustatus.

Multi-Monitor-Verbesserungen für Remote PC Access VDAs mit Nicht-vGPU-Grafikkarten

Diese Version behebt die folgenden Probleme, die auftreten, wenn Benutzer auf Remote PC Access-Sitzungen zugreifen:

- Der Monitor des Remote-PCs kann nicht ausgeschaltet werden. Das Anzeigen von Sitzungsinhalten kann ein Sicherheitsrisiko darstellen.
- Monitore können Artefakte anzeigen, wenn mehrere Monitore für den Zugriff auf Remote PC Access-Sitzungen verwendet werden.

Weitere Informationen finden Sie unter Nicht-vGPU-Grafikkarten.

Benutzerdefinierte Hintergründe und Bannermeldungen auf Anmeldebildschirmen für Sitzungen

Sie können Anmeldebildschirme für Sitzungen jetzt mit benutzerdefinierten Hintergründen und Bannermeldungen anpassen. Weitere Informationen finden Sie unter Benutzerdefinierte Hintergründe und Bannermeldungen auf Anmeldebildschirmen für Sitzungen.

Automatische DPI-Skalierung

Der Linux VDA unterstützt jetzt die automatische DPI-Skalierung. Wenn ein Benutzer einen virtuellen Desktop oder eine Anwendungssitzung öffnet, ändert sich der DPI-Wert in der Sitzung automatisch, um der DPI-Einstellung auf der Clientseite zu entsprechen. Weitere Informationen finden Sie unter Automatische DPI-Skalierung.

Schnellere LDAP-Abfragen

Zusätzlich zur Abfrage jedes LDAP-Servers im Polling-Modus kann der Linux VDA jetzt LDAP-Server in einer Multi-Domänen-Gesamtstruktur gleichzeitig abfragen. Um die schnelleren LDAP-Abfragen zu aktivieren, aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben Sie die relevante LDAP-Portnummer als 3268 an. Informationen zum Angeben von LDAP-Servern und LDAP-Ports finden Sie in der Beschreibung der Variable CTX_XDL_LDAP_LIST im Linux VDA-Installationsartikel, basierend auf Ihrer Distribution.

Benutzerdefinierter FAS-Port

Bisher war der Linux VDA fest für die Kommunikation mit FAS-Servern über Port 80 codiert. Ab dieser Version können Sie den FAS-Port auf der Linux VDA-Seite über CTX_XDL_FAS_LIST in der ctxsetup.sh anpassen. Weitere Informationen finden Sie im Installationsartikel für den Linux VDA, basierend auf Ihrer Distribution.

Neuerungen in Version 2204

Version 2204 des Linux VDA enthält die folgenden neuen Features und Verbesserungen:

Hardwarecodierung auf selektiven Codec erweitert

Die H.264-Hardwarecodierung, die zuvor nur für den gesamten Bildschirm verfügbar war, unterstützt jetzt die selektive Verwendung für sich aktiv ändernde Bereiche. Diese Funktion verlagert den CPU-Videokomprimierungsverbrauch auf die Hardware und verbessert die Bildqualität sowie die Anzahl der Bilder pro Sekunde (FPS). Informationen zum Aktivieren dieser Funktion finden Sie unter Grafikkonfiguration und Feinabstimmung.

Unterstützung für die Anmeldung mit einem temporären Home-Verzeichnis

Ab dieser Version können Sie ein temporäres Home-Verzeichnis für Fälle angeben, in denen der Bereitstellungspunkt auf dem Linux VDA fehlschlägt. Wenn ein temporäres Home-Verzeichnis angegeben ist, wird bei einem Fehler des Bereitstellungspunkts während der Sitzungsanmeldung eine Eingabeaufforderung angezeigt. Benutzerdaten werden dann im temporären Home-Verzeichnis gespeichert. Weitere Informationen finden Sie unter Anmeldung mit einem temporären Home-Verzeichnis.

SOCKS5-Proxy-Unterstützung für Rendezvous HDX-Datenverkehr

Der Linux VDA erweitert nun die SOCKS5-Proxy-Unterstützung für den Aufbau von Rendezvous-Verbindungen. Weitere Informationen finden Sie unter Rendezvous V1 und Rendezvous V2.

Transparente Proxy-Unterstützung für Rendezvous

Transparenter HTTP-Proxy wird jetzt für Rendezvous unterstützt. Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist keine zusätzliche Konfiguration auf dem VDA erforderlich.

Unterstützung für GNOME Classic-Desktop

Diese Version fügt GNOME Classic als Desktop-Option hinzu, die Sie über `CTX_XDL_DESKTOP_ENVIRONMENT` in der ctxsetup.sh angeben können. Weitere Informationen finden Sie im Installationsartikel für den Linux GNOME Classic VDA, basierend auf Ihrer Distribution.

Gruppierung von App-Taskleistenschaltflächen

Zuvor wurden alle Taskleistenschaltflächen veröffentlichter Anwendungen, die in derselben Sitzung ausgeführt wurden, zu einer einzigen Gruppe zusammengefasst. Ab dieser Version wird jede App als einzelne Taskleistenschaltfläche angezeigt, selbst wenn mehrere Fenster für eine App geöffnet sind.

Neuerungen in 2203

Version 2203 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Volle Unterstützung für Rendezvous V2

Bei Verwendung des Citrix Gateway-Dienstes ermöglicht das Rendezvous-Protokoll, dass der Datenverkehr die Citrix Cloud™ Connectors umgeht und sich direkt und sicher mit der Citrix Cloud-Steuerungsebene verbindet.

Es sind zwei Arten von Datenverkehr zu berücksichtigen: 1) Steuerdatenverkehr für die VDA-Registrierung und das Session Brokering; 2) HDX-Datenverkehr.

Rendezvous V1 ermöglicht es dem HDX-Datenverkehr, die Cloud Connectors zu umgehen, erfordert jedoch weiterhin, dass Cloud Connectors den gesamten Steuerdatenverkehr für die VDA-Registrierung und das Session Brokering als Proxy fungieren.

Standard-AD-Domänen-verbundene Maschinen und nicht-Domänen-verbundene Maschinen werden für die Verwendung von Rendezvous V2 mit Einzel-Sitzungs- und Multi-Sitzungs-Linux-

VDAs unterstützt. Bei nicht-Domänen-verbundenen Maschinen ermöglicht Rendezvous V2, dass sowohl HDX-Datenverkehr als auch Steuerdatenverkehr die Cloud Connectors umgehen.

Weitere Informationen finden Sie unter Rendezvous V2.

Easy Install GUI ist jetzt verfügbar

Zuvor konnten Sie für die Verwendung von Easy Install nur eine Befehlszeilenschnittstelle bedienen. Diese Version bietet eine Easy Install GUI, die Sie durch die folgenden Vorgänge führt:

- Überprüfen der Systemumgebung
- Abhängigkeiten installieren
- Beitreten des VDA zu einer angegebenen Domäne
- Konfigurieren der Laufzeitumgebung

Um die Easy Install GUI zu verwenden, führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktop-Umgebung Ihres VDA aus. Weitere Informationen finden Sie im Abschnitt **Interaktiver Modus** des Artikels Schnelle Installation mit Easy Install (Empfohlen).

HDX-Grafikverbesserung

Thinwire kann jetzt die Anzahl der Bilder pro Sekunde (FPS) verbessern, indem bestimmte Aufgaben parallelisiert werden, was jedoch zu einem geringfügig höheren gesamten CPU-Verbrauch führt. Diese Funktion ist standardmäßig deaktiviert. Weitere Informationen finden Sie im Abschnitt Parallele Verarbeitung des Artikels Grafiken konfigurieren.

Neuerungen in Version 2201

Version 2201 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

MATE-Desktop-Unterstützung unter SUSE 15.3 und SUSE 15.2

Sie können MATE jetzt als Standard-Desktop für SUSE 15.3- und SUSE 15.2-Sitzungen angeben. Weitere Informationen zu Desktop-Umgebungen finden Sie in den Installationsartikeln.

Sitzungsschattenfunktion auf alle unterstützten Distributionen erweitert

Die Sitzungsschattenfunktion ermöglicht Domänenadministratoren, die ICA-Sitzungen von Benutzern in einem Intranet anzuzeigen. Bisher nur für RHEL 7.x und Ubuntu 16.04 verfügbar, wurde die Funktion nun auf alle vom Linux VDA unterstützten Distributionen erweitert. Weitere Informationen finden Sie unter Sitzungen schatten.

Erstellen lokaler Benutzer mit angegebenen Attributen auf nicht in die Domäne eingebundenen VDAs

Wenn Sie eine auf einem nicht in die Domäne eingebundenen VDA gehostete Sitzung öffnen, erstellt der VDA automatisch einen lokalen Benutzer mit Standardattributen. Der VDA erstellt den lokalen Benutzer basierend auf dem Benutzernamen, den Sie für die Anmeldung bei der Citrix Workspace-App verwendet haben. Sie können jetzt Benutzerattribute wie die Benutzer-ID (UID), Gruppen-ID (GID), das Home-Verzeichnis und die Anmelde-Shell des Benutzers angeben. Weitere Informationen finden Sie unter Nicht in die Domäne eingebundene VDAs.

Unterstützung für Transport Layer Security (TLS) 1.3

Der Linux VDA unterstützt jetzt TLS 1.3. Das Skript `enable_vdassl.sh` im Verzeichnis /opt/Citrix/VDA/sbin ermöglicht Ihnen, TLS zu aktivieren und die minimale TLS-Version festzulegen. Weitere Informationen finden Sie unter Benutzersitzungen mit TLS sichern.

> **Hinweis:**
>
> Ab dieser Version müssen Sie .NET Runtime 6.0 installieren, bevor Sie den Linux VDA installieren.

Neuerungen in Version 2112

Version 2112 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für Amazon Linux 2 (Vorschau)

Wir haben Amazon Linux 2 als unterstützte Distribution hinzugefügt. Weitere Informationen finden Sie unter Systemanforderungen.

Volle Unterstützung für HDX-Bildschirmfreigabe

Die HDX-Bildschirmfreigabe wird jetzt vollständig unterstützt. Sie können den Bildschirm Ihres virtuellen Desktops mit Sitzungsbenutzern auf anderen virtuellen Desktops teilen. Die Bildschirmfreigabefunktion ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter HDX-Bildschirmfreigabe.

Rendezvous-Verbindung über einen HTTP-Proxy

Der Linux VDA unterstützt jetzt den Aufbau von Rendezvous-Verbindungen über einen HTTP-Proxy, der TCP als Transportprotokoll für ICA verwendet. Weitere Informationen finden Sie unter Rendezvous-Protokoll.

Rendezvous-Proxy-Authentifizierung

Ein in die Domäne eingebundener Linux VDA kann sich jetzt für Rendezvous-Verbindungen bei einem Proxyserver authentifizieren. Weitere Informationen finden Sie unter Rendezvous-Protokoll.

Unterstützung für adaptives Audio

Adaptives Audio ist standardmäßig aktiviert. Mit adaptivem Audio müssen Sie die Audioqualitätsrichtlinien auf dem VDA nicht manuell konfigurieren. Adaptives Audio passt die Audio-Sampling-Bitraten dynamisch an die Netzwerkbedingungen an, um ein erstklassiges Audioerlebnis zu bieten. Weitere Informationen finden Sie unter Adaptives Audio.

Unterstützung für neue Linux-Streaming-Zielgeräte

Für Linux-Streaming werden jetzt die folgenden Betriebssysteme unterstützt:

- SUSE Linux Enterprise Server 15 SP2 (SUSE 15.2)
- SUSE Linux Enterprise Server 15 SP3 (SUSE 15.3)

Weitere Informationen finden Sie unter Streaming-Linux-Zielgeräte in der Citrix Provisioning-Dokumentation.

Verbesserung der Tastaturlayout-Synchronisierung

Wenn **KeyboardLayout** in der Datei WFCLIENT.ini auf **Server Default** eingestellt ist, bleibt das zuvor ausgewählte Tastaturlayout nach der erneuten Verbindung mit einer Sitzung erhalten.

Verbesserung der Tastatureingabe

Wir haben mehrere Probleme behoben und die Unterstützung für weitere Sonderzeichen und Tastenkombinationen hinzugefügt.

Neuerungen in 2110

Version 2110 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für SUSE 15.3 und SUSE 15.2

Wir haben SUSE Linux Enterprise Server 15 SP3 (SUSE 15.3) und SUSE Linux Enterprise Server 15 SP2 (SUSE 15.2) als unterstützte Distributionen hinzugefügt. Weitere Informationen finden Sie unter Systemanforderungen.

HDX-Webcam-Videokomprimierungsunterstützung für SUSE 15.3, SUSE 15.2 und SUSE 12.5

Benutzer von Videokonferenzanwendungen, die in SUSE 15.3-, SUSE 15.2- und SUSE 12.5-Sitzungen ausgeführt werden, können ihre Webcams jetzt mit HDX-Webcam-Videokomprimierung verwenden. Weitere Informationen finden Sie unter HDX-Webcam-Videokomprimierung.

FAS-Unterstützung für MCS-erstellte VMs, die PowerBroker Identity Services (PBIS) verwenden

Sie können jetzt FAS verwenden, um Benutzer zu authentifizieren, die sich bei einem MCS-erstellten Linux VDA anmelden, der mithilfe von PBIS einer Windows-Domäne beigetreten ist. Weitere Informationen finden Sie unter Federated Authentication Service konfigurieren und FAS auf einer MCS-erstellten VM aktivieren.

Zwei Umgebungsvariablen werden zu ctxfascfg.sh hinzugefügt

Wir haben die folgenden Variablen zu ctxfascfg.sh hinzugefügt:

- CTX_FAS_KDC_HOSTNAME: Gibt den Hostnamen des Key Distribution Center (KDC) an, wenn Sie PBIS auswählen.
- CTX_FAS_PKINIT_KDC_HOSTNAME: Gibt den PKINIT KDC-Hostnamen an, der CTX_FAS_KDC_HOSTNAME entspricht, sofern nicht anders angegeben.

Weitere Informationen finden Sie unter Run ctxfascfg.sh.

Sitzungsstart mit anderen Anmeldeinformationen als denen, die für die Anmeldung bei der Citrix Workspace-App verwendet wurden

Nach der Anmeldung bei der Citrix Workspace-App können Sie andere Anmeldeinformationen verwenden, um Citrix Virtual Apps™- und Desktops-Sitzungen zu starten. Um diese Funktion zu aktivieren, führen Sie den folgenden Befehl auf Ihrem Linux VDA aus:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t
"REG_DWORD" -v "fPromptForDifferentUser" -d "0x00000001" --force
```

Wenn die Funktion aktiviert ist, werden Sie beim Starten von Sitzungen zur Eingabe von Anmeldeinformationen aufgefordert. Die Funktion wird für die folgenden Distributionen unterstützt:

- RHEL 8.4 / CentOS 8 (2105)
- RHEL 7.9 / CentOS 7.9
- Ubuntu 16.04
- Debian 10.9
- SUSE 15.3
- SUSE 15.2

Neuerungen in 2109

Version 2109 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für HDX-Bildschirmfreigabe (Vorschau)

Der Linux VDA ermöglicht es Ihnen jetzt, den Bildschirm Ihres virtuellen Desktops mit Sitzungsbenutzern auf anderen virtuellen Desktops zu teilen. Die Bildschirmfreigabefunktion ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter HDX screen sharing.

Citrix Virtual Channel Software Development Kit (SDK) für den Linux VDA (Vorschau)

Das Citrix Virtual Channel SDK für den Linux VDA ist jetzt verfügbar. Mit dem Virtual Channel SDK 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 steht auf der Downloadseite für Citrix Virtual Apps and Desktops zum Download bereit. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um den Linux VDA-Download auszuwählen.

FAS-Unterstützung für VDAs, die PBIS verwenden

Sie können FAS jetzt verwenden, um Benutzer zu authentifizieren, die sich bei einem Linux VDA anmelden, der mithilfe von PowerBroker Identity Services (PBIS) einer Windows-Domäne beigetreten ist. Wenn Sie PBIS während der Ausführung von ctxfascfg.sh auswählen, geben Sie den Hostnamen des Key Distribution Center (KDC) ein, wenn Sie vom Skript dazu aufgefordert werden. Weitere Informationen finden Sie unter Federated Authentication Service konfigurieren.

Linux-Streaming-Unterstützung für RHEL 8.4, RHEL 7.9 und SUSE 12.5

Mithilfe der Linux-Streaming-Funktion mit Citrix Provisioning können Sie virtuelle Linux-Desktops direkt in der Citrix Virtual Apps and Desktops-Umgebung bereitstellen. Weitere Informationen finden Sie unter Verwenden von Citrix Provisioning zum Erstellen von Linux-VMs.

Unterstützung der Tastaturlayout-Synchronisierung für MATE-Desktop

Wir haben die Unterstützung der Tastaturlayout-Synchronisierung auf den MATE-Desktop erweitert. Jedes Mal, wenn sich das Tastaturlayout auf Ihrem Clientgerät ändert, passt sich das Layout auf Ihrem VDA, auf dem Sie die MATE-Desktopumgebung installiert haben, entsprechend an. Weitere Informationen finden Sie unter Dynamische Tastaturlayout-Synchronisierung.

Dienstprogramm zur Abfrage von Sitzungsdaten

Wir stellen jetzt ein Dienstprogramm (`ctxsdcutil`) bereit, mit dem Sie Sitzungsdaten auf jedem Linux VDA abfragen können. Um die folgenden Daten aller Sitzungen oder einer bestimmten Sitzung, die auf einem VDA gehostet wird, abzufragen, führen Sie den Befehl `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]` aus. Das Argument `[-c]` bedeutet, Daten jede Sekunde abzufragen.

- **Eingabebandbreite der Sitzung**
- **Ausgabebandbreite der Sitzung**
- **Leitungsgeschwindigkeit der Ausgabesitzung**
- **Latenz – zuletzt aufgezeichnet**
- **Roundtripzeit**
- **Ausgabe ThinWire Bandbreite**
- **Ausgabe Audio Bandbreite**
- **Ausgabe Drucker Bandbreite**
- **Eingabe Laufwerk Bandbreite**
- **Ausgabe Laufwerk Bandbreite**

Neue Linux-Sitzungsmetriken sind verfügbar

Wir haben die folgenden Metriken hinzugefügt, damit Sie die Leistung Ihrer Linux-Sitzungen verfolgen, aggregieren und visualisieren können:

- Anmeldedauer

Die Anmeldedauer ist ein Maß für den Anmeldevorgang von dem Zeitpunkt, zu dem sich ein Benutzer über die Citrix Workspace-App verbindet, bis zu dem Zeitpunkt, zu dem eine Sitzung zur Verwendung bereit ist. Sie können diese Metrik auf der Registerkarte Monitor von Citrix DaaS anzeigen. Monitor ist als Director-Konsole verfügbar, um Citrix Virtual Apps and Desktops Current Release und LTSR Bereitstellungen zu überwachen und Fehler zu beheben.

- Anzahl der automatischen Sitzungswiederverbindungen

  Sie können jetzt die Anzahl der automatischen Wiederverbindungen in einer Linux-Sitzung über die Ansicht **Trends** von Citrix Director und Monitor anzeigen. Die automatische Wiederverbindung wird aktiviert, wenn die Richtlinien **Sitzungszuverlässigkeit** oder **Automatische Client-Wiederverbindung** wirksam sind. Weitere Informationen zu Sitzungswiederverbindungen finden Sie unter Sitzungen. Weitere Informationen zu Richtlinien finden Sie unter Richtlinieneinstellungen für die automatische Client-Wiederverbindung und Richtlinieneinstellungen für die Sitzungszuverlässigkeit.

Weitere Informationen finden Sie unter Überwachen von Linux-VMs und Linux-Sitzungen.

Neuerungen in 2107

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

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

Wir haben die Centrify-Unterstützung für das Beitreten von mit MCS erstellten RHEL 7/CentOS 7- und RHEL 8/CentOS 8-Maschinen zu Windows-Domänen hinzugefügt.

Vereinfachter Neuaufbau des Kernelmoduls für USB-Umleitung

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

Unterstützung für RHEL 8.4 und CentOS 8 (2105)

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

Smartcard-Unterstützung für Debian

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

Neuerungen in 2106

Version 2106 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Linux VDA-Selbstaktualisierung

Diese Funktion hilft, Ihre Linux VDA-Software automatisch zu aktualisieren – sofort oder zu einem geplanten Zeitpunkt. Dies ist vorteilhaft, da Sie keine Administratorrechte für die VMs in Azure haben. Weitere Informationen finden Sie unter Linux VDA-Selbstaktualisierung.

Unterstützung für Machine Creation Services™ (MCS) auf Nutanix AHV

Sie können jetzt MCS verwenden, um Linux-VMs auf Nutanix AHV zu erstellen. Weitere Informationen finden Sie unter MCS zum Erstellen von Linux-VMs auf Nutanix AHV verwenden.

PBIS-Unterstützung für das Beitreten von mit MCS erstellten Maschinen zu Windows-Domänen

Wir haben die PBIS-Unterstützung für das Beitreten von mit MCS erstellten Maschinen zu Windows-Domänen hinzugefügt. Weitere Informationen finden Sie unter Machine Creation Services (MCS) zum Erstellen von Linux-VMs verwenden.

Unterstützung für HDX-Webcam-Videokomprimierung

Benutzer von Videokonferenzanwendungen, die in Linux-VDA-Sitzungen ausgeführt werden, können ihre Webcams jetzt mit HDX-Webcam-Videokomprimierung verwenden. Die HDX-Webcam-Videokomprimierung wird auch als **optimierter** Webcam-Modus bezeichnet. Diese Art der Webcam-Videokomprimierung sendet das H.264-Video direkt an die Videokonferenzanwendung, die in der virtuellen Sitzung ausgeführt wird. Die HDX-Webcam-Videokomprimierung verwendet die Multimedia-Framework-Technologie, die Teil des Client-Betriebssystems ist, um Videos von Erfassungsgeräten abzufangen, zu transkodieren und zu komprimieren. Diese Funktion ist standardmäßig aktiviert. Wir empfehlen Ihnen, nach Möglichkeit immer die HDX-Webcam-Videokomprimierung zu verwenden. Weitere Informationen finden Sie unter HDX-Webcam-Videokomprimierung.

Schieberegler für Grafikqualität

Wir haben einen Schieberegler für die Grafikqualität in das Grafikstatusanzeige-Tool integriert, das in Ihren virtuellen Linux-Sitzungen ausgeführt wird. Der Schieberegler hilft, die richtige Balance zwischen Bildqualität und Interaktivität zu finden. Weitere Informationen finden Sie unter Schieberegler für Grafikqualität.

Unterstützung für die Auswertung von Richtlinien für bei Secure Browser angemeldete Benutzer während CGP-Sitzungswiederverbindungen

Der Linux-VDA unterstützt jetzt die Auswertung und Anwendung benutzerspezifischer Richtlinien, die Sie im Secure Browser-Dienst festlegen, während CGP-Sitzungswiederverbindungen. Die folgenden Richtlinien werden unterstützt:

- Zwischenablage
  - Client-Zwischenablagenumleitung
  - Aktualisierungsmodus für die Zwischenablageauswahl
  - Aktualisierungsmodus für die primäre Auswahl
- Drucken
  - Clientdruckerumleitung
  - PDF Universal Printer automatisch erstellen
- Dateiübertragung
  - Dateitransfer zwischen Desktop und Client zulassen
  - Datei vom Desktop herunterladen
  - Datei auf den Desktop hochladen

Linux-Streaming-Unterstützung für RHEL 8.3 und Ubuntu 18.04

Linux-Streaming für RHEL 8.3 und Ubuntu 18.04 wird jetzt vollständig unterstützt. Mit der Linux-Streaming-Funktion und Citrix Provisioning können Sie virtuelle Linux-Desktops direkt in der Citrix Virtual Apps and Desktops-Umgebung bereitstellen. Weitere Informationen finden Sie unter Citrix Provisioning zum Erstellen von Linux-VMs verwenden.

Neuerungen in 2104

Version 2104 des Linux-VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für nicht in Domänen eingebundene Linux-VDAs in Citrix DaaS™

Sie können MCS jetzt verwenden, um nicht in Domänen eingebundene Linux-VDAs in Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) zu erstellen.

OpenJDK 11 ist erforderlich

Der Linux-VDA erfordert jetzt die Anwesenheit von OpenJDK 11. Unter den vom Linux-VDA unterstützten Linux-Distributionen müssen Sie OpenJDK 11 nur unter Ubuntu 16.04 manuell installieren. Auf den anderen unterstützten Distributionen wird OpenJDK 11 bei der Installation des Linux-VDA automatisch als Abhängigkeit installiert.

XDPing-Änderungen

Das Ausführen von `ctxsetup.sh` installiert `XDPing` nicht mehr. Sie können `sudo /opt/Citrix/VDA/bin/xdping` ausführen, um `XDPing` zu installieren. Dieser Befehl erstellt auch eine virtuelle Python3-Umgebung, die für `XDPing` erforderlich ist. Weitere Informationen finden Sie unter **XDPing**.

Smartcard-Unterstützung für Ubuntu

Benutzer können eine mit dem Clientgerät verbundene Smartcard zur Authentifizierung verwenden, wenn sie sich bei einer virtuellen Linux-Desktopsitzung anmelden. Diese Version ermöglicht Ihnen außerdem die Verwendung der Smartcard-Passthrough-Authentifizierung in Ubuntu 20.04-, Ubuntu 18.04- und Ubuntu 16.04-Sitzungen. Weitere Informationen finden Sie unter Passthrough-Authentifizierung mit Smartcards.

Unterstützung für den MATE-Desktop

Wir haben die Unterstützung für den schlanken MATE-Desktop unter CentOS, RHEL, Ubuntu und Debian hinzugefügt. Sie können den MATE- oder GNOME-Desktop jetzt über eine neue Variable angeben, die in den Skripten ctxinstall.sh, ctxsetup.sh und deploymcs.sh verfügbar ist. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie diesen Variablenwert auf mate setzen. Weitere Informationen finden Sie unter Einfache Installation und in den Artikeln zur manuellen Installation, z. B. Installieren des Linux Virtual Delivery Agent für RHEL/CentOS.

PBIS-Unterstützung für RHEL 8, CentOS 8 und SUSE 12.5

Wir haben die PBIS-Unterstützung für das Beitreten von RHEL 8-, CentOS 8- und SUSE 12.5-Maschinen zu Windows-Domänen hinzugefügt.

Neuerungen in 2103

Version 2103 des Linux-VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für Debian 10.7 und CentOS 8.3

Wir haben Debian 10.7 und CentOS 8.3 als unterstützte Distributionen hinzugefügt. Weitere Informationen finden Sie unter Systemanforderungen, Installieren des Linux Virtual Delivery Agent für Debian und Installieren des Linux Virtual Delivery Agent für RHEL/CentOS.

SSSD-Unterstützung für das Beitreten von SUSE-Maschinen zu Windows-Domänen

Wir haben die SSSD-Unterstützung für das Beitreten von SUSE-Maschinen zu Windows-Domänen hinzugefügt.

Ein einziges Linux-VDA-Image für domänenverbundene und nicht domänenverbundene Anwendungsfälle

Wir stellen jetzt ein einziges Image für die Erstellung von domänenverbundenen und nicht domänenverbundenen Linux-VDAs in Citrix Virtual Apps and Desktops Standard für Azure bereit. Diese Funktion vereinfacht die Image-Vorbereitung und -Wartung. Weitere Informationen finden Sie unter Erstellen von Linux-VDAs in Citrix Virtual Apps and Desktops Standard für Azure.

Verbesserung der Dateiübertragung

Wir haben die Dateiübertragungsfunktion verbessert, indem wir die Fortschrittsanzeige neu gestaltet, die Download-Geschwindigkeit beschleunigt und einige Fehler behoben haben. Wir haben auch die Anzahl der Dateien, die Sie gleichzeitig übertragen können, von 10 auf 100 erhöht. Weitere Informationen finden Sie unter Dateiübertragung.

Unterstützung für die Konfiguration von Sitzungsverbindungs-Timern in Citrix Studio

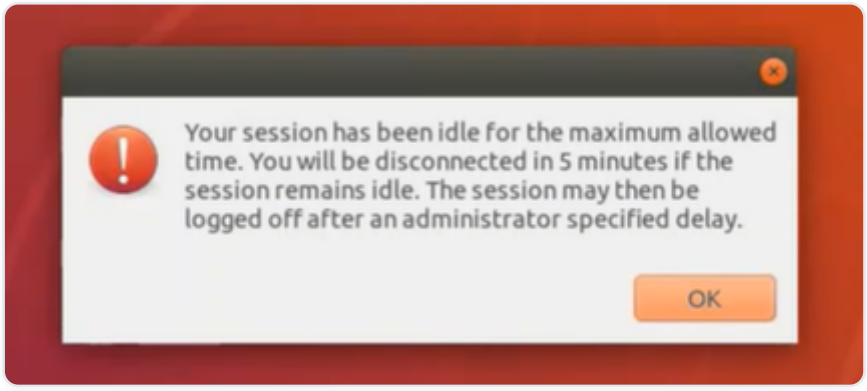
Bisher konnten Sie Zeitlimits für inaktive und getrennte Sitzungen nur über `/opt/Citrix/VDA/bin/ctxcfg` separat auf und für jeden VDA konfigurieren. Diese Version fügt die folgenden Richtlinien hinzu, mit denen Sie Sitzungsverbindungs-Timer in Citrix Studio konfigurieren können:

- **Sitzungs-Inaktivitätstimer**: Legt fest, ob ein Zeitlimit für inaktive Sitzungen erzwungen werden soll.
- **Intervall des Sitzungs-Inaktivitätstimers**: Legt ein Zeitlimit für inaktive Sitzungen fest. Wenn der **Sitzungs-Inaktivitätstimer** auf **Aktiviert** gesetzt ist und eine aktive Sitzung während der festgelegten Zeit keine Benutzereingaben erhalten hat, wird die Sitzung getrennt.

- **Timer für getrennte Sitzungen**: Legt fest, ob ein Zeitlimit für getrennte Sitzungen erzwungen werden soll.
- **Intervall des Timers für getrennte Sitzungen**: Legt ein Intervall fest, bevor eine getrennte Sitzung abgemeldet wird.

Wenn Sie Richtlinieneinstellungen aktualisieren, stellen Sie sicher, dass diese in Ihrer gesamten Bereitstellung konsistent sind. Weitere Informationen zu den Richtlinien finden Sie in der Richtlinien-Supportliste.

Eine Warnmeldung wird angezeigt, wenn Ihr Zeitlimit für inaktive Sitzungen abläuft. Ein Beispiel finden Sie im folgenden Screenshot. Durch Drücken von **OK** wird die Warnmeldung geschlossen, aber Ihre Sitzung kann dadurch nicht aktiv gehalten werden. Um Ihre Sitzung aktiv zu halten, geben Sie Benutzereingaben ein, um den Inaktivitätstimer zurückzusetzen.



Neue Metriken für Linux-VMs und Linux-Sitzungen sind in Citrix Director verfügbar

Diese Version bietet neue Metriken für Linux-VMs und Linux-Sitzungen in Citrix Director.

Neue Metrik für jede Linux-VM:

- Die Anzahl der CPU-Kerne
- Speichergröße
- Festplattenkapazität
- Aktuelle und historische CPU- und Speicherauslastung

Neue Metrik für jede Linux-Sitzung:

- Leerlaufzeit

Weitere Informationen finden Sie unter Überwachen von Linux-VMs und Linux-Sitzungen in Citrix Director.

FAS-Verbesserung für den Linux-VDA

Wir bieten jetzt aufschlussreichere Protokollausgaben und ermöglichen Ihnen, einen Pfad anzugeben, der sowohl das Stammzertifikat als auch alle Zwischenzertifikate enthält, wenn Sie das Skript ctxfascfg.sh ausführen. Konfigurationsinformationen finden Sie unter Konfigurieren des Federated Authentication Service.

Linux-Streaming-Unterstützung für RHEL 8.3 und Ubuntu 18.04.5 (Vorschau)

Mit der Linux-Streaming-Funktion und Citrix Provisioning können Sie Linux-basierte virtuelle Desktops direkt in der Citrix Virtual Apps and Desktops-Umgebung bereitstellen. Weitere Informationen finden Sie unter Linux-Streaming.

Neuerungen in 2012

Version 2012 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Enlightened Data Transport (EDT) MTU-Erkennung

EDT ermittelt automatisch die maximale Übertragungseinheit (MTU) beim Aufbau einer Sitzung. Dadurch wird eine EDT-Paketfragmentierung verhindert, die zu Leistungseinbußen oder zum Fehlschlagen des Sitzungsaufbaus führen könnte. Weitere Informationen finden Sie unter EDT MTU-Erkennung.

Unterstützung für LDAP-Kanalbindung

Zuvor konnte der Linux VDA sich nicht bei einem Delivery Controller™ registrieren, wenn die Kanalbindung in Active Directory aktiviert war. Diese Version des Linux VDA unterstützt die Kanalbindung, um die Sicherheit der Kommunikation mit den Active Directory-Domänencontrollern zu erhöhen. Stellen Sie sicher, dass Sie eine Python3-virtuelle Umgebung erstellen, bevor Sie die Kanalbindung auf dem Linux VDA aktivieren.

XDPing in den Linux VDA integriert

Das Linux-Tool **XDPing** ist eine Befehlszeilenanwendung, die den Prozess der Überprüfung auf häufige Konfigurationsprobleme in einer Linux VDA-Umgebung automatisiert. Zuvor mussten Sie **XDPing** von der Seite CTX202015 herunterladen und das Tool separat vom Linux VDA installieren. Ab dieser Version ist `XDPing` in den Linux VDA integriert und kann bei der Installation des Linux VDA automatisch installiert werden.

Unterstützung für RHEL 7.9, RHEL 8.3

Wir haben RHEL 7.9 und RHEL 8.3 als unterstützte Distributionen hinzugefügt.

Unterstützung für Ubuntu 20.04

Ubuntu 20.04 wird in dieser Version vollständig unterstützt.

Unterstützung für das Rendezvous-Protokoll

Der Linux VDA unterstützt jetzt das Rendezvous-Protokoll. In Umgebungen, die den Citrix Gateway-Dienst verwenden, ermöglicht das Rendezvous-Protokoll HDX-Sitzungen, den Citrix Cloud Connector™ zu umgehen und sich direkt und sicher mit dem Citrix Gateway-Dienst zu verbinden.

Unterstützung für Machine Creation Services (MCS) auf Google Cloud Platform (GCP)

Sie können jetzt MCS verwenden, um Linux-VMs auf GCP zu erstellen. Weitere Informationen finden Sie unter Verwenden von Machine Creation Services (MCS) zum Erstellen von Linux-VMs.

Wake on LAN für Linux-Maschinen verfügbar

Die integrierte Wake-on-LAN-Funktionalität ist jetzt für Linux-Maschinen verfügbar.

> **Hinweis:**
>
> Ab dieser Version müssen Sie .NET Core Runtime 3.1 installieren, bevor Sie den Linux VDA installieren.

Neuerungen in 2009

Version 2009 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für RHEL 8.2

Citrix hat RHEL 8.2 als unterstützte Distribution hinzugefügt.

Unterstützung für Ubuntu 20.04 (Vorschau)

Sie können den Linux VDA auf Ubuntu 20.04 verteilen.

Unterstützung für Browserinhaltsumleitung

Ab dieser Version unterstützt der Linux VDA die Browserinhaltsumleitung in Google Chrome. Die Browserinhaltsumleitung ermöglicht das Rendern von Webseiten in der Zulassungsliste auf Clientseite. Weitere Informationen finden Sie unter Browserinhaltsumleitung.

Unterstützung für Sitzungswasserzeichen

Der Linux VDA unterstützt jetzt Sitzungswasserzeichen. Sie können ein Wasserzeichen als Textebene festlegen, die über dem gesamten Sitzungsbildschirm angezeigt wird, ohne den Inhalt des Originaldokuments zu ändern. Textbasierte Sitzungswasserzeichen helfen, Datendiebstahl zu verhindern und die Nachverfolgung zu ermöglichen. Diese nachverfolgbaren Informationen werden auf dem Sitzungsdesktop angezeigt, um Personen abzuschrecken, die Fotos und Bildschirmaufnahmen verwenden, um Daten zu stehlen. Weitere Informationen finden Sie unter Sitzungswasserzeichen.

Unterstützung für nicht in die Domäne eingebundene Linux-VDAs in Citrix Virtual Apps and Desktops Standard für Azure

Sie können jetzt nicht in die Domäne eingebundene Linux-VDAs in Citrix Virtual Apps and Desktops Standard für Azure erstellen, um virtuelle Apps und Desktops von Microsoft Azure auf beliebige Geräte bereitzustellen. Weitere Informationen finden Sie unter Erstellen von Linux-VDAs in Citrix DaaS Standard für Azure und Citrix Virtual Apps and Desktops Standard für Azure.

Richtlinie verfügbar zum Festlegen der dynamischen Tastaturlayoutsynchronisierung und der Client-IME-Benutzeroberflächensynchronisierung

Bisher mussten Sie zum Aktivieren oder Deaktivieren der Funktionen für die dynamische Tastaturlayoutsynchronisierung und die Client-IME-Benutzeroberflächensynchronisierung die Registrierung auf jedem Ziel-VDA bearbeiten. Ab dieser Version können Sie die Richtlinie **Client-Tastaturlayoutsynchronisierung und IME-Verbesserung** verwenden, um die Funktionen festzulegen. Diese Richtlinie hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Maschinenobjekte oder auf alle Objekte in Ihrer Site angewendet werden. Weitere Informationen finden Sie unter Dynamische Tastaturlayoutsynchronisierung und Client-IME-Benutzeroberflächensynchronisierung.

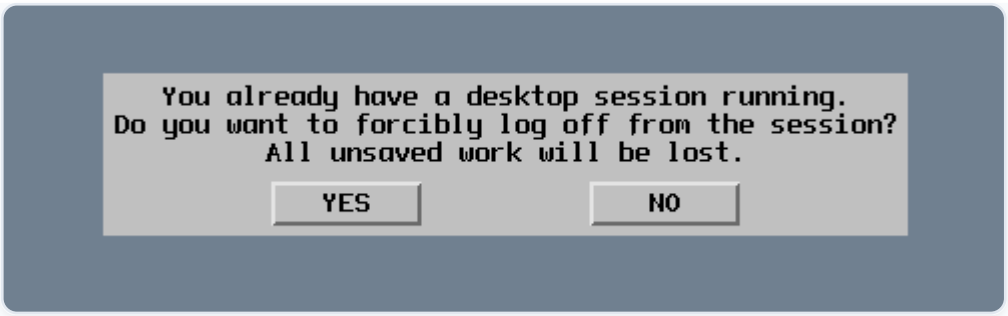
Eingabeaufforderung beim Öffnen einer zusätzlichen Desktopsitzung von einem VDA

Sie können eine Desktopsitzung von einem VDA über Citrix HDX, RDP und direkte Konsolenverbindungen öffnen. Versuche, eine zusätzliche HDX-Desktopsitzung vom selben Ubuntu-VDA zu öffnen, schlugen jedoch vor dieser Version fehl. Das Problem trat bei Ubuntu-VDAs auf, die mit dem GNOME-Desktop installiert sind. Als Verbesserung ermöglicht eine erzwungene Abmeldung von Ihrer aktuellen Desktopsitzung bei der folgenden Eingabeaufforderung, mit der neuen Desktopsitzung fortzufahren. Die Eingabeaufforderung wird

jedes Mal angezeigt, wenn Sie eine zusätzliche Desktopsitzung von einem VDA öffnen, unabhängig davon, auf welcher Linux-Plattform der VDA installiert ist.

Hinweis:

- Wenn Sie bei der Anmeldung am VDA über gdm3 bei der Eingabeaufforderung auf **JA** klicken, erscheint der Bildschirm Ihres Konsolen-Desktops schwarz und scheint nicht zu reagieren. Sie können Strg+Alt+F1 verwenden, um zum VDA-Anmeldefenster zurückzukehren.
- Die Eingabeaufforderung bleibt 30 Sekunden lang sichtbar. Danach wird die Antwort automatisch auf **NEIN** gesetzt.



Neuerungen in 2006

Version 2006 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Sprachunterstützung

Der Linux VDA ist jetzt in italienischer Sprache verfügbar. Weitere Informationen finden Sie unter Sprachunterstützung für Citrix-Produkte.

Unterstützung für SUSE 12 SP5

Ab dieser Version hat Citrix SUSE 12 SP5 als unterstützte Distribution hinzugefügt.

Verbesserung der Clientlaufwerkszuordnung

Diese Version verbessert die Clientlaufwerkszuordnung, um Dateiübertragungen zwischen dem Linux VDA und Ihrem Clientgerät zu beschleunigen, insbesondere unter Bedingungen hoher Netzwerklatenz.

Unterstützung für das Kopieren und Einfügen von Dateien zwischen Sitzungen und Clients

Mit Citrix Virtual Apps and Desktops 2006 und Citrix Workspace-App 1903 oder höher für Windows können Benutzer jetzt Dateien zwischen einer Sitzung und einem lokalen Client kopieren und einfügen. Kopier- und Einfügefunktionen werden über das Rechtsklickmenü oder Tastenkombinationen ausgeführt. Weitere Informationen finden Sie unter Dateien kopieren und einfügen.

> **Hinweis:**
>
> Ab dieser Version müssen Sie .NET Core Runtime 2.1 installieren, bevor Sie den Linux VDA installieren.

Neuerungen in 2003

Version 2003 des Linux VDA enthält die folgenden neuen Funktionen und Verbesserungen:

Unterstützung für RHEL 8

Ab dieser Version hat Citrix RHEL 8 als unterstützte Distribution hinzugefügt.

Integration mit dem Citrix Telemetry Service

Der Citrix Telemetry Service (**ctxtelemetry**) ist in die Linux VDA-Software integriert. Sie können jetzt Citrix Scout vom Delivery Controller ausführen, um Protokolle über den Linux VDA zu sammeln. Weitere Informationen finden Sie unter Citrix Scout.

Unterstützung für den schlanken virtuellen NSAP-Kanal

Der Linux VDA unterstützt den virtuellen NSAP-Kanal. Alle HDX Insight-Daten stammen ausschließlich vom virtuellen NSAP-Kanal und werden unkomprimiert gesendet, was Skalierbarkeit und Leistung verbessert. Weitere Informationen finden Sie unter HDX Insight.

Automatischer Download

Citrix hat den automatischen Download als Verbesserung für Dateiübertragungen hinzugefügt. Er ist für die Citrix Workspace-App für HTML5 und für Chrome verfügbar. Diese Verbesserung stellt das Verzeichnis **Auf meinem Gerät speichern** auf dem VDA bereit. Dateien, die Sie in das Verzeichnis **Auf meinem Gerät speichern** herunterladen oder verschieben, werden automatisch auf das Clientgerät übertragen. Weitere Informationen finden Sie unter Dateiübertragung.

Unterstützung für NVIDIA Tesla T4

NVIDIA Tesla T4 wird unterstützt.

Systemanforderungen

Die Current Release des Linux VDA ist auf Citrix Virtual Apps and Desktops abgestimmt. Sie ist auch abwärtskompatibel mit früheren Versionen von Citrix Virtual Apps and Desktops, die das Ende ihres Lebenszyklus noch nicht erreicht haben. Informationen zum Citrix Produktlebenszyklus und wann Citrix die Unterstützung für bestimmte Produktversionen einstellt, finden Sie in der Citrix Product Lifecycle Matrix.

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

Systemanforderungen für hier nicht behandelte Komponenten (wie die Citrix Workspace™ app) werden in den jeweiligen Dokumentationen beschrieben.

Informationen zur Verwendung einer Current Release (CR) in einer Long Term Service (LTSR)-Umgebung und weitere FAQs finden Sie im Knowledge Center-Artikel.

Unterstützte Linux-Distributionen, Xorg-Versionen und Desktop-Umgebungen

Eine Matrix der Linux-Distributionen, Xorg-Versionen und Desktop-Umgebungen, die diese Version des Linux VDA unterstützt, finden Sie in der folgenden Tabelle. 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
RHEL 9.2/9.0	1.20	GNOME
RHEL 8.8/8.6	1.20	GNOME, GNOME Classic, MATE

LINUX-DISTRIBUTION	XORG-VERSION	UNTERSTÜTZTER DESKTOP
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 der Support Ihres Betriebssystemanbieters abläuft, kann Citrix bei der Behebung von Problemen nur eingeschränkt helfen. Informationen zu veralteten oder entfernten Plattformen finden Sie unter Veraltet.
- Mindestens ein Desktop muss installiert sein. Sie können über das Skript ctxinstall.sh oder ctxsetup.sh die Desktopumgebung GNOME, GNOME Classic oder MATE für die Verwendung in Sitzungen angeben.
- Gemäß der Red Hat Enterprise Linux-Dokumentation ist GNOME die einzige in RHEL 9 verfügbare Desktopumgebung.
- Verwenden Sie `HWE kernel` oder `HWE Xorg` nicht unter Ubuntu.
- Ihr Benutzername muss den Syntaxregeln von `systemd` für Ihren aktuellen Display Manager entsprechen. Weitere Informationen zur Benutzernamensyntax von `systemd` finden Sie unter Syntax für Benutzer-/Gruppennamen.

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 ist die unterstützte Prozessorarchitektur x86-64.

Ab der Version 2203 können Sie den Linux VDA auf Microsoft Azure, AWS und GCP für Citrix Virtual Apps and Desktops sowie Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) hosten. Um diese öffentlichen Cloud-Hostverbindungen zu Ihrer Citrix Virtual Apps and Desktops-Bereitstellung hinzuzufügen, benötigen Sie Citrix Universal Subscription- oder Hybrid Rights-Lizenzen. Informationen zu Universal Subscription- und Hybrid Rights-Lizenzen finden Sie unter Transition and Trade Up (TTU) with Citrix Universal Subscription.

Active Directory-Integrationspakete

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

	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)

	WINBIND	SSSD	CENTRIFY	PBIS	QUEST
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 Sie Desktops und Anwendungen bereitstellen, die mit einer Graphics Processing Unit (GPU) zur Hardwarebeschleunigung die beste Leistung erzielen.

Hypervisoren

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

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

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

GPUs

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

NVIDIA vGPUs

Um zu erfahren, welche NVIDIA-GPU-Karten Ihre Linux-Distribution unterstützt, 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 installieren. 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 Access-Szenarien verwendet werden
- GPUs, die von einem Hypervisor durchgereicht werden

NVIDIA-GPUs, die das NVIDIA Capture SDK für Linux unterstützen

Für NVIDIA-GPUs, die das NVIDIA Capture SDK für Linux unterstützen, aktivieren Sie HDX 3D Pro, indem Sie bei der Installation des Linux VDA **CTX_XDL_HDX_3D_PRO** auf **Y** setzen. Es ist keine zusätzliche Konfiguration erforderlich. Die Hardwarebeschleunigung ist standardmäßig aktiviert, nachdem Sie HDX 3D Pro aktiviert haben.

Installationsübersicht

Dieser Abschnitt führt Sie durch die folgenden Verfahren:

- Domänenverbundene VDAs mit Easy Install erstellen
- Nicht-domänenverbundene Linux-VDAs mit MCS erstellen
- Linux-VDAs mit MCS erstellen
- Linux-VDAs mit Citrix Provisioning erstellen
- Linux-VDAs in Citrix DaaS Standard für Azure erstellen
- Linux VDA manuell installieren
  - Linux VDA manuell unter Amazon Linux 2, CentOS, RHEL und Rocky Linux installieren
  - Linux VDA manuell unter SUSE installieren
  - Linux VDA manuell unter Ubuntu installieren
  - Linux VDA manuell unter Debian installieren

Domänengebundene VDAs mit Easy Install erstellen

Wichtig:

- Für Neuinstallationen empfehlen wir Ihnen, diesen Artikel für eine schnelle Installation zu Rate zu ziehen. Dieser Artikel beschreibt, wie der Linux VDA mit Easy Install installiert und konfiguriert wird. Easy Install spart Zeit und Arbeit und ist weniger fehleranfällig als die manuelle Installation. Es hilft Ihnen, eine funktionierende Umgebung des Linux VDA einzurichten, indem es die notwendigen Pakete installiert und die Konfigurationsdateien automatisch anpasst.
- Easy Install unterstützt den Domänenbeitritt über Quest nicht.
- Um nicht-domänengebundene VDAs zu erstellen, müssen Sie Machine Creation Services (MCS) verwenden. Weitere Informationen finden Sie unter Nicht-domänengebundene Linux VDAs erstellen.

- Um mehr über die für nicht-domänengebundene VDAs verfügbaren Funktionen zu erfahren, gehen Sie zu Nicht-domänengebundene VDAs.

Schritt 1: Konfigurationsinformationen und die Linux-Maschine vorbereiten

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

- Hostname – Hostname der Maschine, auf der der Linux VDA installiert werden soll.
- IP-Adresse des Domänennamenservers.
- IP-Adresse oder Zeichenfolgenname des NTP-Servers.
- Domänenname – Der NetBIOS-Name der Domäne.
- Realm-Name – Der Kerberos-Realm-Name.
- Vollqualifizierter Domänenname (FQDN) der Domäne.
- Active Directory (AD)-Integrationsmethode – Derzeit unterstützt Easy Install Winbind, SSSD, Centrify und PBIS.
- Benutzername – Der Name des Benutzers, der die Maschine in die Domäne aufnimmt.
- Passwort – Das Kennwort des Benutzers, der die Maschine der Domäne beitritt.
- OU – Die Organisationseinheit. Optional.

Wichtig:

- Um den Linux VDA zu installieren, stellen Sie sicher, dass die Repositorys auf der Linux-Maschine korrekt hinzugefügt wurden.
- Um eine Sitzung zu starten, stellen Sie sicher, dass das X Window System und die Desktop-Umgebungen installiert sind.
- Aus Sicherheitsgründen speichert die einfache Installation das Kennwort für den Domänenbeitritt nicht. Jedes Mal, wenn Sie das Easy Install-Skript (ctxinstall.sh) im interaktiven Modus ausführen, müssen Sie das Kennwort für den Domänenbeitritt manuell eingeben. Im unbeaufsichtigten Modus müssen Sie das Kennwort für den Domänenbeitritt in **/Citrix/VDA/sbin/ctxinstall.conf** festlegen oder das Kennwort exportieren. Wir empfehlen, das Administratorkonto nicht für den Domänenbeitritt zu verwenden. Delegieren Sie stattdessen die Berechtigungen für den Domänenbeitritt an einen Active Directory-Benutzer, der nicht das Administratorkonto ist. Delegieren Sie dazu

> die Kontrolle auf dem Domänencontroller mithilfe des **Assistenten zum Delegieren von Berechtigungen**.

Schritt 2: Hypervisor vorbereiten

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

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

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

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

```
su -



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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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

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

`xen.independent_wallclock = 1`

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

```
su -



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

Dieser Befehl gibt den Wert 1 zurück.

Zeitliche Synchronisierung auf Microsoft Hyper-V korrigieren

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

Vom Verwaltungsbetriebssystem aus:

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

Hinweis:

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

Zeitliche Synchronisierung auf ESX und ESXi korrigieren

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

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

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

Schritt 3: .NET Runtime 6.0 installieren

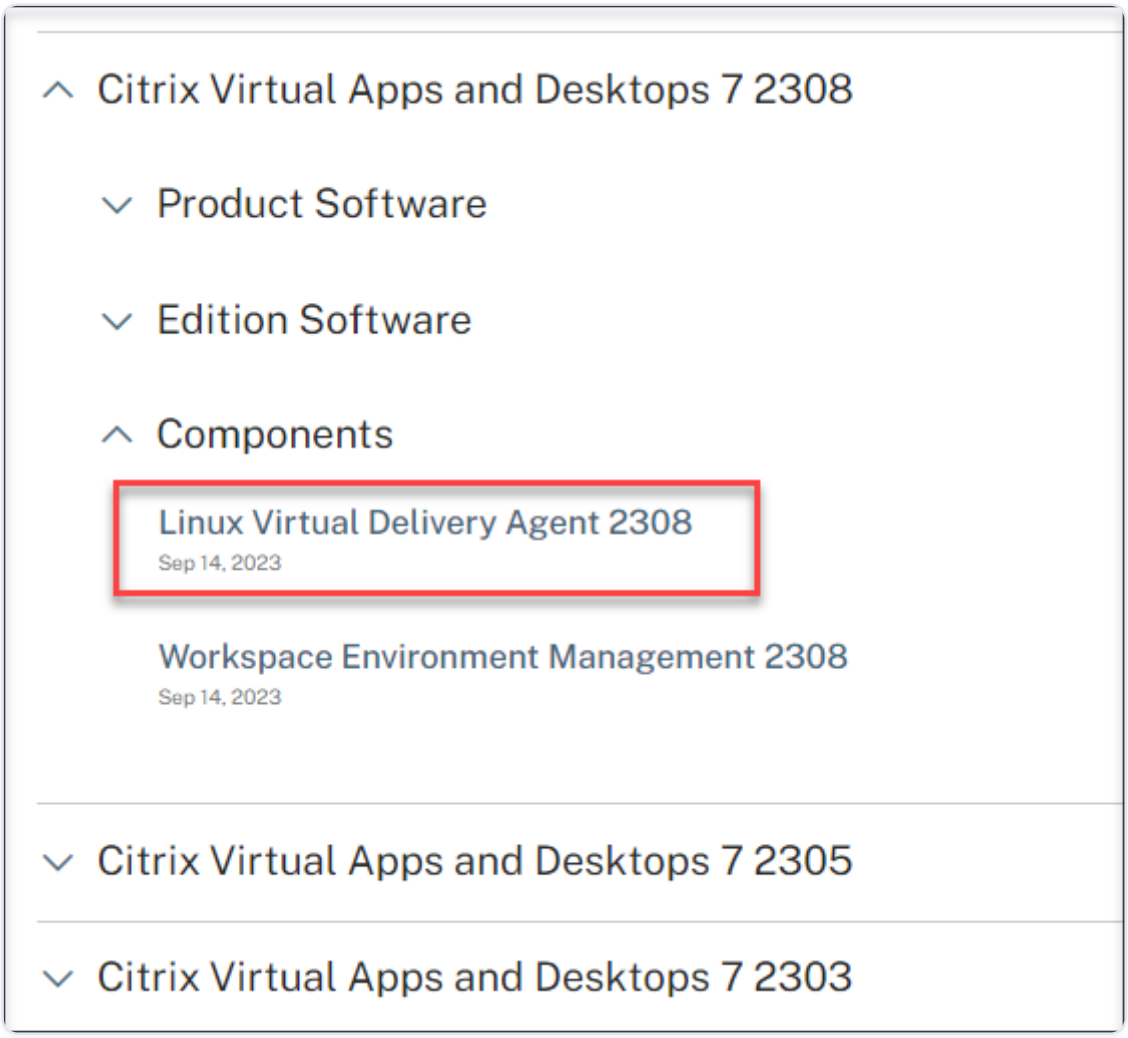
Bevor Sie den Linux VDA installieren, installieren Sie .NET Runtime 6.0 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

Nach der Installation von .NET Runtime 6.0 führen Sie den Befehl **which dotnet** aus, um Ihren Runtime-Pfad zu finden.

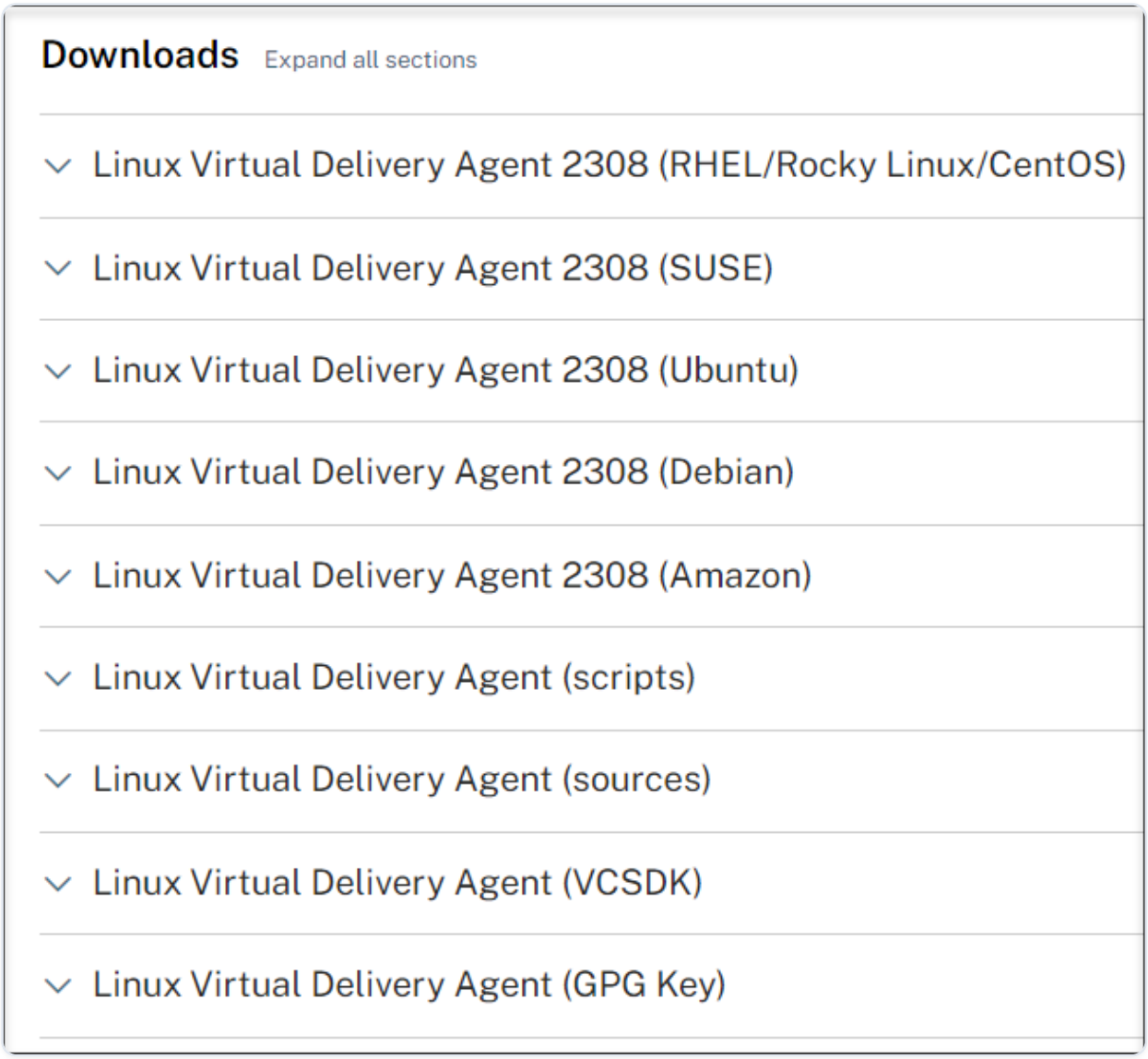
Basierend auf der Befehlsausgabe legen Sie den binären .NET-Runtime-Pfad fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als binären .NET-Pfad.

Schritt 4: Linux VDA-Paket herunterladen

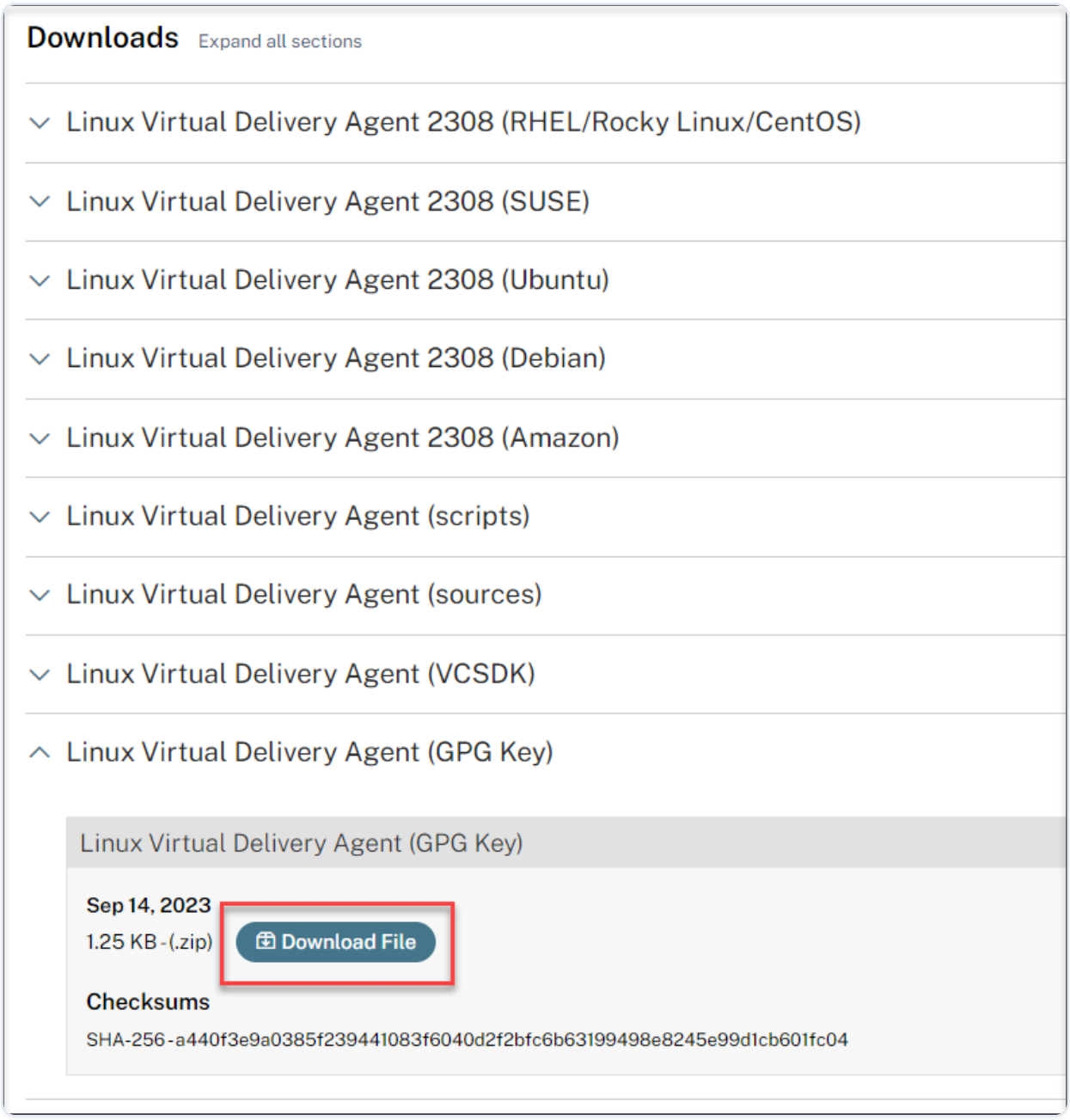
1. Gehen Sie zur Citrix Virtual Apps and Desktops Downloadseite.
2. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. erweitern Sie **Komponenten**, um den Linux VDA zu finden. Zum Beispiel:



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. Zum Beispiel:



So überprüfen Sie die 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>
```

- 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>
```

Schritt 5: Linux VDA-Paket installieren

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

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

Hinweis:

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

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

Hinweis:

Nach der Installation des Linux VDA auf RHEL 8.x/9.x und Rocky Linux 8.x/9.x, die auf GCP gehostet werden, kann die Ethernet-Verbindung verloren gehen und der Linux VDA nach einem VM-Neustart unerreichbar sein. Um dieses Problem zu umgehen, legen Sie beim ersten Anmelden an der VM ein Root-Passwort fest und stellen Sie sicher, dass Sie sich als Root 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
```

Für Ubuntu/Debian-Distributionen:

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

sudo apt-get install -f
```

Hinweis:

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

Für SUSE-Distributionen:

1. Stellen Sie für SUSE 15.4 unter AWS, Azure und GCP sicher, dass:
   - Sie **libstdc++6** Version 12 oder höher verwenden.
   - Der Parameter **Default_WM** in **/etc/sysconfig/windowmanager** auf **„gnome“** festgelegt ist.
2. Führen Sie den folgenden Befehl aus, um den Linux VDA zu installieren:

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

Schritt 6: NVIDIA GRID-Treiber installieren

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 Anleitungen:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Führen Sie die folgenden allgemeinen Schritte aus, um die NVIDIA GRID-Gast-VM-Treiber zu installieren und zu konfigurieren:

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

Schritt 7: Zu verwendende Datenbank angeben

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

Hinweis:

- Wir empfehlen die Verwendung von SQLite nur für den VDI-Modus und PostgreSQL für ein Bereitstellungsmodell für gehostete Shared Desktops.
- Für die einfache Installation und MCS können Sie SQLite oder PostgreSQL angeben, ohne sie manuell installieren zu müssen. Sofern nicht anders über **/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 zur Vervollständigung der Installation

Nach der Installation des Linux VDA-Pakets konfigurieren Sie die Laufzeitumgebung mithilfe des Skripts ctxinstall.sh oder der GUI.

Hinweis:

Bevor Sie die Laufzeitumgebung einrichten, stellen Sie sicher, dass das Gebietsschema **en_US.UTF-8** in Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema in Ihrem Betriebssystem nicht verfügbar ist, führen Sie den Befehl **sudo locale-gen en_US.UTF-8** aus. Bearbeiten Sie für Debian die Datei **/etc/locale.gen**, indem Sie die Zeile # **en_US.UTF-8 UTF-8** auskommentieren, und führen Sie dann den Befehl **sudo locale-gen** aus.

ctxinstall.sh

ctxinstall.sh ist das Easy-Install-Skript, das die Laufzeitumgebung für den Linux VDA konfiguriert. Weitere Informationen erhalten Sie mit dem Hilfebefehl **ctxinstall.sh -h**.

Easy Install verwendet **/opt/Citrix/VDA/sbin/ctxinstall.conf** als Konfigurationsdatei, um die Werte aller Umgebungsvariablen, die für die GUI und ctxinstall.sh benötigt werden, festzulegen, zu speichern und zu synchronisieren. Wenn Sie die Konfigurationsdatei zum ersten Mal erstellen, verwenden Sie eine der folgenden Methoden:

- Durch Kopieren der Vorlagendatei **/opt/Citrix/VDA/sbin/ctxinstall.conf.tmpl** und Speichern als **/opt/Citrix/VDA/sbin/ctxinstall.conf**.
- Durch Ausführen von ctxinstall.sh. Jedes Mal, wenn Sie ctxinstall.sh ausführen, wird Ihre Eingabe in **/opt/Citrix/VDA/sbin/ctxinstall.conf** gespeichert.

Hinweis:

- Gemäß dem Prinzip der geringsten Rechte stellen Sie sicher, dass nur der Root-Benutzer **/opt/Citrix/VDA/sbin/ctxinstall.conf** lesen kann, da das Domänenbeitrittspasswort in der Datei festgelegt sein könnte.
- Das Deinstallieren des Linux VDA entfernt Dateien unter **/opt/Citrix/VDA**. Wir empfehlen Ihnen, **/opt/Citrix/VDA/sbin/ctxinstall.conf** zu sichern, bevor Sie den VDA deinstallieren.

Sie können ctxinstall.sh im interaktiven Modus oder im unbeaufsichtigten Modus ausführen. Bevor Sie das Skript ausführen, legen Sie die folgenden Umgebungsvariablen fest:

- **CTX_EASYINSTALL_HOSTNAME=host-name** – Der Hostname des Linux-VDA-Servers.
- **CTX_EASYINSTALL_DNS=ip-address-of-dns** – Die IP-Adresse des DNS.

- **CTX_EASYINSTALL_NTPS=address-of-ntps** – Die IP-Adresse oder der Zeichenfolgenname des NTP-Servers.
- **CTX_EASYINSTALL_REALM=realm-name** – Der Kerberos-Realm-Name.
- **CTX_EASYINSTALL_FQDN=ad-fqdn-name**
- **CTX_EASYINSTALL_USERNAME=domain-user-name** – Der Name des Benutzers, der den Computer der Domäne beitritt.
- **CTX_EASYINSTALL_PASSWORD=password** – Das Kennwort des Benutzers, der den Computer der Domäne beitritt.

> **Hinweis:**
>
> Wir empfehlen, das Administratorkonto nicht für den Domänenbeitritt zu verwenden. Delegieren Sie stattdessen die Berechtigungen für den Domänenbeitritt an einen anderen Active Directory-Benutzer als das Administratorkonto. Delegieren Sie dazu die Kontrolle auf dem Domänencontroller mithilfe des **Assistenten zum Delegieren von Kontrollberechtigungen**.

Die folgenden vier Variablen sind optional. Auch wenn sie nicht festgelegt sind, wird ctxinstall.sh im unbeaufsichtigten Modus nicht abgebrochen, und Sie werden im interaktiven Modus nicht zur Benutzereingabe aufgefordert. Sie können sie nur durch Exportieren ihrer Werte oder Bearbeiten von **/Citrix/VDA/sbin/ctxinstall.conf** festlegen.

- **CTX_EASYINSTALL_NETBIOS_DOMAIN=netbios-domain-name** – Der NetBIOS-Domänenname ist typischerweise 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 verschiedenen **AD**-Integrationsmethoden. Ein Beispiel für OU-Werte finden Sie in der Tabelle im Abschnitt Überlegungen dieses Artikels. Diese Variable ist optional.
- **CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=centrify-local-path** – Easy Install hilft beim Herunterladen des Centrify-Pakets aus dem Internet. Wenn Centrify jedoch bereits installiert ist, können Sie das Centrify-Paket aus einem lokalen Verzeichnis abrufen, das durch diese Variable definiert ist. Diese Variable ist optional.
- **CTX_EASYINSTALL_PBIS_LOCAL_PATH= pbis-local-path** – Easy Install hilft beim Herunterladen des PBIS-Pakets aus dem Internet. Wenn PBIS jedoch bereits installiert ist,

können Sie das PBIS-Paket aus einem lokalen Verzeichnis abrufen, das durch diese Variable definiert ist. Diese Variable ist optional.

Das Ausführen von ctxinstall.sh ruft ein weiteres Skript auf, ctxsetup.sh. ctxsetup.sh verwendet die folgenden Variablen:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste von vollständig qualifizierten Domänennamen (FQDNs) der Delivery Controller, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. Mindestens ein FQDN oder CNAME muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** – Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux Virtual Desktop-Dienste werden nach dem Start der Maschine gestartet.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux VDA-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Ports 80 und 1494) automatisch in der System-Firewall für den Linux Virtual Desktop öffnen.
- **CTX_XDL_AD_INTEGRATION=winbind \| sssd \| centrify \| pbis** – Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird vom installierten und konfigurierten Active Directory-Integrationstool auf dem System bestimmt.
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung von grafikintensiven Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für VDI-Desktops im Einzel-Sitzungs-Modus konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Gibt an, ob die Maschine als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie den Wert auf Y.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf eine lokale Site zu beschränken, geben Sie einen DNS-Sitenamen an. Falls nicht erforderlich, setzen Sie den Wert auf **\<none\>**.

- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum Beispiel ad1.mycompany.com:389 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. Um schnellere LDAP-Abfragen innerhalb einer Active Directory-Gesamtstruktur zu ermöglichen, aktivieren Sie den **Globalen Katalog** auf einem Domänencontroller und geben Sie die relevante LDAP-Portnummer als 3268 oder als 3269 an, wenn Sie LDAPS verwenden. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne gesetzt ist (z. B. DC=mycompany,DC=com). Um die Suchleistung zu verbessern, können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Falls nicht erforderlich, setzen Sie den Wert auf **\<none\>**.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt keine AD-Gruppenrichtlinie, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit 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 zur Installation von .NET Runtime 6.0 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP_ENVIRONMENT=gnome/gnome-classic/mate** – Gibt die GNOME-, GNOME Classic- oder MATE-Desktop-Umgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.
- **CTX_XDL_START_SERVICE=Y \| N** – Legt fest, ob die Linux VDA-Dienste gestartet werden, wenn die Konfiguration abgeschlossen ist.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Abhören von Citrix Scout. Der Standardport ist 7503.

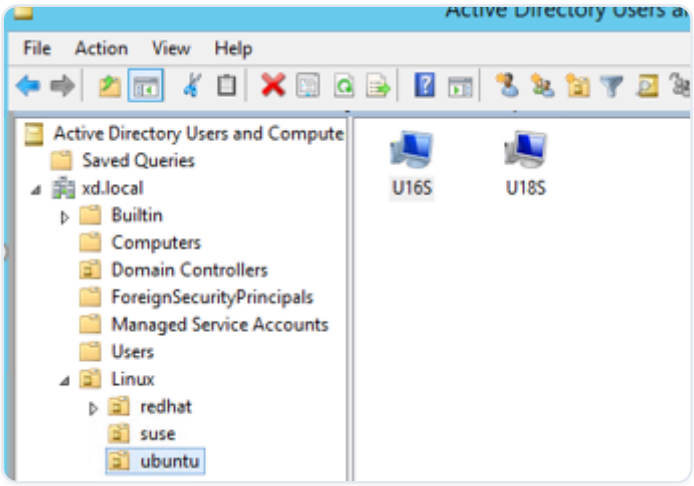
- **CTX_XDL_TELEMETRY_PORT** – Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

Überlegungen

- Der NetBIOS-Domänenname ist typischerweise die erste Komponente des DNS-Domänennamens, getrennt durch einen Punkt (.). Um einen anderen NetBIOS-Domänennamen in Ihrer Umgebung anzupassen, legen Sie die Umgebungsvariable **CTX_EASYINSTALL_NETBIOS_DOMAIN** in **/opt/Citrix/VDA/sbin/ctxinstall.conf** fest.
- Um Ihren VDA einer bestimmten OU beizutreten, gehen Sie wie folgt vor:

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

  Ein Beispiel für eine OU finden Sie im folgenden Screenshot



  b. 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 zeigt die Beispiel-OU-Namen im vorhergehenden Screenshot. Sie können in Ihrer Organisation beliebige andere OU-Namen verwenden.

BETRIEBSSYSTEM	WINBIND	SSSD	CENTRIFY	PBIS
Amazon Linux 2	`"Linux/amazon"`	`"Linux/amazon"`	`"XD.LOCAL/Linux/amazon"`	`"Linux/amazon"`

BETRIEBSSYSTEM	WINBIND	SSSD	CENTRIFY	PBIS
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"`	N/A	N/A
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"`	N/A	N/A
RHEL 7	`"Linux/redhat"`	`"Linux/redhat"`	`"XD.LOCAL/Linux/redhat"`	`"Linux/redhat"`
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. Mindestens ein DNS-Server, der **IPv4** verwendet, ist in /etc/resolv.conf erforderlich, damit **adclient** AD-Dienste ordnungsgemäß finden kann.

  Protokoll:

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

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

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

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

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

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

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

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

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

  a. Erstellen Sie eine `.xsession`- oder `.Xclients`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA. Wenn Sie Amazon Linux 2 verwenden, erstellen Sie eine `.Xclients`-Datei. Wenn Sie andere Distributionen verwenden, erstellen Sie eine `.xsession`-Datei.

  b. Bearbeiten Sie die Datei `.xsession` oder `.Xclients`, um eine Desktop-Umgebung basierend auf Distributionen anzugeben.

  - **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
```

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

Ab Version 2209 können Sitzungsbenutzer ihre Desktop-Umgebungen anpassen. Um diese Funktion zu aktivieren, müssen Sie im Voraus umschaltbare Desktop-Umgebungen auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktop-Umgebungen durch Sitzungsbenutzer.

- Wenn Sie Centrify als Methode zum Beitreten einer Domäne wählen, benötigt das Skript ctxinstall.sh das Centrify-Paket. Möglichkeiten für ctxinstall.sh, das Centrify-Paket zu erhalten:

  - Easy Install hilft, das Centrify-Paket automatisch aus dem Internet herunterzuladen. Im Folgenden sind die URLs für jede Distribution aufgeführt:

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

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

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

Für 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 aus einem lokalen Verzeichnis ab, wenn Centrify bereits installiert ist. Um das Verzeichnis des Centrify-Pakets festzulegen, setzen Sie **CTX_EASYINSTALL_CENTRIFY_LOCAL_PATH=/home/mydir** in **/opt/Citrix/VDA/sbin/ctxinstall.conf**. Zum 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
```

- Wenn Sie PBIS als Methode zum Beitreten einer Domäne wählen, benötigt das Skript ctxinstall.sh das PBIS-Paket. Möglichkeiten für ctxinstall.sh, das PBIS-Paket zu erhalten:
  - Easy Install hilft, das PBIS-Paket automatisch aus dem Internet herunterzuladen. Zum Beispiel sind dies die URLs für jede Distribution:

    Für 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>`

    Für 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 aus dem Internet ab. Ändern Sie dazu die Zeilen "pbisDownloadRelease" und "pbisDownloadExpectedSHA256" in der Datei /opt/Citrix/VDA/sbin/ctxinstall.sh.

    Ein Beispiel finden Sie im folgenden Screenshot:

  - Rufen Sie das PBIS-Paket aus einem lokalen Verzeichnis ab, wenn PBIS bereits installiert ist. Um das Verzeichnis des PBIS-Pakets festzulegen, setzen Sie die Umgebungsvariable **CTX_EASYINSTALL_PBIS_LOCAL_PATH** in **/opt/Citrix/VDA/sbin/ctxinstall.conf**.

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 den entsprechenden Variablenwert bei jeder Aufforderung in der Befehlszeilenschnittstelle ein. Wenn eine Variable bereits festgelegt ist, fragt ctxinstall.sh nach einer Bestätigung, falls Sie sie ändern möchten.

Stiller Modus

Im stillen Modus müssen Sie die oben genannten Variablen mit **/opt/Citrix/VDA/sbin/ctxinstall.conf** oder dem Exportbefehl festlegen. Führen Sie danach **ctxinstall.sh -S** aus (beachten Sie, dass der Buchstabe **S** hier **großgeschrieben** ist). Wenn nicht alle erforderlichen Variablen festgelegt oder einige Werte ungültig sind, bricht **ctxinstall.sh** die Ausführung ab, es sei denn, es gibt Standardwerte.

Der exportierte Wert für jede Variable überschreibt den Wert in **/Citrix/VDA/sbin/ctxinstall.conf**, es sei denn, er ist nicht festgelegt. Alle aktualisierten Werte werden in **/Citrix/VDA/sbin/ctxinstall.conf** gespeichert, mit Ausnahme des Kennworts für den Domänenbeitritt. Im stillen Modus müssen Sie das Kennwort für den Domänenbeitritt also 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

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 | 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/ctxinstall.sh -S
```

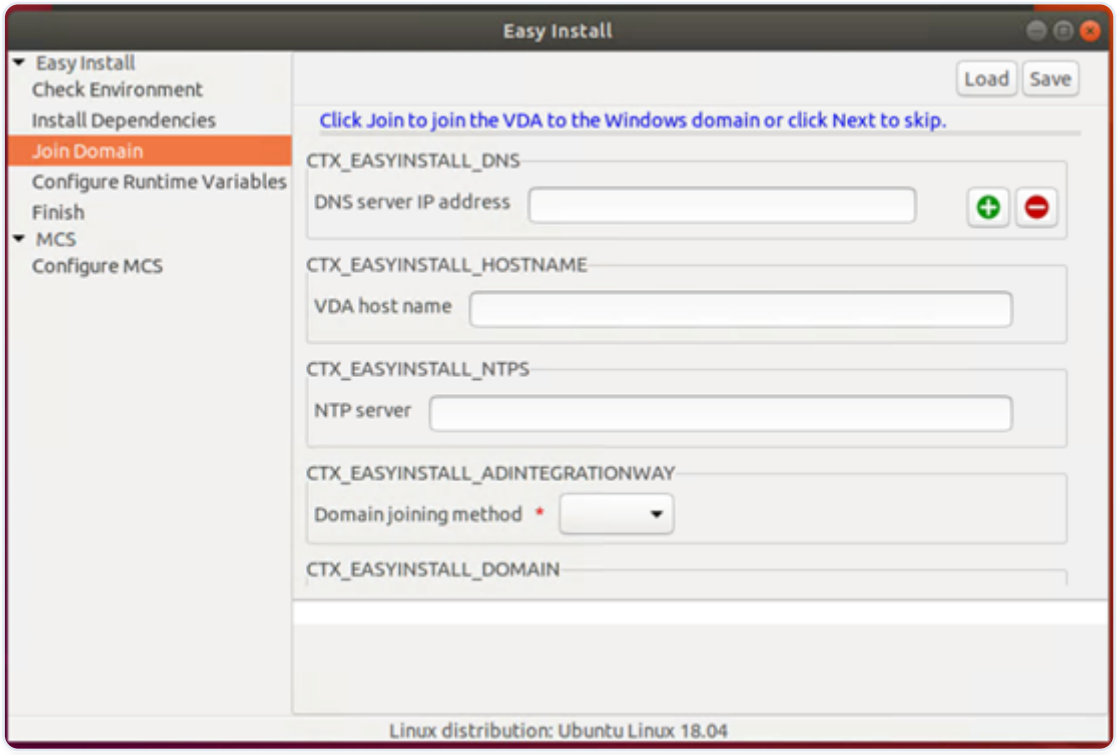
Wenn Sie den sudo-Befehl ausführen, geben Sie die Option **-E** ein, um die vorhandenen Umgebungsvariablen an die neue Shell zu übergeben, die er erstellt. Wir empfehlen, eine Shell-Skriptdatei aus den oben genannten Befehlen mit **#\!/bin/bash** als erster Zeile zu erstellen.

Alternativ können Sie alle Variablen mit einem einzigen Befehl angeben.

Um die Umgebungsvariablen der VDA-Laufzeit (die mit '**CTX_XDL_**' beginnen) einzurichten, können Sie **ctxinstall.sh -s** ausführen (beachten Sie, dass der Buchstabe **s** hier **kleingeschrieben** ist).

GUI

Wenn Sie SSSD oder Winbind als Methode für den Domänenbeitritt verwenden, können Sie die einfache Installation über eine GUI nutzen. Führen Sie den Befehl **/opt/Citrix/VDA/bin/easyinstall** in der Desktop-Umgebung Ihres VDA aus und folgen Sie dann den Anweisungen in der GUI für die einfache Installation.



Die GUI für die einfache Installation führt Sie durch die folgenden Vorgänge:

- Systemumgebung prüfen
- Abhängigkeiten installieren
- VDA einer angegebenen Domäne beitreten lassen
- Laufzeitumgebung konfigurieren

> **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 zum Konfigurieren von MCS-Variablen finden Sie unter Schritt 3: Masterimage vorbereiten.

- Das Skript ctxinstall.sh speichert alle Variableneinstellungen außer dem Kennwort für den Domänenbeitritt in **/Citrix/VDA/sbin/ctxinstall.conf**.

Schritt 9: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um nach häufigen Konfigurationsproblemen in einer Linux-VDA-Umgebung zu suchen. Weitere Informationen finden Sie unter **XDPing**.

Schritt 10: Linux-VDA ausführen

Linux-VDA starten:

So starten Sie die Linux-VDA-Dienste:

```
sudo systemctl start ctxhdx.service



sudo systemctl start ctxvda.service
```

Linux-VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo systemctl stop ctxvda.service



sudo systemctl stop ctxhdx.service
```

Hinweis:

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

Linux VDA neu starten:

So starten Sie die Linux VDA-Dienste neu:

```
sudo systemctl stop ctxvda.service



sudo systemctl restart ctxhdx.service



sudo systemctl start ctxvda.service
```

Status des Linux VDA überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda.service



sudo systemctl status ctxhdx.service
```

Schritt 11: Maschinenkataloge erstellen

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

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

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

> **Hinweis:**

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

Tipp:

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

Schritt 12: Bereitstellungsgruppen erstellen

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

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

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

Wichtig:

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

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

Schritt 13: Linux VDA aktualisieren (optional)

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

Für RHEL 7 und CentOS 7:

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

Für RHEL 8 und Rocky Linux 8:

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

Für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

Hinweis:

Bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 aktualisieren, aktualisieren Sie das Paket **libsepol** auf Version 3.4 oder höher.

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

Für SUSE:

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

Für Ubuntu 20.04:

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

Für Ubuntu 22.04:

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

Problembehandlung

Verwenden Sie die Informationen in diesem Abschnitt, um Probleme zu beheben, die bei der Verwendung der Easy-Install-Funktion auftreten können.

Beitritt zu einer Domäne mithilfe von SSSD schlägt fehl

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

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

/var/log/xdl/vda.log:

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

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

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

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

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

-  Kerberos is correctly configured on this machine.

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

Error Details:

Exception 'General security error (An error occurred in trying to obtain a
```

```
TGT: Client not found in Kerberos database (6))' of type 'class
javax.xml.ws.soap.SOAPFaultException'.

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

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

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

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

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

/var/log/messages:

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

Um dieses Problem zu beheben:

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

Ubuntu-Desktopsitzungen zeigen einen grauen Bildschirm

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

So beheben Sie dieses Problem:

1. Führen Sie den Befehl `sudo apt-get update` aus.
2. Führen Sie den Befehl `sudo apt-get install unity lightdm` aus.
3. Fügen Sie die folgende Zeile zu `/etc/lightdm/lightdm.conf` hinzu:

   `greeter-show-manual-login=true`

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

/var/log/xdl/hdx.log:

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



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



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



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

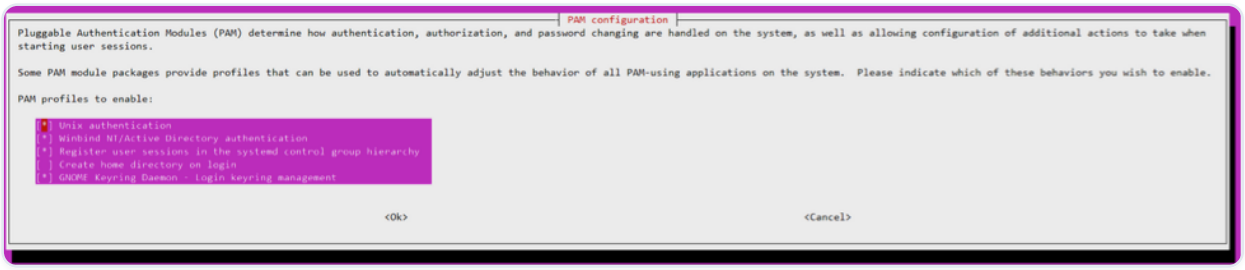
Tipp:

Die Ursache dieses Problems ist, dass das Home-Verzeichnis für den Domänenadministrator nicht erstellt wird.

So beheben Sie dieses Problem:

1. Geben Sie in einer Befehlszeile **pam-auth-update** ein.

2. Vergewissern Sie sich im daraufhin angezeigten Dialogfeld, dass **Home-Verzeichnis-Anmeldung erstellen** ausgewählt ist.



Sitzung startet nicht oder endet schnell mit dbus-Fehler

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

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



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



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



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



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



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

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

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

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



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



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



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



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



Nov  3 11:03:52 user01-HVM-domU pulseaudio[25352]: [pulseaudio] pid.c:
```

```
Daemon already running.Nov  3 11:03:58 user01-HVM-domU citrix-
ctxgfx[24693]: Exiting normally
```

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

SELinux verhindert den Zugriff von SSHD auf das Home-Verzeichnis

Der Benutzer kann eine Sitzung starten, sich aber 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
```

Zur Behebung dieses Problems:

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

   SELINUX=disabled

2. Starten Sie den VDA neu.

Nicht-Domänen-gebundene Linux-VDAs erstellen

Dieser Artikel führt Sie durch die Verwendung von Machine Creation Services™ (MCS) zur Erstellung nicht-Domänen-gebundener Linux-VDAs in Citrix DaaS.

Wichtig:

- Nicht-Domänen-gebundene VDAs werden für Citrix DaaS unterstützt.
  - Ihre Steuerungsebene muss über Citrix DaaS bereitgestellt werden.
  - Sie können nicht-Domänen-gebundene VDAs in einer Public Cloud oder einem lokalen Rechenzentrum bereitstellen. Nicht-Domänen-gebundene 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 nicht-Domänen-gebundene VDAs zu erstellen, müssen Sie MCS verwenden.
  - Bare-Metal-Server werden von MCS nicht unterstützt.
- Die folgenden Funktionen sind für nicht-Domänen-gebundene Linux-VDAs verfügbar:
  - Lokale Benutzer mit bestimmten Attributen auf nicht-Domänen-gebundenen VDAs erstellen
  - Nicht-SSO-Authentifizierung
  - Authentifizierung mit Azure Active Directory
  - Rendezvous V2

(Nur für Nutanix) Schritt 1: Installieren und registrieren Sie das Nutanix AHV-Plug-In

Beziehen Sie das Nutanix AHV-Plug-In-Paket von Nutanix. Installieren und registrieren Sie das Plug-In in Ihrer Citrix Virtual Apps and Desktops-Umgebung. Weitere Informationen finden Sie im Installationshandbuch für das Nutanix Acropolis MCS-Plug-In, das im Nutanix Support Portal verfügbar ist.

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

Nachdem Sie Citrix Virtual Apps and Desktops™ installiert haben, wählen und installieren Sie das **XD MCS AHV Plugin** auf Ihren Delivery Controllern.

Nutanix AHV-Plug-In für lokale Delivery Controller(/en-us/linux-virtual-delivery-agent/2308/media/nutanix-plug-in-for-cvad.png)

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

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

Schritt 1c: Führen Sie die folgenden Schritte nach der Installation des Plug-Ins aus

- Überprüfen Sie, ob ein Nutanix Acropolis-Ordner in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0` erstellt wurde.
- Führen Sie den Befehl `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"` aus.
- Starten Sie die Citrix Host-, Citrix Broker- und Citrix Machine Creation Services auf Ihren lokalen Delivery Controllern neu oder starten Sie den Citrix RemoteHCLServer Service auf Citrix Cloud Connectors neu.

> **Tipp:**
>
> Wir empfehlen, die Citrix Host-, Citrix Broker- und Machine Creation Services zu beenden und dann neu zu starten, wenn Sie das Nutanix AHV-Plug-In installieren oder aktualisieren.

Schritt 2: Eine Hostverbindung erstellen

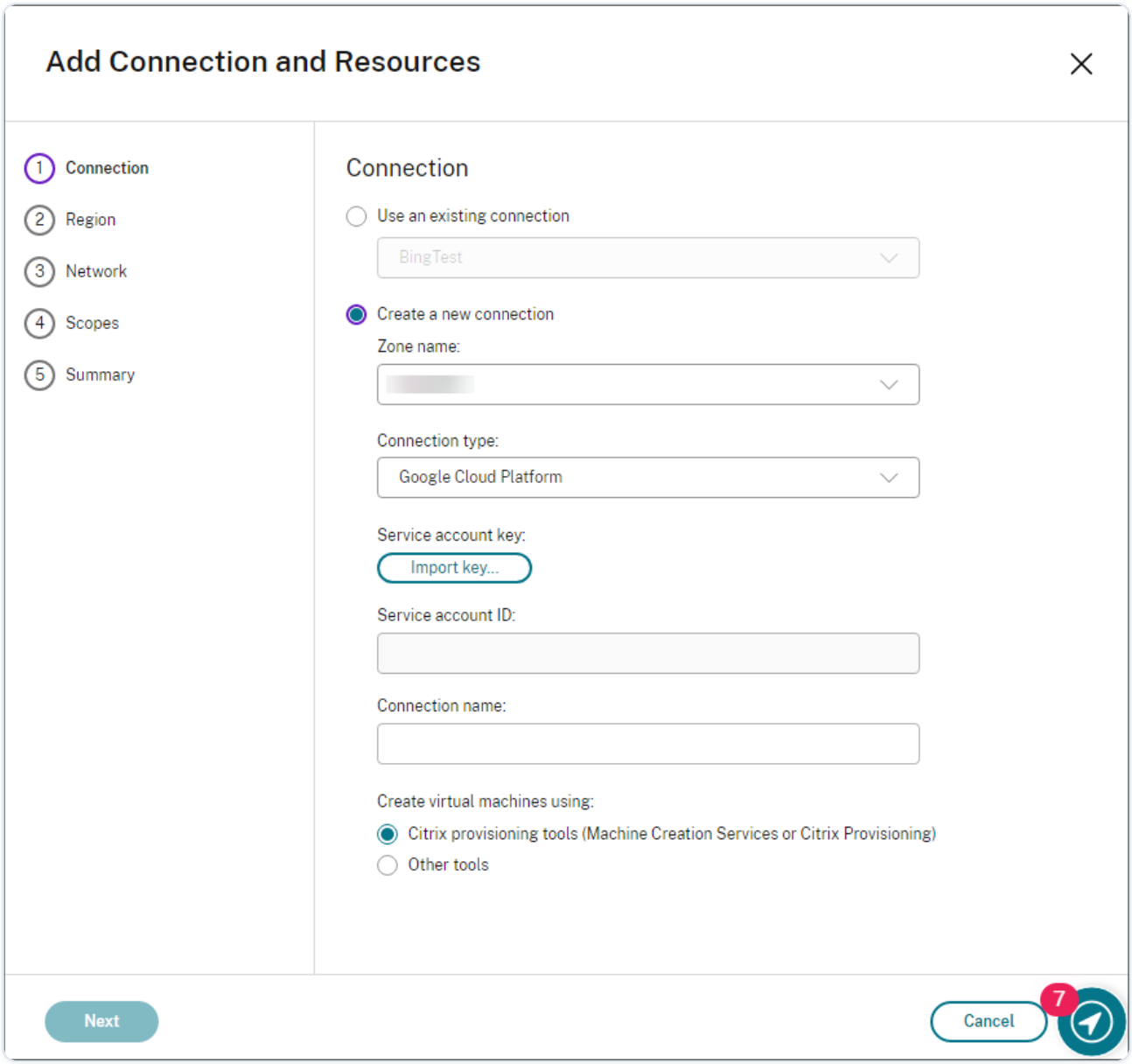
Hosts sind Hypervisoren oder Cloud-Dienste, die an Ihren Ressourcenstandorten verwendet werden. In diesem Schritt können Sie Informationen angeben, die DaaS zur Kommunikation mit VMs auf einem Host verwendet. Detaillierte Informationen umfassen den Ressourcenstandort, den

Hosttyp, die Zugangsdaten, die zu verwendende Speichermethode und welche Netzwerke die VMs auf dem Host verwenden können.

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

1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im oberen linken Menü **Meine Dienste > DaaS**.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste **Verbindungen und Ressourcen hinzufügen** aus.
5. Der Assistent führt Sie durch die folgenden Seiten. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Nachdem Sie jede Seite ausgefüllt haben, wählen Sie **Weiter**, bis Sie die Seite **Zusammenfassung** erreichen.

Schritt 2a: Verbindung



Auf der Seite **Verbindung**:

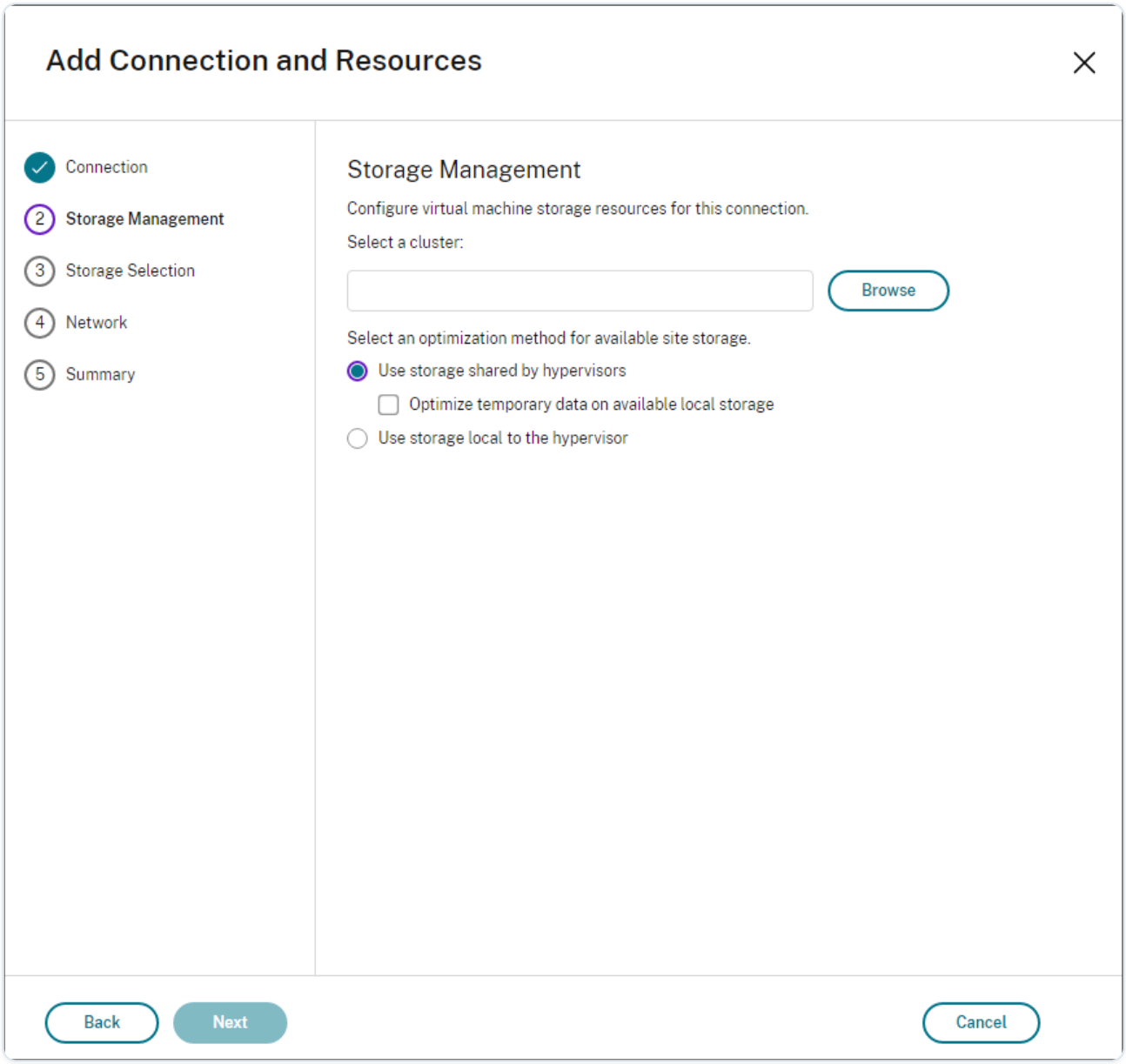
- Um eine Verbindung zu erstellen, wählen Sie **Neue Verbindung erstellen**. Um eine Verbindung basierend auf derselben Hostkonfiguration wie eine vorhandene Verbindung zu erstellen, wählen Sie **Vorhandene Verbindung verwenden** und dann die entsprechende Verbindung aus.
- Wählen Sie eine Zone im Feld **Zonenname** aus. Die Optionen sind alle von Ihnen konfigurierten Ressourcenstandorte.
- Wählen Sie im Feld **Verbindungstyp** einen Hypervisor oder Cloud-Dienst aus. Die Optionen sind Hypervisoren und Cloud-Dienste, deren Plug-Ins in der Zone ordnungsgemäß installiert sind. Alternativ können Sie den PowerShell-Befehl `Get-HypHypervisorPlugin -ZoneUid`

verwenden, um eine Liste der mit der ausgewählten Zone verfügbaren Hypervisor-Plug-Ins abzurufen.

- Geben Sie einen Verbindungsnamen ein. Dieser Name wird in der Anzeige **Verwalten** angezeigt.
- Wählen Sie das Tool zum Erstellen virtueller Maschinen: Machine Creation Services oder Citrix Provisioning.

Die Informationen auf der Seite **Verbindung** unterscheiden sich je nach dem von Ihnen verwendeten Host (Verbindungstyp). Wenn Sie beispielsweise den Azure Resource Manager verwenden, können Sie einen vorhandenen Dienstprinzipal verwenden oder einen neuen erstellen.

Schritt 2b: Speicherverwaltung



Informationen zu Speicherverwaltungstypen und -methoden finden Sie unter Hostspeicher.

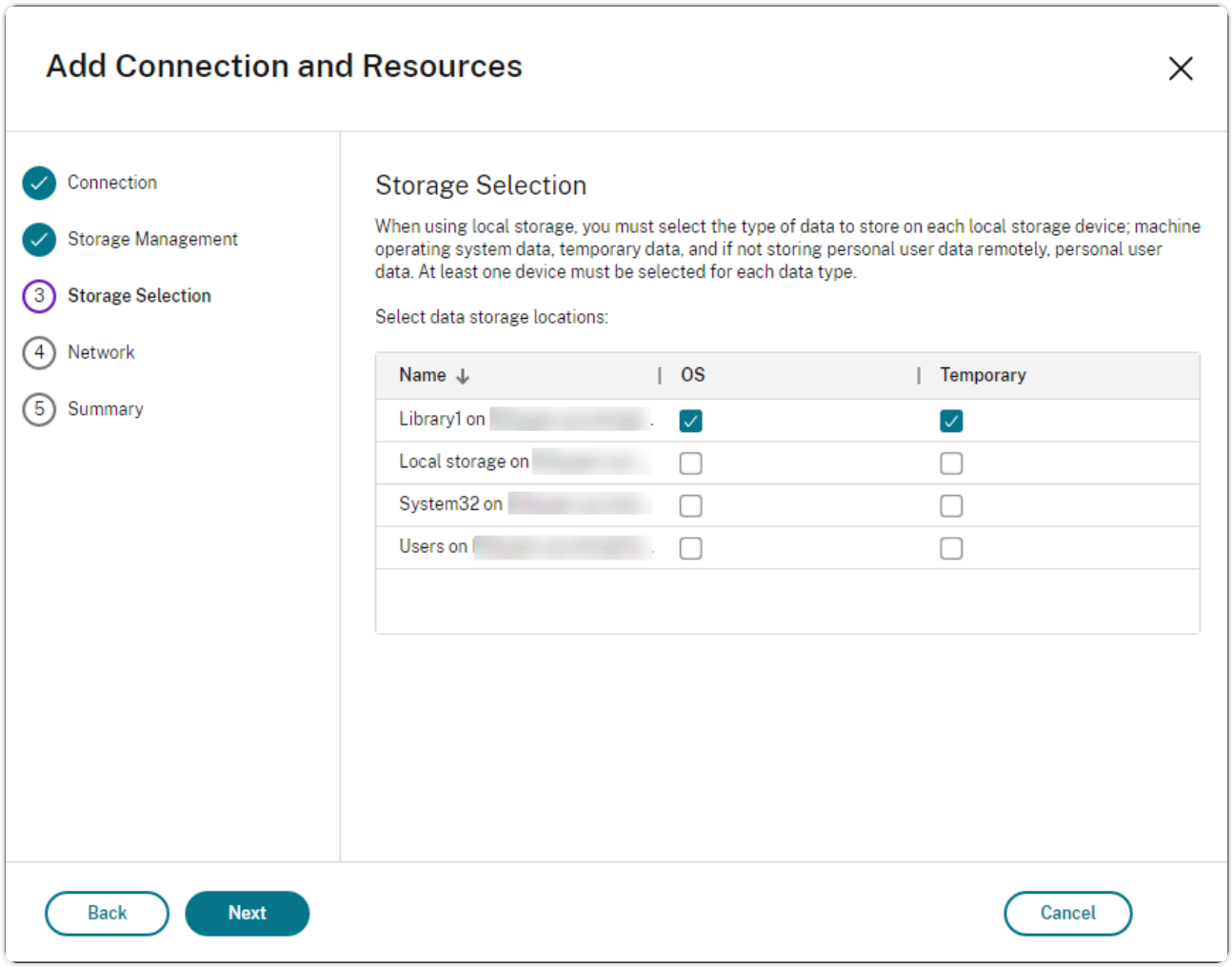
Wenn Sie eine Verbindung zu einem Hyper-V- oder VMware-Host konfigurieren, navigieren Sie zu einem Clusternamen und wählen Sie ihn aus. Andere Verbindungstypen erfordern keinen Clusternamen.

Wählen Sie eine Speicherverwaltungsmethode aus: von Hypervisoren gemeinsam genutzter Speicher oder lokaler Speicher des Hypervisors.

- Wenn Sie von Hypervisoren gemeinsam genutzten Speicher wählen, geben Sie an, ob temporäre Daten auf dem verfügbaren lokalen Speicher aufbewahrt werden sollen. (Sie können nicht standardmäßige temporäre Speichergrößen in den Maschinenkatalogen angeben, die diese Verbindung verwenden.) **Ausnahme:** Bei der Verwendung von Clustered Storage Volumes (CSV) lässt Microsoft System Center Virtual Machine Manager nicht zu, dass temporäre Daten-Cache-Datenträger auf lokalem Speicher erstellt werden. Versuche, diese Speicherverwaltungskonfiguration in der Konsole **Verwalten** zu konfigurieren, schlagen fehl.

Wenn Sie gemeinsam genutzten Speicher in einem Citrix Hypervisor-Pool verwenden, geben Sie an, ob Sie IntelliCache verwenden möchten, um die Last auf dem gemeinsam genutzten Speichergerät zu reduzieren. Siehe Citrix Hypervisor-Virtualisierungsumgebungen.

Schritt 2c: Speicherauswahl



Weitere Informationen zur Speicherauswahl finden Sie unter Hostspeicher.

Wählen Sie mindestens ein Hostspeichergerät für jeden verfügbaren Datentyp aus. Die auf der vorherigen Seite ausgewählte Speicherverwaltungsmethode beeinflusst, welche Datentypen auf dieser Seite zur Auswahl stehen. Sie müssen mindestens ein Speichergerät für jeden unterstützten Datentyp auswählen, bevor Sie im Assistenten zur nächsten Seite wechseln können.

Der untere Bereich der Seite **Speicherauswahl** enthält weitere Konfigurationsoptionen, wenn Sie von Hypervisoren gemeinsam genutzten Speicher ausgewählt und **Temporäre Daten auf verfügbarem lokalen Speicher optimieren** aktiviert haben. Sie können auswählen, welche lokalen Speichergeräte (im selben Hypervisor-Pool) für temporäre Daten verwendet werden sollen.

Die Anzahl der aktuell ausgewählten Speichergeräte wird angezeigt (in der Grafik: „1 Speichergerät ausgewählt“). Wenn Sie den Mauszeiger über diesen Eintrag bewegen, werden die Namen der ausgewählten Geräte angezeigt (es sei denn, es sind keine Geräte konfiguriert).

1. Wählen Sie **Auswählen**, um die zu verwendenden Speichergeräte zu ändern.

2. Wählen oder deaktivieren Sie im Dialogfeld **Speicher auswählen** die Kontrollkästchen für die Speichergeräte und wählen Sie dann **OK**.

Schritt 2d: Region

(Wird nur für bestimmte Hosttypen angezeigt.) Die Regionsauswahl gibt an, wo VMs bereitgestellt werden. Idealerweise wählen Sie eine Region in der Nähe des Standorts, von dem aus Benutzer auf ihre Anwendungen zugreifen.

Schritt 2e: Netzwerk

Geben Sie einen Namen für die Ressourcen ein. Dieser Name wird in der Konsole **Verwalten** angezeigt, um die mit der Verbindung verknüpfte Speicher- und Netzwerkkombination zu identifizieren. Wählen Sie ein oder mehrere Netzwerke aus, die die VMs verwenden.

Einige Verbindungstypen (wie Azure Resource Manager) listen auch Subnetze auf, die von VMs verwendet werden. Wählen Sie ein oder mehrere Subnetze aus.

Schritt 2f: Zusammenfassung

Überprüfen Sie Ihre Auswahl; wenn Sie Änderungen vornehmen möchten, kehren Sie zu den vorherigen Assistentenseiten zurück. Wenn Sie Ihre Überprüfung abgeschlossen haben, wählen Sie **Fertig stellen**.

Hinweis: Wenn Sie temporäre Daten lokal speichern, können Sie nicht standardmäßige Werte für die temporäre Datenspeicherung konfigurieren, wenn Sie den Katalog erstellen, der Maschinen enthält, die diese Verbindung verwenden.

> **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 einziges Image verwenden, um sowohl domänengebundene als auch nicht-domänengebundene VDAs zu erstellen.

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

Installieren Sie die Citrix VM Tools auf der Vorlagen-VM, damit jede VM die xe CLI oder XenCenter verwenden kann. Die VM-Leistung kann langsam sein, wenn Sie die Tools nicht installieren. Ohne die Tools können Sie Folgendes nicht tun:

- Eine VM sauber herunterfahren, neu starten oder anhalten.
- Die VM-Leistungsdaten in XenCenter anzeigen.
- Eine laufende VM migrieren (über `XenMotion`).
- Snapshots oder Snapshots mit Speicher (Checkpoints) erstellen und zu Snapshots zurückkehren.
- Die Anzahl der vCPUs auf einer laufenden Linux-VM anpassen.

1. Führen Sie den folgenden Befehl aus, um die Citrix VM Tools namens guest-tools.iso zu mounten.

   ```
   sudo mount /dev/cdrom /mnt
   ```

2. Führen Sie den folgenden Befehl aus, um das `xe-guest-utilities`-Paket basierend auf Ihrer Linux-Distribution zu installieren.

   Für RHEL/CentOS/Rocky Linux:

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

   Für Ubuntu/Debian:

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

   Für SUSE:

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

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

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

> **Hinweis:**

> Um einen aktuell ausgeführten VDA als Vorlagen-VM zu verwenden, überspringen Sie diesen Schritt.

> Bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Runtime 6.0.

> Führen Sie je nach Linux-Distribution den folgenden Befehl aus, um die Umgebung für den Linux VDA einzurichten:

Für RHEL/CentOS/Rocky Linux:

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

> **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/de-de/epel/>`.

> - Nach der Installation des Linux VDA auf RHEL 8.x/9.x und Rocky Linux 8.x/9.x, die auf GCP gehostet werden, kann die Ethernet-Verbindung verloren gehen und der Linux VDA nach einem VM-Neustart unerreichbar sein. Um dieses Problem zu umgehen, führen Sie die folgenden Befehle aus, bevor Sie die VM neu starten:

```
nmcli dev connect eth0

service NetworkManager restart
```

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE:

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

Schritt 3c: Repositories zum Installieren des Pakets tdb-tools aktivieren (nur für RHEL 7)

Für RHEL 7-Server:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

Für RHEL 7 Workstation:

```
subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

Schritt 3d: (Unter SUSE) ntfs-3g manuell installieren

Auf der SUSE-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

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

```
sudo zypper install gcc

sudo zypper install make
```

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

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

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

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

5. Installieren Sie ntfs-3g:

```
./configure

make

make install
```

Schritt 3e: Eine zu verwendende Datenbank angeben

Als experimentelle Funktion können Sie zusätzlich zu PostgreSQL auch SQLite verwenden. Sie können auch nach der Installation des Linux VDA-Pakets zwischen SQLite und PostgreSQL wechseln. Gehen Sie dazu wie folgt vor:

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

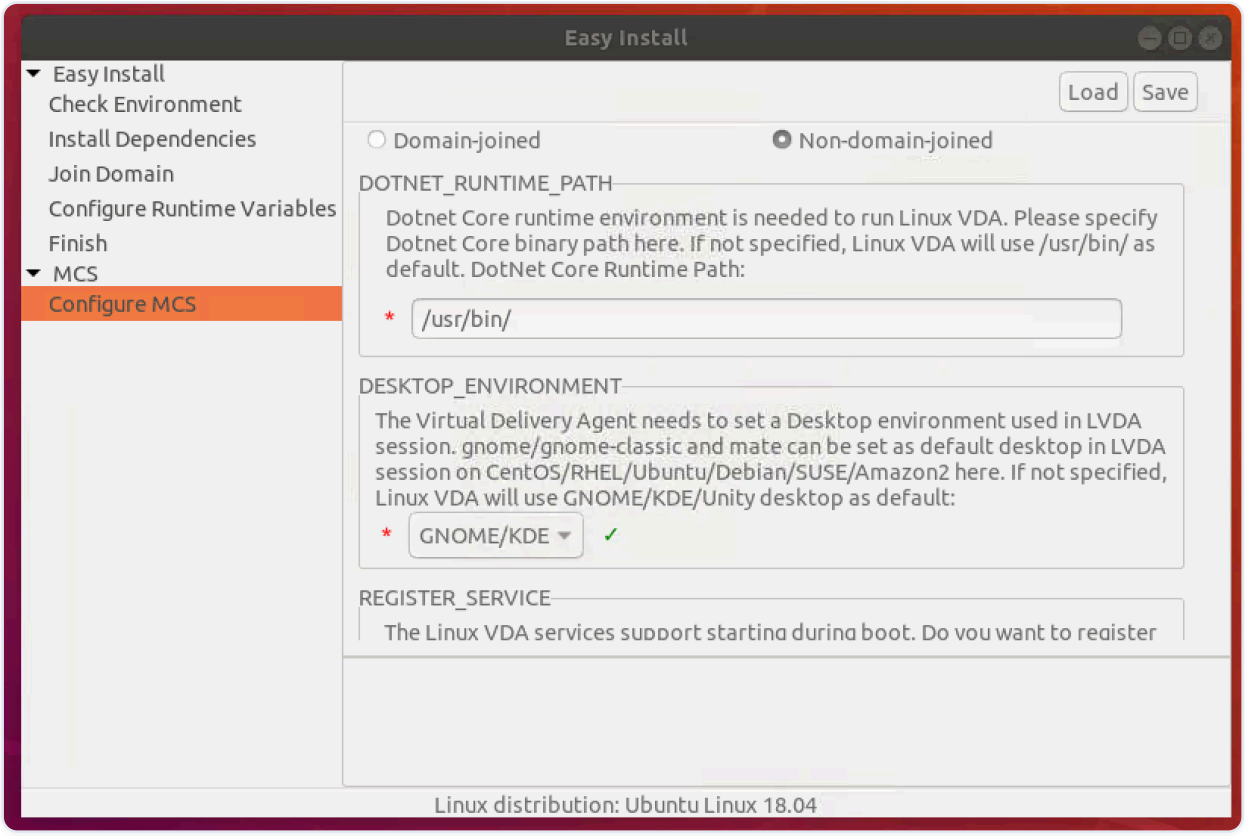
Hinweis:

- Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.
- Für eine einfache Installation und MCS können Sie zwischen SQLite und PostgreSQL wechseln, ohne diese manuell installieren zu müssen. Sofern nicht anders über `/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, MCS-Variablen zu konfigurieren:

- Bearbeiten Sie die `/etc/xdl/mcs/mcs.conf`-Datei.
- Verwenden Sie die GUI für die einfache Installation. Um die GUI für die einfache Installation zu öffnen, führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktop-Umgebung Ihres Linux VDA aus.



> **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 nicht in die Domäne eingebundene Szenarien konfigurieren. Sie können die Standardwerte der Variablen verwenden oder die Variablen bei Bedarf anpassen (optional):

`DOTNET_RUNTIME_PATH`=*path-to-install-dotnet-runtime **

`DESKTOP_ENVIRONMENT`= *gnome | mate ** `REGISTER_SERVICE`=**J | N**

`ADD_FIREWALL_RULES`=**J | N** `VDI_MODE`=**J | N**

`START_SERVICE`=**J | N**

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

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

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

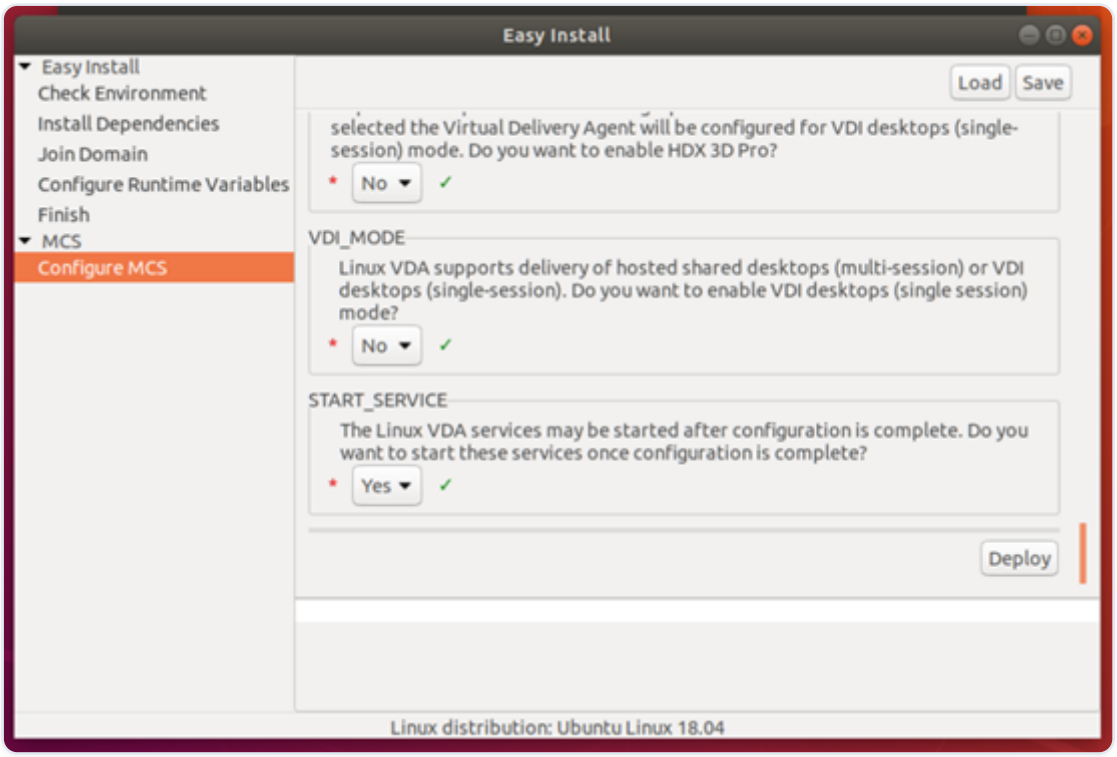
Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
```

```
update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -v "Flags" -d "0x00000003"
```

Schritt 3h: Ein Masterimage erstellen

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, überschreiben die in der GUI festgelegten Variablen die Variablen, die Sie in der `/etc/xdl/mcs/mcs.conf`-Datei festgelegt haben.

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

   - **(Für 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.
   - **(Für Azure)** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM über das Azure-Portal herunter. Stellen Sie sicher, dass der Energiestatus der Vorlagen-VM **Beendet (Zuordnung aufgehoben)** anzeigt. Merken Sie sich hier den Namen der Ressourcengruppe. Sie benötigen den Namen, um Ihr Masterimage in Azure zu finden.

     Angehaltener Energiestatus der Vorlagen-VM(/en-us/linux-virtual-delivery-agent/2308/media/stopped-deallocated2.png)
   - **(Für AWS)** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM über das AWS EC2-Portal herunter. Stellen Sie sicher, dass der Instanzstatus der Vorlagen-VM **Beendet** anzeigt. Klicken Sie mit der rechten Maustaste auf die Vorlagen-VM und wählen Sie **Image > Image erstellen**. Geben Sie Informationen ein und nehmen Sie die erforderlichen Einstellungen vor. Klicken Sie auf **Image erstellen**.

Erstellen eines EBS-Images(/en-us/linux-virtual-delivery-agent/2308/media/create-ebs-image.png)

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

> **Hinweis:**
>
> Sie müssen Acropolis-Snapshot-Namen mit `XD_` präfixieren, um sie in Citrix Virtual Apps™ and Desktops verwenden zu können. Verwenden Sie die Acropolis-Konsole, um Ihre Snapshots bei Bedarf umzubenennen. Nachdem Sie einen Snapshot umbenannt haben, starten Sie den Assistenten **Katalog erstellen** neu, um eine aktualisierte Liste zu erhalten.

Schritt 4: Maschinenkatalog erstellen

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 Maschinenkataloge**.
4. Der Assistent führt Sie durch die Erstellung eines Maschinenkatalogs.

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

   Wählen Sie auf der Seite **Masterimage** den Image-Snapshot aus.

   Auf der Seite **Virtuelle Maschinen** prüfen Sie die Anzahl der virtuellen CPUs und die Anzahl der Kerne pro vCPU. Wählen Sie MCS als Methode zur Maschinenbereitstellung und wählen Sie **Nicht in Domäne eingebunden** als Identität für die im Katalog zu erstellenden Maschinen.

   Führen Sie bei Bedarf weitere Konfigurationsaufgaben aus. Weitere Informationen finden Sie unter Maschinenkataloge erstellen.

> **Hinweis:**
>
> Wenn der Erstellungsprozess Ihres Maschinenkatalogs auf dem Delivery Controller™ viel Zeit in Anspruch nimmt, wechseln Sie zu Nutanix Prism und schalten Sie die Maschine, die

mit **Preparation** beginnt, manuell ein. Dieser Ansatz hilft, den Erstellungsprozess fortzusetzen.

Schritt 5: Eine Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Sie legt fest, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

Linux-VDAs mit Machine Creation Services™ (MCS) erstellen

Sie können domänenverbundene und nicht-domänenverbundene VDAs mit MCS erstellen.

Wichtig:

Die folgenden wichtigen Änderungen gelten ab Release 2212:

- Diese Variable **AD_INTEGRATION** in der Datei /etc/xdl/mcs/mcs.conf oder in der Easy Install-GUI hat keinen Standardwert mehr. Sie müssen einen Wert nach Bedarf 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 **enabled** oder **disabled**, sondern **Y** oder **N**. Weitere Informationen finden Sie im Abschnitt Automatisches Aktualisieren von Maschinenkontokennwörtern 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

	WINBIND	SSSD	CENTRIFY	PBIS
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 RHEL 8.x/9.x- oder Rocky Linux 8.x/9.x-VDA, der über SSSD mit der Domäne verbunden ist, als Vorlagen-VM für MCS zu verwenden, stellen Sie sicher, dass:

- Der VDA manuell und nicht über die einfache Installation installiert wird. Die einfache Installation verwendet **Adcli** für RHEL 8.x/9.x und Rocky Linux 8.x/9.x, und die Kombination aus SSSD und **Adcli** wird von MCS nicht unterstützt.
- Ein Samba-Server so konfiguriert ist, dass er SSSD für die AD-Authentifizierung verwendet. Weitere Informationen finden Sie im Red Hat-Artikel unter `<https://access.redhat.com/solutions/3802321>`.

Unterstützte Hypervisoren

- AWS
- Citrix Hypervisor™
- GCP
- Microsoft Azure
- Nutanix AHV

- VMware vSphere

Unerwartete Ergebnisse können auftreten, wenn Sie versuchen, ein Masterimage auf anderen als den unterstützten Hypervisoren vorzubereiten.

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 Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) hosten. Um diese Hostverbindungen für öffentliche Clouds zu Ihrer Citrix Virtual Apps and Desktops-Bereitstellung hinzuzufügen, benötigen Sie Citrix Universal Subscription- oder Hybrid Rights-Lizenzen. Informationen zu Universal Subscription- und Hybrid Rights-Lizenzen finden Sie unter Transition and Trade Up (TTU) with Citrix Universal Subscription.
- Bare-Metal-Server werden nicht zur Verwendung mit MCS zum Erstellen virtueller Maschinen unterstützt.
- Citrix® verwendet die folgenden Centrify-Versionen für die anfängliche Funktionsvalidierung auf den relevanten Linux-Distributionen:

LINUX-DISTRIBUTION	CENTRIFY-VERSION
RHEL 7/8	5.8.0
SUSE	5.7.1
Debian, Ubuntu	5.6.1

  Die Verwendung anderer Centrify-Versionen kann zu Fehlern führen. Verwenden Sie Centrify nicht, um eine Vorlagenmaschine einer Domäne beizutreten.
- Wenn Sie PBIS oder Centrify verwenden, um von MCS erstellte Maschinen Windows-Domänen beizutreten, führen Sie die folgenden Aufgaben aus:
  - Konfigurieren Sie auf der Vorlagenmaschine den Downloadpfad des PBIS- oder Centrify-Pakets in der Datei `/etc/xdl/mcs/mcs.conf` oder installieren Sie das PBIS- oder Centrify-Paket direkt.
  - Bevor Sie `/opt/Citrix/VDA/sbin/deploymcs.sh` ausführen, erstellen Sie eine Organisationseinheit (OU), die Schreib- und Kennwortrücksetzberechtigungen für alle untergeordneten, von MCS erstellten Maschinen besitzt.

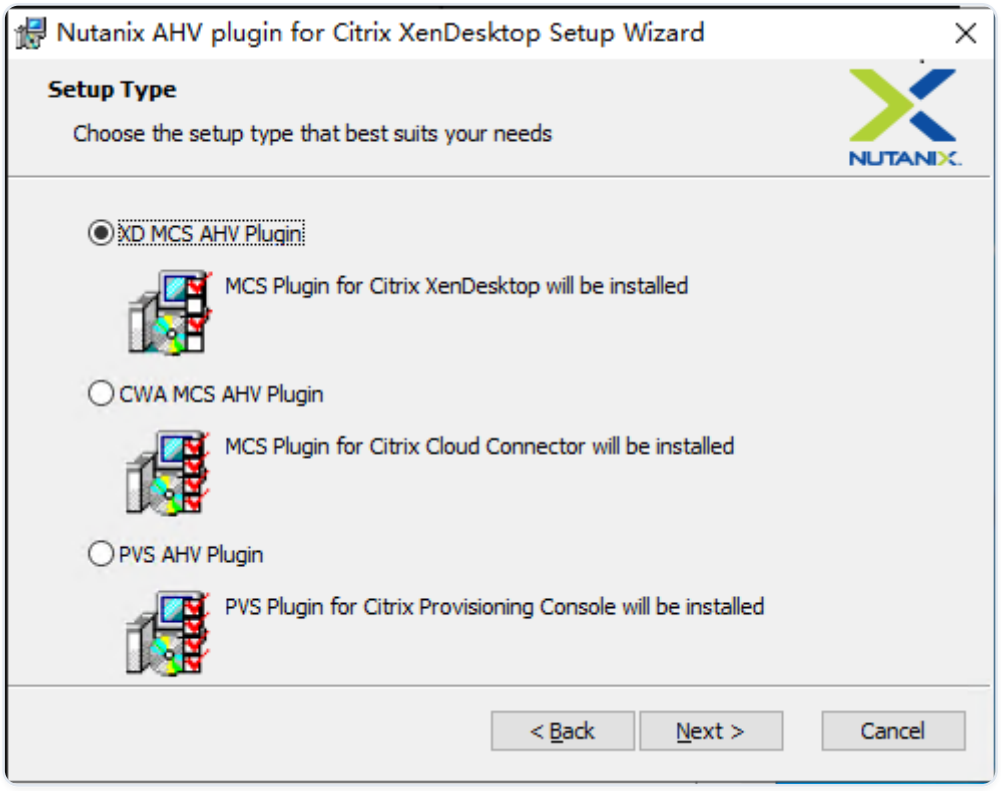
- Bevor Sie von MCS erstellte Maschinen neu starten, nachdem `/opt/Citrix/VDA/sbin/deploymcs.sh` abgeschlossen ist, führen Sie `klist -li 0x3e4 purge` auf Ihrem Delivery Controller oder auf Ihrem Citrix Cloud Connector aus, je nach Ihrer Bereitstellung.

(Nur für Nutanix) Schritt 1: Installieren und registrieren Sie das Nutanix AHV-Plug-In

Beziehen Sie das Nutanix AHV-Plug-In-Paket von Nutanix. Installieren und registrieren Sie das Plug-In in Ihrer Citrix Virtual Apps and Desktops-Umgebung. Weitere Informationen finden Sie im Installationshandbuch für das Nutanix Acropolis MCS-Plug-In, das im Nutanix Support Portal verfügbar ist.

Schritt 1a: Installieren und registrieren Sie das Nutanix AHV-Plug-In für lokale Delivery Controller

Nachdem Sie Citrix Virtual Apps and Desktops™ installiert haben, wählen und installieren Sie das **XD MCS AHV Plugin** auf Ihren Delivery Controllern.



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

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

Schritt 1c: Führen Sie die folgenden Schritte nach der Installation des Plug-ins aus

- Stellen Sie sicher, dass ein Nutanix Acropolis-Ordner in `C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0` erstellt wurde.
- Führen Sie den Befehl `"C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe" -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"` aus.
- Starten Sie die Citrix Host-, Citrix Broker- und Citrix Machine Creation Services auf Ihren lokalen Delivery Controllern neu oder starten Sie den Citrix RemoteHCLServer-Dienst auf den Citrix Cloud Connectors neu.

> **Tipp:**
>
> Wir empfehlen, die Citrix Host-, Citrix Broker- und Machine Creation Services zu beenden und dann neu zu starten, wenn Sie das Nutanix AHV-Plug-in installieren oder aktualisieren.

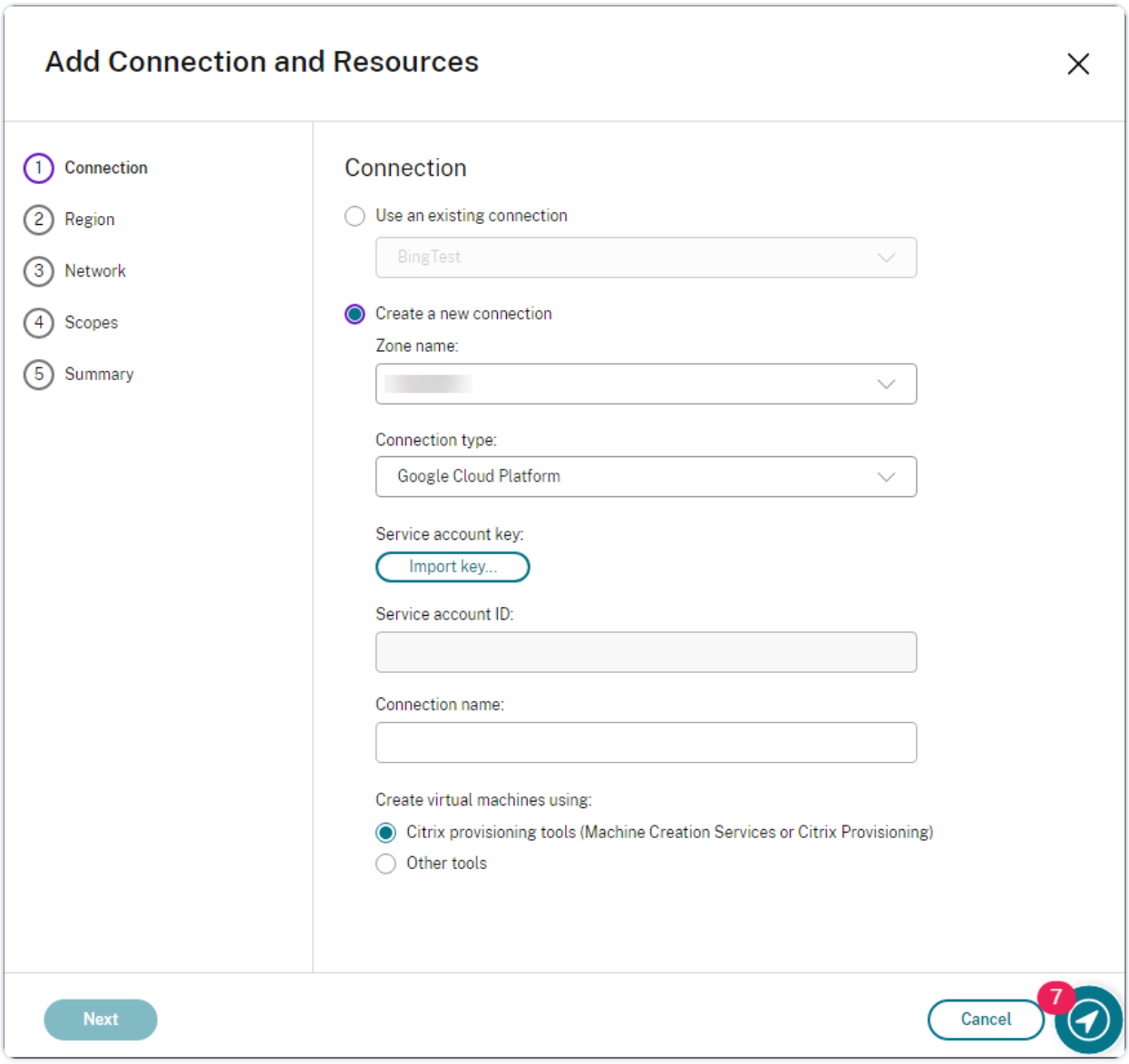
Schritt 2: Hostverbindung erstellen

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

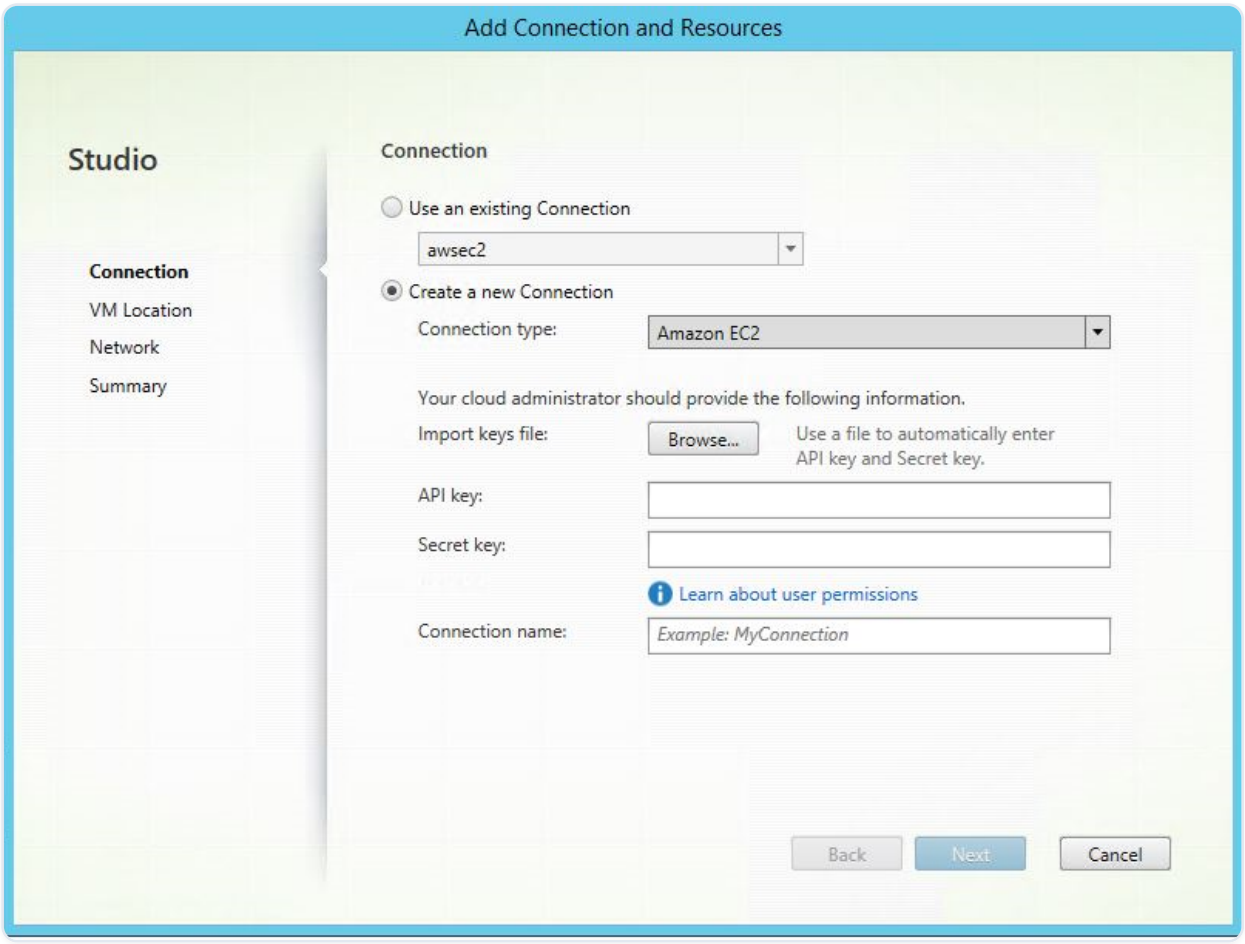
1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im oberen linken Menü **My Services > DaaS**.
3. Wählen Sie unter **Manage > Full Configuration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste **Verbindung und Ressourcen hinzufügen** aus.



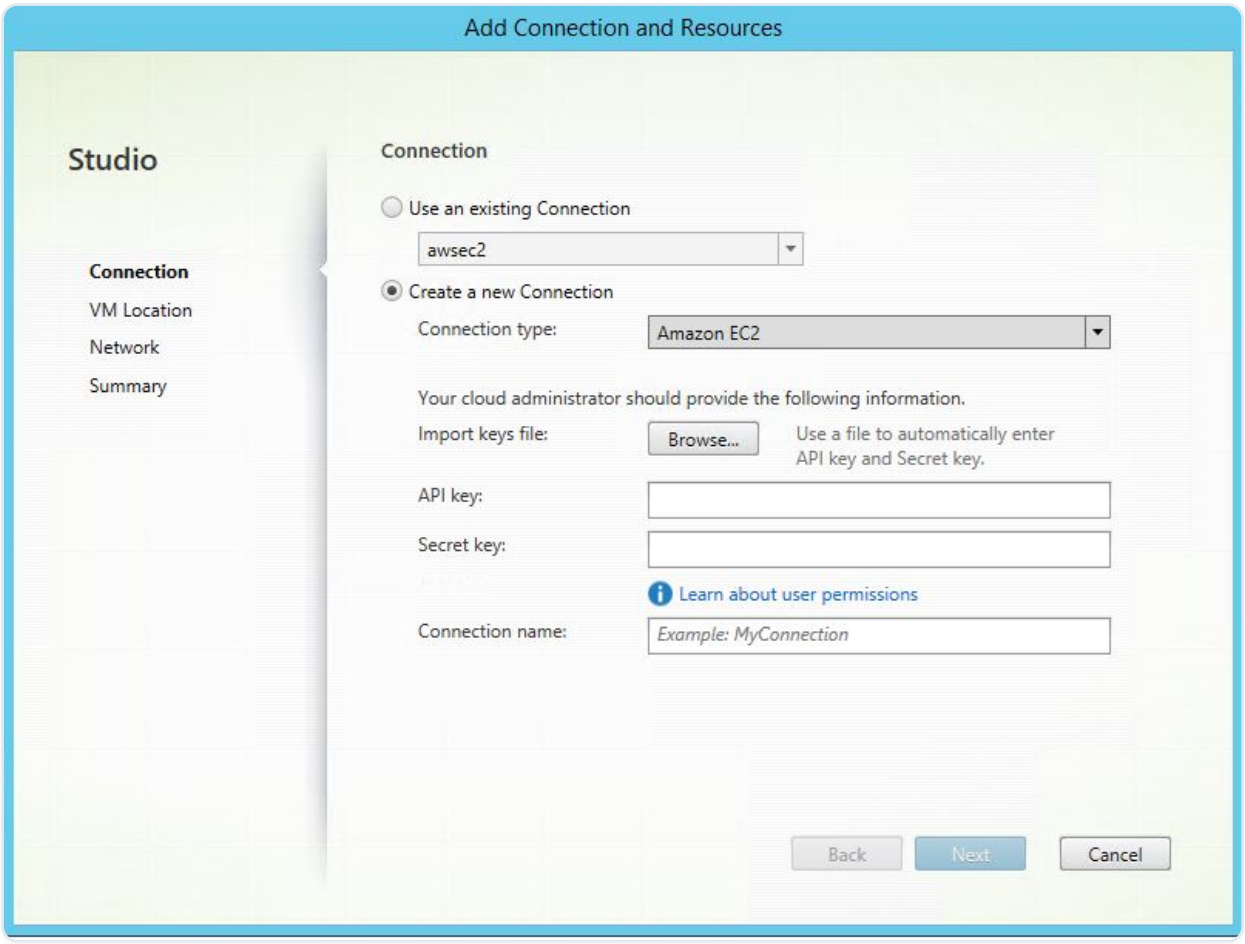
5. Wählen Sie Microsoft Azure als Verbindungstyp aus.
6. Der Assistent führt Sie durch die Seiten. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Nachdem Sie jede Seite ausgefüllt haben, wählen Sie **Next**, bis Sie die Seite **Summary** erreichen. Weitere Informationen finden Sie unter **Schritt 2: Hostverbindung erstellen** im Artikel Erstellen von nicht in die Domäne eingebundenen Linux-VDAs.

Hostverbindung zu AWS in Citrix Studio erstellen

1. Wählen Sie in Citrix Studio **Configuration** > **Hosting** > **Add Connection and Resources**.
2. Wählen Sie **Amazon EC2** als Verbindungstyp aus.



3. Geben Sie den API-Schlüssel und den geheimen Schlüssel Ihres AWS-Kontos sowie den Namen Ihrer Verbindung ein.



Der **API-Schlüssel** ist Ihre Zugriffsschlüssel-ID und der **geheime Schlüssel** ist Ihr geheimer Zugriffsschlüssel. Sie werden als Zugriffsschlüsselpaar betrachtet. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, können Sie den Zugriffsschlüssel löschen und einen neuen erstellen. Gehen Sie wie folgt vor, um einen Zugriffsschlüssel zu erstellen:

a. Melden Sie sich bei den AWS-Diensten an.
b. Navigieren Sie zur Konsole für Identity and Access Management (IAM).
c. Wählen Sie im linken Navigationsbereich **Users**.
d. Wählen Sie den Zielbenutzer aus und scrollen Sie nach unten, um die Registerkarte **Sicherheitsanmeldeinformationen** auszuwählen.
e. Scrollen Sie nach unten und klicken Sie auf **Zugriffsschlüssel erstellen**. Ein neues Fenster wird angezeigt.
f. Klicken Sie auf **.csv-Datei herunterladen** und speichern Sie den Zugriffsschlüssel an einem sicheren Ort.

4. Der Assistent führt Sie durch die Seiten. Der spezifische Seiteninhalt hängt vom ausgewählten Verbindungstyp ab. Nachdem Sie jede Seite ausgefüllt haben, wählen Sie **Weiter**, bis Sie die Seite **Zusammenfassung** erreichen.

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** aus.
5. Wählen Sie **Citrix Hypervisor** als Verbindungstyp.
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 zu erstellen.

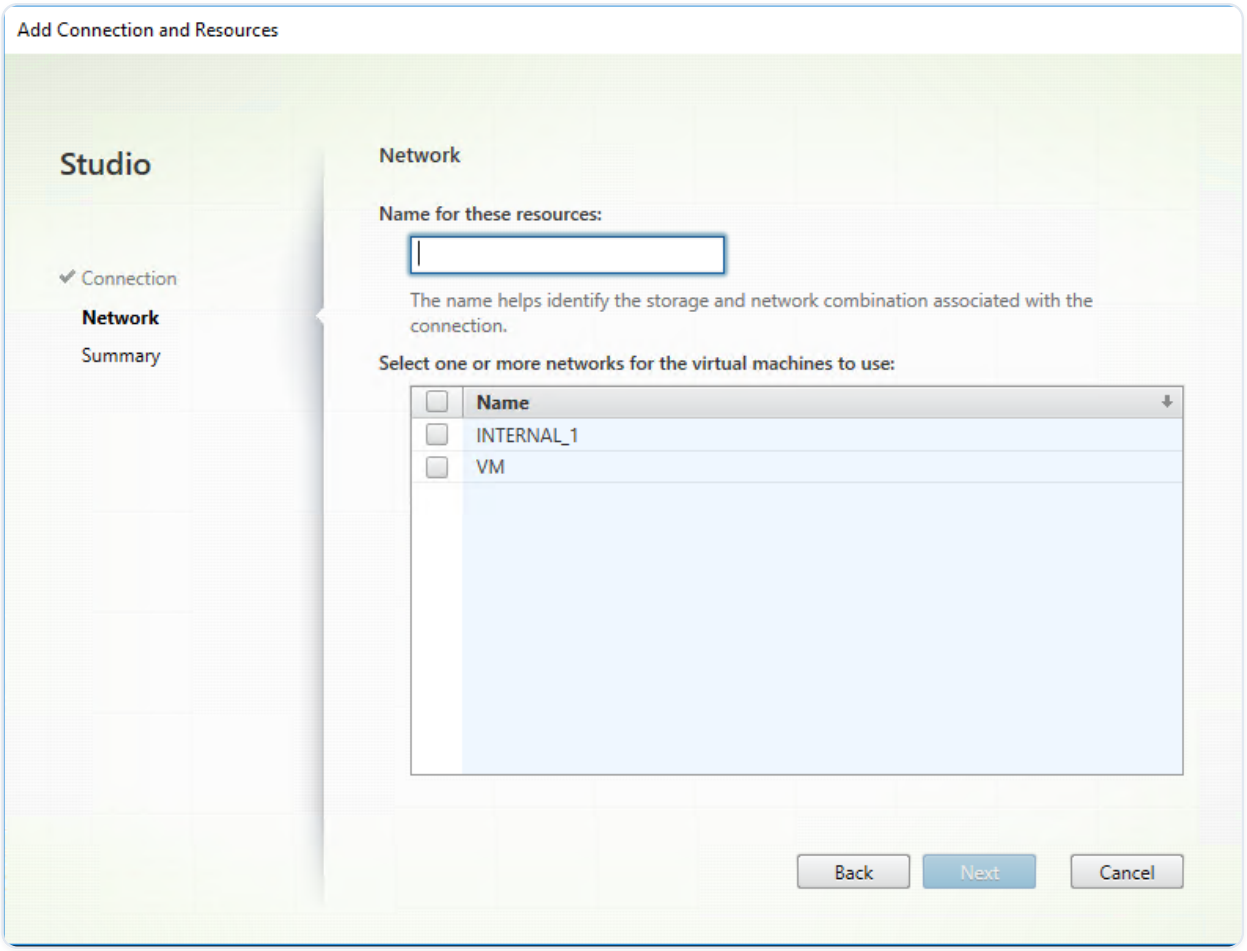
1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie im Menü oben links **Meine Dienste > DaaS**.
3. Wählen Sie unter **Verwalten > Vollständige Konfiguration** im linken Bereich **Hosting**.
4. Wählen Sie in der Aktionsleiste **Verbindung und Ressourcen hinzufügen** aus.
5. Wählen Sie **Google Cloud Platform** als Verbindungstyp.
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. Nachdem Sie jede Seite ausgefüllt haben, wählen Sie **Weiter**, bis Sie die Seite **Zusammenfassung** erreichen. Weitere Informationen finden Sie unter **Schritt 2: Hostverbindung erstellen** im Artikel Nicht in Domäne eingebundene Linux-VDAs erstellen.

Hostverbindung zu Nutanix in Citrix Studio erstellen

1. Wählen Sie für lokale Delivery Controller in der lokalen Citrix Studio die Option **Konfiguration > Hosting > Verbindung und Ressourcen hinzufügen**. Wählen Sie für Cloud Delivery Controller in der webbasierten Studio-Konsole in Citrix Cloud die Option **Verwalten > Hosting > Verbindung und Ressourcen hinzufügen**, um eine Verbindung zum Nutanix-Hypervisor herzustellen.
2. Wählen Sie im Assistenten **Verbindung und Ressourcen hinzufügen** auf der Seite **Verbindung** Nutanix AHV als Verbindungstyp aus und geben Sie dann die Hypervisor-

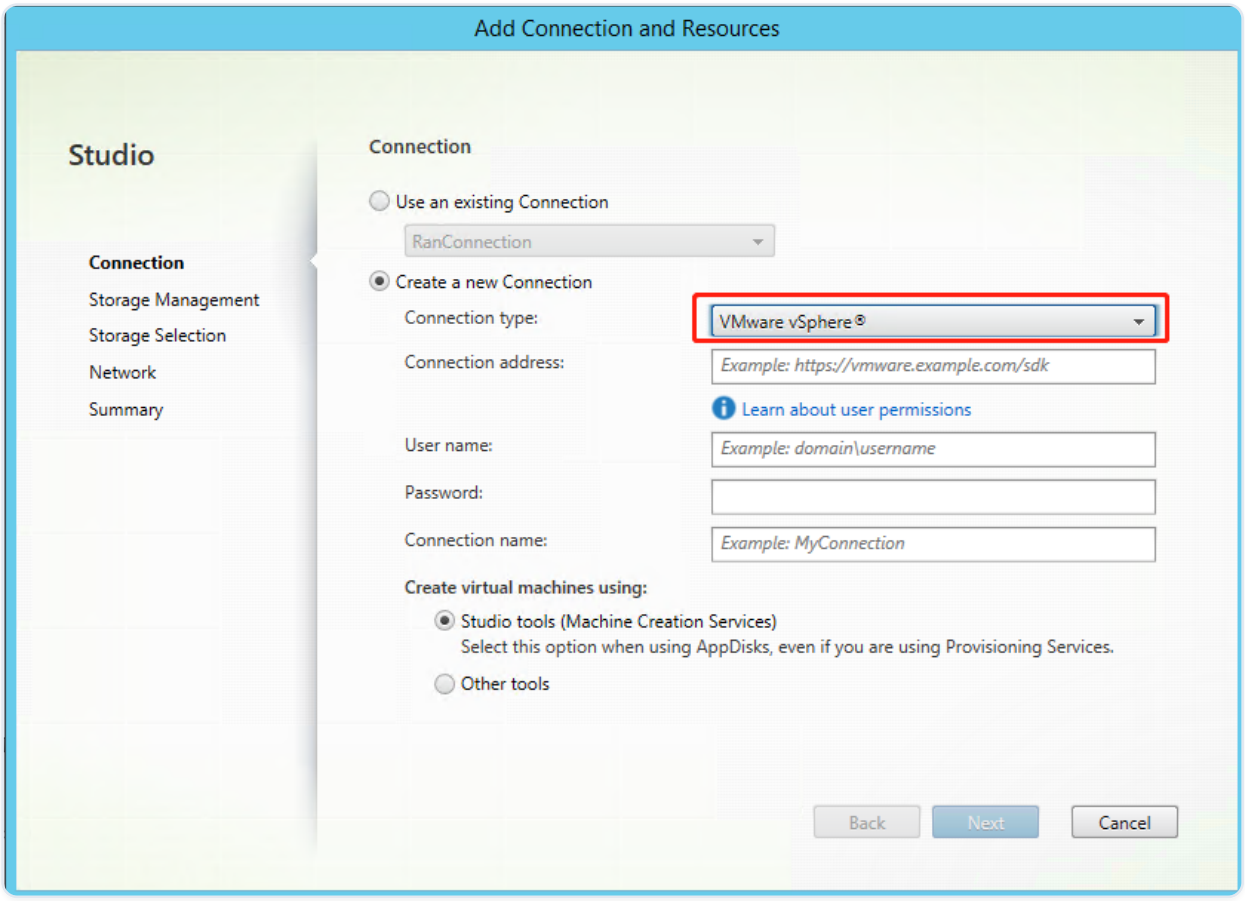
Adresse, die Anmeldeinformationen und Ihren Verbindungsnamen an. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Einheit aus.

Zum Beispiel in der lokalen Citrix Studio:

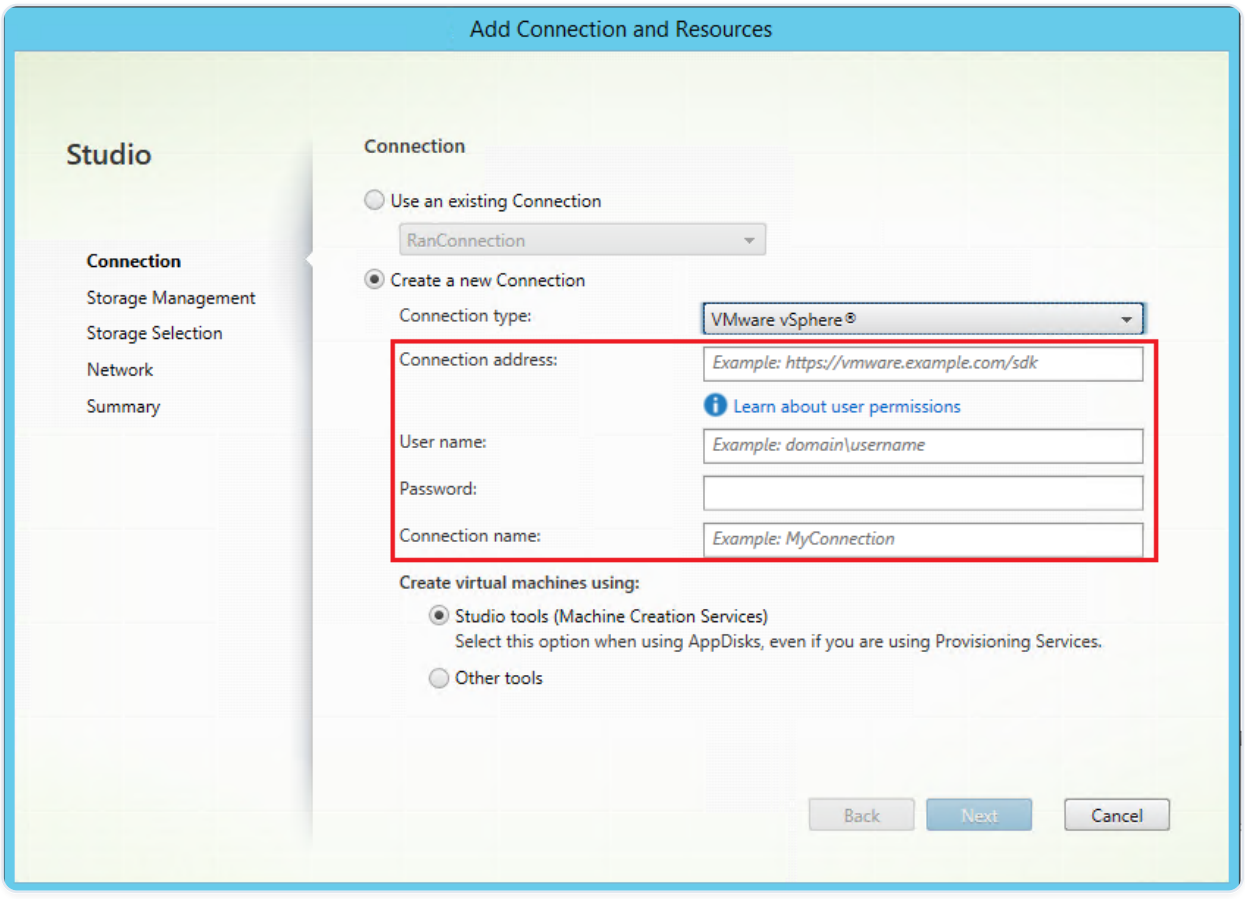


Hostverbindung zu VMware in Citrix Studio erstellen

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 VMware vSphere als Verbindungstyp aus.



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



Schritt 3: Masterimage vorbereiten

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

Installieren Sie die Citrix VM Tools auf der Vorlagen-VM, damit jede VM die xe CLI oder XenCenter verwenden kann. Die VM-Leistung kann langsam sein, wenn Sie die Tools nicht installieren. Ohne die Tools können Sie Folgendes nicht tun:

- Eine VM sauber herunterfahren, neu starten oder anhalten.
- Die VM-Leistungsdaten in XenCenter anzeigen.
- Eine laufende VM migrieren (über `XenMotion`).
- Snapshots oder Snapshots mit Arbeitsspeicher (Checkpoints) erstellen und zu Snapshots zurückkehren.
- Die Anzahl der vCPUs auf einer laufenden Linux-VM anpassen.

1. Führen Sie den folgenden Befehl aus, um die Citrix VM Tools namens guest-tools.iso zu mounten.

   ```
   sudo mount /dev/cdrom /mnt
   ```

2. Führen Sie den folgenden Befehl aus, um das `xe-guest-utilities`-Paket basierend auf Ihrer Linux-Distribution zu installieren.

   Für RHEL/CentOS/Rocky Linux:

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

   Für Ubuntu/Debian:

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

   Für SUSE:

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

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

Schritt 3b: Konfigurationen für SUSE 15.4 unter AWS, Azure und GCP überprüfen

Stellen Sie für SUSE 15.4 unter AWS, Azure und GCP sicher, dass:

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

Schritt 3c: RDNS für Ubuntu 20.04 auf GCP deaktivieren

Fügen Sie auf der Vorlagen-VM die Zeile **rdns = false** unter in /etc/krb5.conf hinzu.

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

> **Hinweis:**
>
> - Um einen aktuell ausgeführten VDA als Vorlagen-VM zu verwenden, überspringen Sie diesen Schritt. Um einen aktuell ausgeführten RHEL 8.x/9.x- oder Rocky Linux 8.x/9.x-VDA, der über SSSD mit der Domäne verbunden ist, als Vorlagen-VM zu verwenden, stellen Sie sicher, dass:
>   - Der VDA manuell und nicht über die einfache Installation installiert wurde. Die einfache Installation verwendet **Adcli** für RHEL 8.x/9.x und Rocky Linux 8.x/9.x, und die Kombination aus SSSD und **Adcli** wird von MCS nicht unterstützt.
>   - Ein Samba-Server für die AD-Authentifizierung SSSD verwendet. Weitere Informationen finden Sie im Red Hat-Artikel unter `<https://access.redhat.com/solutions/3802321>`.
> - Bevor Sie das Linux VDA-Paket auf der Vorlagen-VM installieren, installieren Sie .NET Runtime 6.0.

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

Für 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/de-de/epel/>`.
- Bevor Sie den Linux VDA auf RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 installieren, aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher.

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

Für Ubuntu/Debian:

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



apt-get install -f
```

Für SUSE:

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

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

Für RHEL 7-Server:

```
subscription-manager repos --enable=rhel-7-server-optional-rpms
```

Für RHEL 7-Workstation:

```
subscription-manager repos --enable=rhel-7-workstation-optional-rpms
```

Schritt 3f: (Unter SUSE) ntfs-3g manuell installieren

Auf der SUSE-Plattform stellt kein Repository ntfs-3g bereit. Laden Sie den Quellcode herunter, kompilieren und installieren Sie ntfs-3g manuell:

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

```
sudo zypper install gcc

sudo zypper install make
```

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

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

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

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

5. Installieren Sie ntfs-3g:

```
./configure

make

make install
```

Schritt 3g: Zu verwendende Datenbank angeben

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

Hinweis:

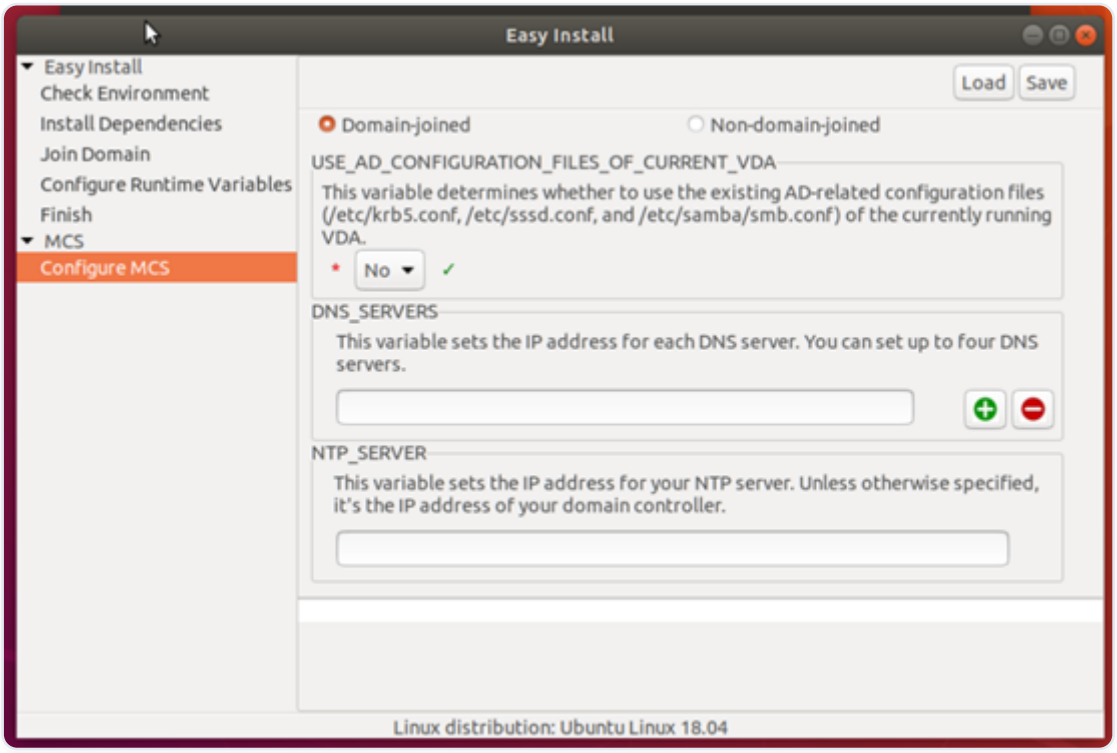
- Wir empfehlen, SQLite nur für den VDI-Modus und PostgreSQL für ein Bereitstellungsmodell mit gehosteten Shared Desktops zu verwenden.
- Für eine einfache Installation und MCS können Sie SQLite oder PostgreSQL zur Verwendung angeben, ohne sie manuell installieren zu müssen. Sofern nicht anders über **/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. Überspringen Sie diesen Schritt, 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, MCS-Variablen zu konfigurieren:

- Bearbeiten Sie die Datei `/etc/xdl/mcs/mcs.conf`.
- Verwenden Sie die einfache Installations-GUI. Um die einfache Installations-GUI zu öffnen, führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktop-Umgebung Ihres Linux VDA aus.



> **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.

Im Folgenden sind MCS-Variablen aufgeführt, die Sie für Szenarien ohne Domänenbeitritt und mit Domänenbeitritt konfigurieren können:

- **Für Szenarien ohne Domänenbeitritt**

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

`DOTNET_RUNTIME_PATH` =*Pfad-zu-install-dotnet-runtime *

`DESKTOP_ENVIRONMENT` = *gnome | mate ** `REGISTER_SERVICE` =**J | N**

`ADD_FIREWALL_RULES` =**J | N** `VDI_MODE` =**J | N**

`START_SERVICE` =**J | N**

- **Für Szenarien mit Domänenbeitritt**
  - `Use_AD_Configuration_Files_Of_Current_VDA`: Legt fest, ob die vorhandenen AD-bezogenen Konfigurationsdateien (/etc/krb5.conf, /etc/sssd.conf und /etc/samba/smb.conf) des aktuell ausgeführten VDA verwendet werden sollen. Wenn auf Y gesetzt, sind die Konfigurationsdateien auf MCS-erstellten Maschinen dieselben wie die entsprechenden auf dem aktuell ausgeführten VDA. Sie müssen jedoch weiterhin die Variablen `dns` und `AD_INTEGRATION` konfigurieren. Der Standardwert ist N, was bedeutet, dass die Konfigurationsvorlagen auf dem Masterimage die Konfigurationsdateien auf MCS-erstellten Maschinen bestimmen. Um einen aktuell ausgeführten VDA als Vorlagen-VM zu verwenden, setzen Sie den Wert auf Y. Andernfalls setzen Sie ihn auf N.
  - `dns`: Legt die IP-Adresse für jeden DNS-Server fest. Sie können bis zu vier DNS-Server einrichten.
  - `NTP_SERVER`: Legt die IP-Adresse für Ihren NTP-Server fest. Sofern nicht anders angegeben, ist dies die IP-Adresse Ihres Domänencontrollers.
  - `WORKGROUP`: Legt den Arbeitsgruppennamen auf den NetBIOS-Namen (Groß-/Kleinschreibung beachten) fest, den Sie in AD konfiguriert haben. Andernfalls verwendet MCS den Teil des Domänennamens, der unmittelbar auf den Hostnamen des Computers folgt, als Arbeitsgruppennamen. Wenn das Computerkonto beispielsweise **user1.lvda.citrix.com** lautet, verwendet MCS **lvda** als Arbeitsgruppennamen, während **citrix** die richtige Wahl wäre. Stellen Sie sicher, dass Sie den Arbeitsgruppennamen korrekt festlegen.
  - `AD_INTEGRATION`: Legt Winbind, SSSD, PBIS oder Centrify fest. Eine Matrix der von MSC unterstützten Linux-Distributionen und Domänenbeitrittsmethoden finden Sie unter Unterstützte Distributionen in diesem Artikel.
  - `CENTRIFY_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Server Suite Free (ehemals Centrify Express)-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.

- `CENTRIFY_SAMBA_DOWNLOAD_PATH`: Legt den Pfad zum Herunterladen des Centrify Samba-Pakets fest. Der Wert wird nur wirksam, wenn Sie die Variable `AD_INTEGRATION` auf Centrify setzen.
- `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 setzen.
- `UPDATE_MACHINE_PW`: Aktiviert oder deaktiviert die Automatisierung von Kennwortaktualisierungen für Computerkonten. Weitere Informationen finden Sie unter Automatisieren von Kennwortaktualisierungen für Computerkonten.
- Linux VDA-Konfigurationsvariablen:

  `DOTNET_RUNTIME_PATH`=*Pfad-zur-dotnet-Laufzeitumgebung-Installation *

  `DESKTOP_ENVIRONMENT`= *gnome | mate ** `SUPPORT_DDC_AS_CNAME`=**J | N**

  `VDA_PORT`=**Portnummer** `REGISTER_SERVICE`=**J | N**

  `ADD_FIREWALL_RULES`=**J | N** `HDX_3D_PRO`=**J | N**

  `VDI_MODE`=**J | N** `SITE_NAME`=**dns-site-name | '<keine\\>'**

  `LDAP_LIST`=**'list-ldap-servers' | '<keine\\>'** `SEARCH_BASE`=**search-base-set | '<keine\\>'**

  `FAS_LIST`=**'list-fas-servers' | '<keine\\>'** `START_SERVICE`=**J | N**

  `TELEMETRY_SOCKET_PORT`=**Portnummer** `TELEMETRY_PORT`=**Portnummer**

Schritt 3i: Registrierungswerte für MCS schreiben oder aktualisieren

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

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

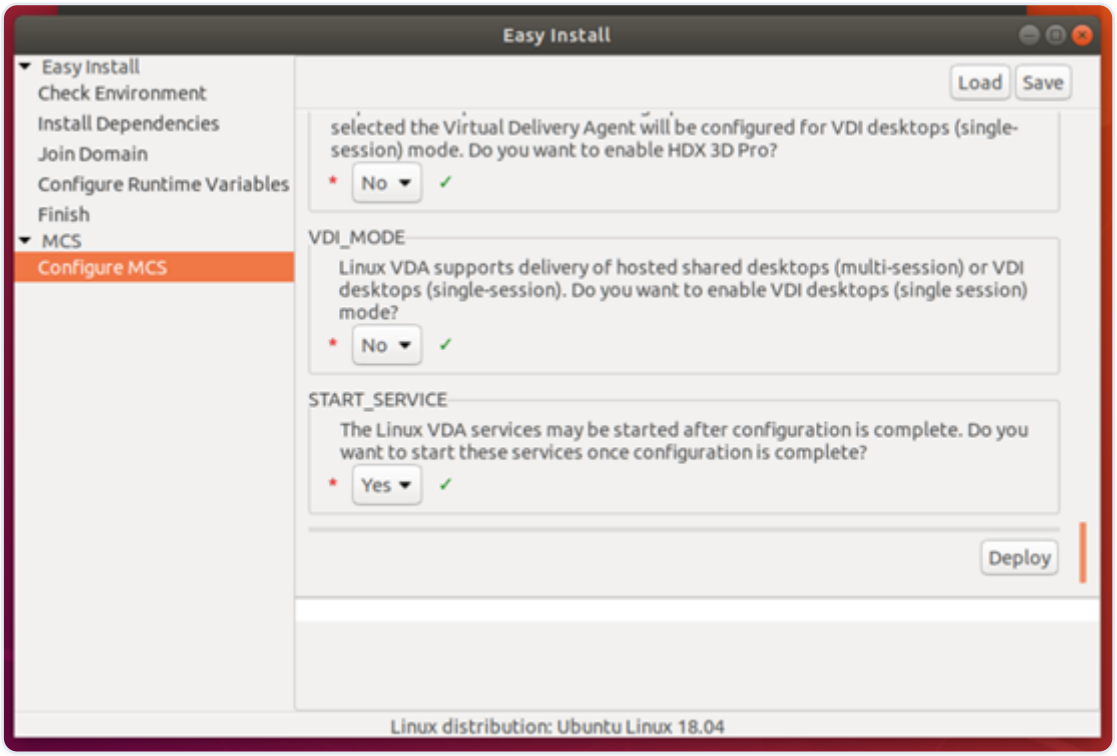
Sie können beispielsweise die folgenden Befehlszeilen zur Datei `/etc/xdl/mcs/mcs_local_setting.reg` hinzufügen, um einen Registrierungswert zu schreiben bzw. zu aktualisieren:

```
create -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -t "REG_DWORD" -v "Flags" -d "0x00000003" --force
```

```
update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Clipboard\Cl
ipboardSelection" -v "Flags" -d "0x00000003"
```

Schritt 3j: Master-Image erstellen

1. (Nur für 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, überschreiben die in der GUI festgelegten Variablen die Variablen, die Sie in der Datei `/etc/xdl/mcs/mcs.conf` festgelegt haben.

3. (Wenn Sie eine aktuell ausgeführte VDA als Vorlagen-VM verwenden oder wenn es sich um ein Szenario ohne Domänenbeitritt handelt, überspringen Sie diesen Schritt.) 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`.

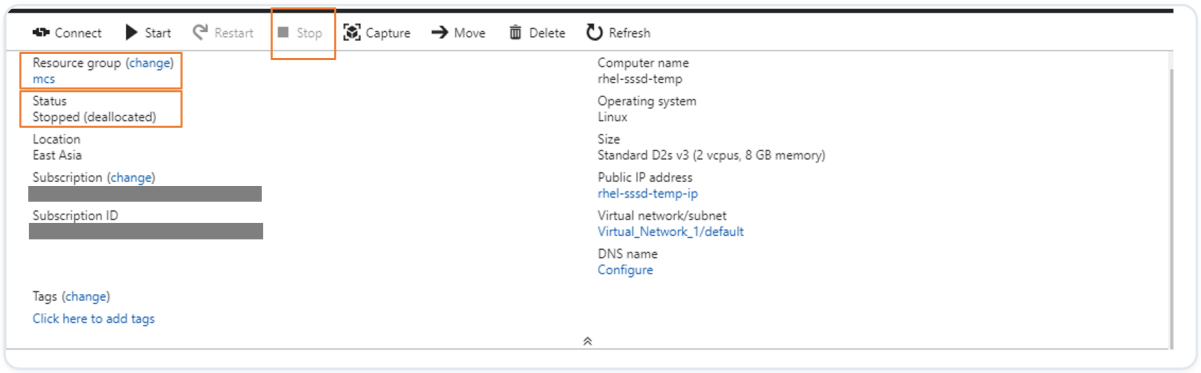
Aktualisieren Sie für SSSD-Benutzer die Vorlagen `/etc/xdl/ad_join/sssd.conf.tmpl`, `/etc/xdl/ad_join/sssd_krb5.conf.tmpl` und `/etc/xdl/ad_join/sssd_smb.conf.tmpl`.

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

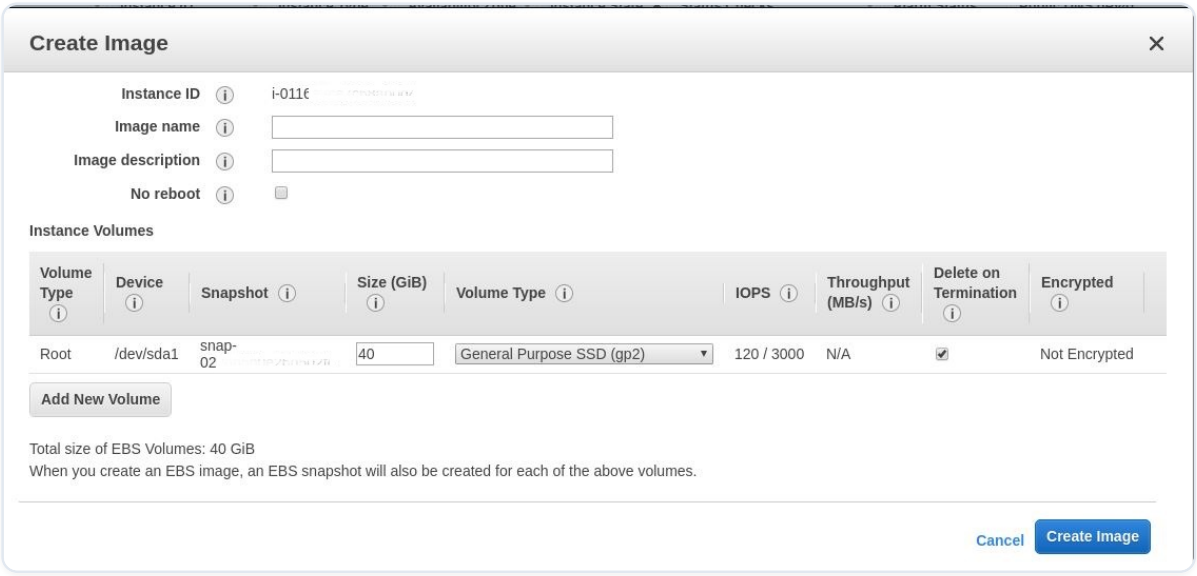
> **Hinweis:**
>
> Behalten Sie das in den Vorlagendateien verwendete Format bei und verwenden Sie Variablen wie $WORKGROUP, $REALM, $realm, ${new_hostname} und $AD_FQDN.

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

   - **(Für 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.
   - **(Für Azure)** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM über das Azure-Portal herunter. Stellen Sie sicher, dass der Energiestatus der Vorlagen-VM **Beendet (Zuordnung aufgehoben)** anzeigt. Merken Sie sich hier den Namen der Ressourcengruppe. Sie benötigen den Namen, um Ihr Masterimage in Azure zu finden.



- **(Für AWS)** Installieren Sie Anwendungen auf der Vorlagen-VM und fahren Sie die Vorlagen-VM über das AWS EC2-Portal herunter. Stellen Sie sicher, dass der Instanzstatus der Vorlagen-VM **Beendet** ist. Klicken Sie mit der rechten Maustaste auf die Vorlagen-VM und wählen Sie **Image > Create Image**. Geben Sie die erforderlichen Informationen ein und nehmen Sie die Einstellungen vor. Klicken Sie auf **Create Image**.



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

> **Hinweis:**
>
> Sie müssen Acropolis-Snapshot-Namen mit `XD_` präfixieren, um sie in Citrix Virtual Apps™ und Desktops verwenden zu können. Verwenden Sie die Acropolis-Konsole, um Ihre Snapshots bei Bedarf umzubenennen. Nachdem Sie einen Snapshot umbenannt haben, starten Sie den Assistenten **Katalog erstellen** neu, um eine aktualisierte Liste zu erhalten.

(Für GCP) Schritt 3k: Ethernet-Verbindung auf RHEL 8.x/9.x und Rocky Linux 8.x/9.x konfigurieren

Nachdem Sie den Linux VDA auf RHEL 8.x/9.x und Rocky Linux 8.x/9.x, die auf GCP gehostet werden, installiert haben, kann die Ethernet-Verbindung verloren gehen und der Linux VDA nach einem VM-Neustart unerreichbar sein. Um dieses Problem zu umgehen, legen Sie beim ersten Anmelden an der VM ein Root-Passwort fest und stellen Sie sicher, dass Sie sich als Root an der VM anmelden können. Führen Sie dann nach dem Neustart der VM die folgenden Befehle in der Konsole aus:

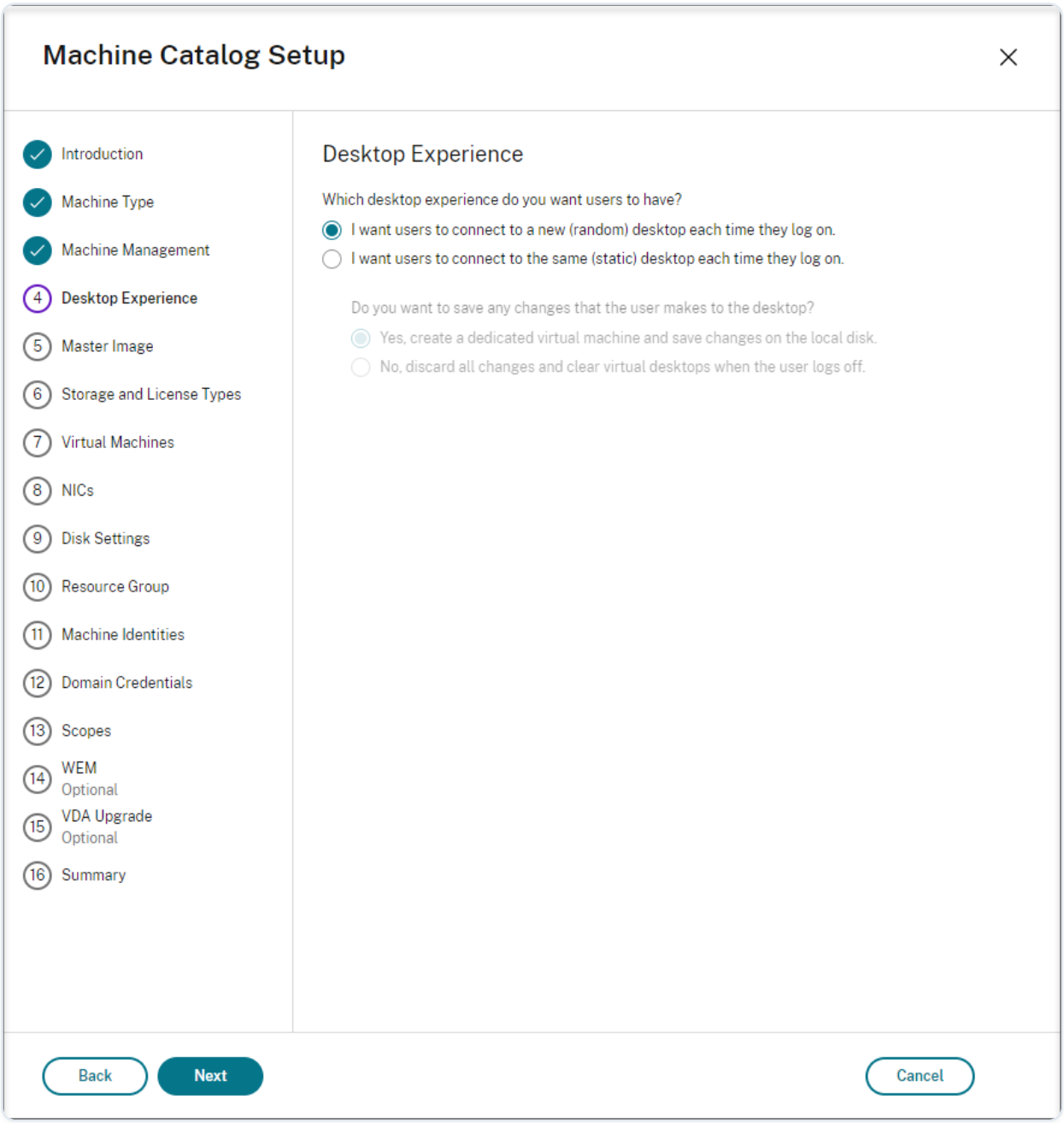
```
nmcli dev connect eth0

service NetworkManager restart
```

Schritt 4: Maschinenkatalog erstellen

Erstellen Sie in Citrix Studio oder Web Studio einen Maschinenkatalog und geben Sie die Anzahl der VMs an, die im Katalog erstellt werden sollen. Wählen Sie beim Erstellen des Maschinenkatalogs Ihr Masterimage aus und beachten Sie Folgendes:

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



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

- Benutzer stellen bei jeder Anmeldung eine Verbindung zu einem neuen (zufälligen) Desktop her.
- Benutzer stellen bei jeder Anmeldung eine Verbindung zu demselben (statischen) Desktop her.

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

Wenn Sie die zweite Option wählen und MCS zum Bereitstellen der Maschinen verwenden, können Sie konfigurieren, wie Benutzeränderungen am Desktop behandelt werden:

    - Benutzeränderungen am Desktop auf der lokalen Festplatte speichern (persistent).
    - Benutzeränderungen verwerfen und den virtuellen Desktop beim Abmelden des Benutzers löschen (nicht persistent). Wählen Sie diese Option, wenn Sie die Benutzerpersonalisierungsebene verwenden.

- Beim Aktualisieren des Masterimages für einen MCS-Katalog, der persistente Maschinen enthält, verwenden alle neuen Maschinen, die dem Katalog hinzugefügt werden, das aktualisierte Image. Vorhandene Maschinen verwenden weiterhin das ursprüngliche Masterimage.

Weitere Informationen finden Sie unter Maschinenkatalogerstellung in der Dokumentation zu Citrix Virtual Apps and Desktops und in der Dokumentation zu Citrix DaaS.

> **Hinweis:**

> Wenn in Nutanix-Umgebungen der Erstellungsprozess Ihres Maschinenkatalogs auf dem Delivery Controller™ viel Zeit in Anspruch nimmt, gehen Sie zu Nutanix Prism und schalten Sie die Maschine, die mit **Preparation** beginnt, manuell ein. Dieser Ansatz hilft, den Erstellungsprozess fortzusetzen.

Schritt 5: Bereitstellungsgruppe erstellen

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Sie legt fest, welche Benutzer diese Maschinen verwenden können und welche Anwendungen und Desktops diesen Benutzern zur Verfügung stehen.

Weitere Informationen finden Sie unter Erstellung von Bereitstellungsgruppen in der Citrix Virtual Apps and Desktops-Dokumentation und der Citrix DaaS-Dokumentation.

> **Hinweis:**

> Die VMs, die Sie mit MCS erstellen, können sich möglicherweise nicht bei Citrix Cloud Connectors registrieren und werden als **Nicht registriert** angezeigt. Das Problem tritt auf, wenn Sie die VMs in Azure hosten und sie mit Samba Winbind in die AD-Domäne aufnehmen. Um das Problem zu umgehen, führen Sie die folgenden Schritte aus:

1. Gehen Sie zur ADSI-Bearbeitungskonsole, wählen Sie eine nicht registrierte VM aus und bearbeiten Sie das Attribut **msDS-SupportedEncryptionTypes** ihres Maschinenkontos.
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 nach den folgenden Zeilen in der Datei **/var/xdl/mcs/ad_join.sh** eine Zeile hinzu: **net ads enctypes set $NEW_HOSTNAME\$ <Dezimalwert des Verschlüsselungstypattributs, z. B. 28\> -U $NEW_HOSTNAME\$ -P password:**

   ```
   if [ "$AD_INTEGRATION" == "winbind" ]; then

                   join_domain_samba

                   restart_service winbind /usr/bin/systemctl
   ```

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

Verwenden Sie MCS, um Ihr Linux VDA zu aktualisieren

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

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

Hinweis:

Sie können auch die Linux VDA-Selbstaktualisierungsfunktion verwenden, um automatische Software-Updates zu planen. Um dies zu erreichen, fügen Sie Befehlszeilen zur Datei etc/xdl/mcs/mcs_local_setting.reg auf der Vorlagenmaschine hinzu. Sie können beispielsweise die folgenden Befehlszeilen hinzufügen:

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

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



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



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

Für RHEL 7 und CentOS 7:

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

Für RHEL 8.x und Rocky Linux 8.x:

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

Für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

Hinweis:

Bevor Sie den Linux VDA auf RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 aktualisieren, aktualisieren Sie das Paket **libsepol** auf Version 3.4 oder höher.

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

Für SUSE:

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

Für Ubuntu 20.04:

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

Für Ubuntu 22.04:

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

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

Automatisierung von Maschinenkontokennwortaktualisierungen

Maschinenkontokennwörter laufen standardmäßig 30 Tage nach der Erstellung des Maschinenkatalogs ab. Um den Ablauf von Kennwörtern zu verhindern und die Aktualisierung von Maschinenkontokennwörtern zu automatisieren, gehen Sie wie folgt vor:

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

   `UPDATE_MACHINE_PW="Y"`

2. Nach dem Ausführen von /opt/Citrix/VDA/sbin/deploymcs.sh öffnen Sie /etc/cron.d/mcs_update_password_cronjob, um die Aktualisierungszeit und -häufigkeit festzulegen. Die Standardeinstellung aktualisiert die Maschinenkontokennwörter wöchentlich sonntags um 2:30 Uhr.

Nach jeder Aktualisierung des Maschinenkontokennworts wird der Ticket-Cache auf dem Delivery Controller ungültig, und der folgende Fehler kann in /var/log/xdl/jproxy.log angezeigt werden:

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

Um den Fehler zu beheben, löschen Sie den Ticket-Cache regelmäßig. Sie können eine Cache-Bereinigungsaufgabe auf allen Delivery Controllern oder auf dem Domänencontroller planen.

FAS auf MCS-erstellten VMs aktivieren

Sie können FAS auf von 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

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

1. Importieren Sie das Stamm-CA-Zertifikat.

   ```
   sudo cp root.pem /etc/pki/CA/certs/
   ```

2. Führen Sie ctxfascfg.sh aus.
3. Legen Sie Variablen in `/etc/xdl/mcs/mcs.conf` fest.

   Hinweis:

   Legen Sie alle erforderlichen Variablen in `/etc/xdl/mcs/mcs.conf` fest, da diese Variablen beim Start der VM aufgerufen werden.

   a. Setzen Sie den Wert von `Use_AD_Configuration_Files_Of_Current_VDA` auf Y.

b. Setzen Sie die Variable `FAS_LIST` auf die Adresse Ihres FAS-Servers oder auf mehrere FAS-Serveradressen. Trennen Sie mehrere Adressen durch Semikolons und setzen Sie die Adresse(n) in einfache Anführungszeichen, zum Beispiel `FAS_LIST='<FAS_SERVER_FQDN>;<FAS_SERVER_FQDN>'`.

c. Legen Sie die anderen Variablen nach Bedarf fest, z. B. `VDI_MODE`.

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

FAS auf einer mit MCS erstellten VM aktivieren

Wenn FAS auf der Vorlagenmaschine nicht wie zuvor beschrieben aktiviert ist, können Sie FAS auf jeder mit MCS erstellten VM aktivieren.

Gehen Sie wie folgt vor, um FAS auf einer mit MCS erstellten VM zu aktivieren:

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 Start der VM aufgerufen werden.

a. Setzen Sie den Wert von `Use_AD_Configuration_Files_Of_Current_VDA` auf Y.

b. Setzen Sie die Variable `FAS_LIST` auf die Adresse Ihres FAS-Servers.

c. Legen Sie die anderen Variablen nach Bedarf fest, z. B. `VDI_MODE`.

2. Importieren Sie das Stamm-CA-Zertifikat.

```
sudo cp root.pem /etc/pki/CA/certs/
```

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

Linux-VDAs mit Citrix Provisioning™ erstellen

Sie können domänengebundene VDAs mit Citrix Provisioning erstellen.

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

Die folgenden Linux-Distributionen werden unterstützt:

- Ubuntu 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 Paket, das auf Ihrer Linux-Distribution basiert. Citrix Provisioning Server 2109 oder höher ist erforderlich, um den Linux-Streaming-Agent 2109 und höher zu verwenden.
- Wenn Sie Citrix Provisioning zum Streamen von Linux-Zielgeräten verwenden, erstellen Sie eine separate Boot-Partition auf dem einzelnen gemeinsam genutzten Datenträger-Image, damit die bereitgestellten Geräte wie erwartet starten können.
- Vermeiden Sie die Formatierung von Partitionen mit **btrfs**. GRUB2 hat ein intrinsisches Problem beim Auffinden von **btrfs**-Partitionen. **GRUB** steht für **GRand Unified Bootloader**.

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

Linux VDAs in Citrix DaaS Standard für Azure erstellen

Sie können sowohl domänengebundene als auch nicht-domänengebundene Linux-VDAs in Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard für Azure) erstellen, um virtuelle Apps und Desktops auf jedem Gerät von Microsoft Azure bereitzustellen. Weitere Informationen finden Sie unter Citrix DaaS Standard für Azure.

Unterstützte Linux-Distributionen

Die folgenden Linux-Distributionen unterstützen diese Funktion:

- 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:**
>
> Sie können auch die Funktion Linux VDA-Selbstaktualisierung verwenden, um automatische Softwareupdates zu planen. Fügen Sie dazu Befehlszeilen zur Datei etc/xdl/mcs/mcs_local_setting.reg auf dem Masterimage hinzu. Sie können beispielsweise die folgenden Befehlszeilen hinzufügen:
>
> ```
> create -k "HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_DWORD" -v "fEnabled" -d "0x00000001" –force
> ```

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



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



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

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 auf der VM .NET Runtime 6.0 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.
4. (Nur für Ubuntu) Fügen Sie die Zeile `source /etc/network/interfaces.d/*` zur Datei `/etc/network/interfaces` hinzu.
5. (Nur für Ubuntu) Verweisen Sie `/etc/resolv.conf` auf `/run/systemd/resolve/resolv.conf` anstatt auf `/run/systemd/resolve/stub-resolv.conf`:

   ```
   unlink /etc/resolv.conf



   ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
   ```

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

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

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

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

> **Hinweis:**
>
> - Wir empfehlen die Verwendung von SQLite nur für den VDI-Modus.
> - Für eine einfache Installation und MCS können Sie zwischen SQLite und PostgreSQL wechseln, ohne sie manuell installieren zu müssen. Sofern nicht anders über `/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.

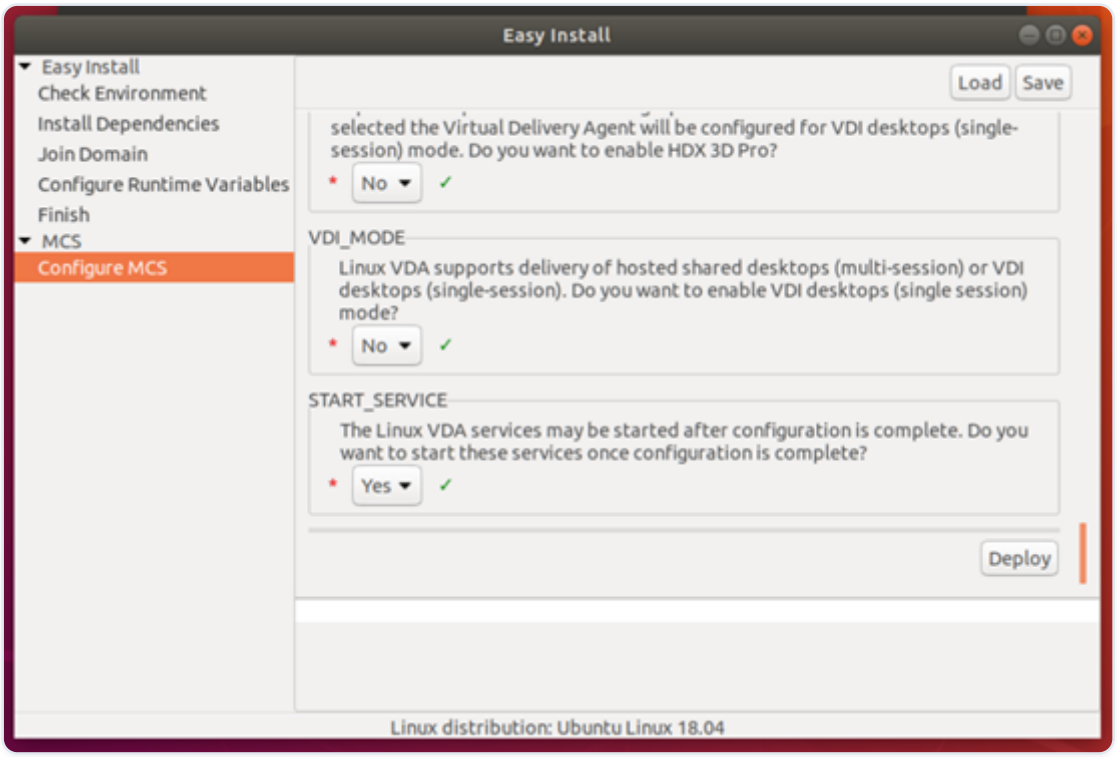
8. MCS-Variablen ändern.

Es gibt zwei Möglichkeiten, MCS-Variablen zu konfigurieren:

- Bearbeiten Sie die Datei `/etc/xdl/mcs/mcs.conf`.
- Verwenden Sie die Easy Install-GUI. Um die Easy Install-GUI zu öffnen, führen Sie den Befehl `/opt/Citrix/VDA/bin/easyinstall` in der Desktop-Umgebung Ihres Linux VDA aus.

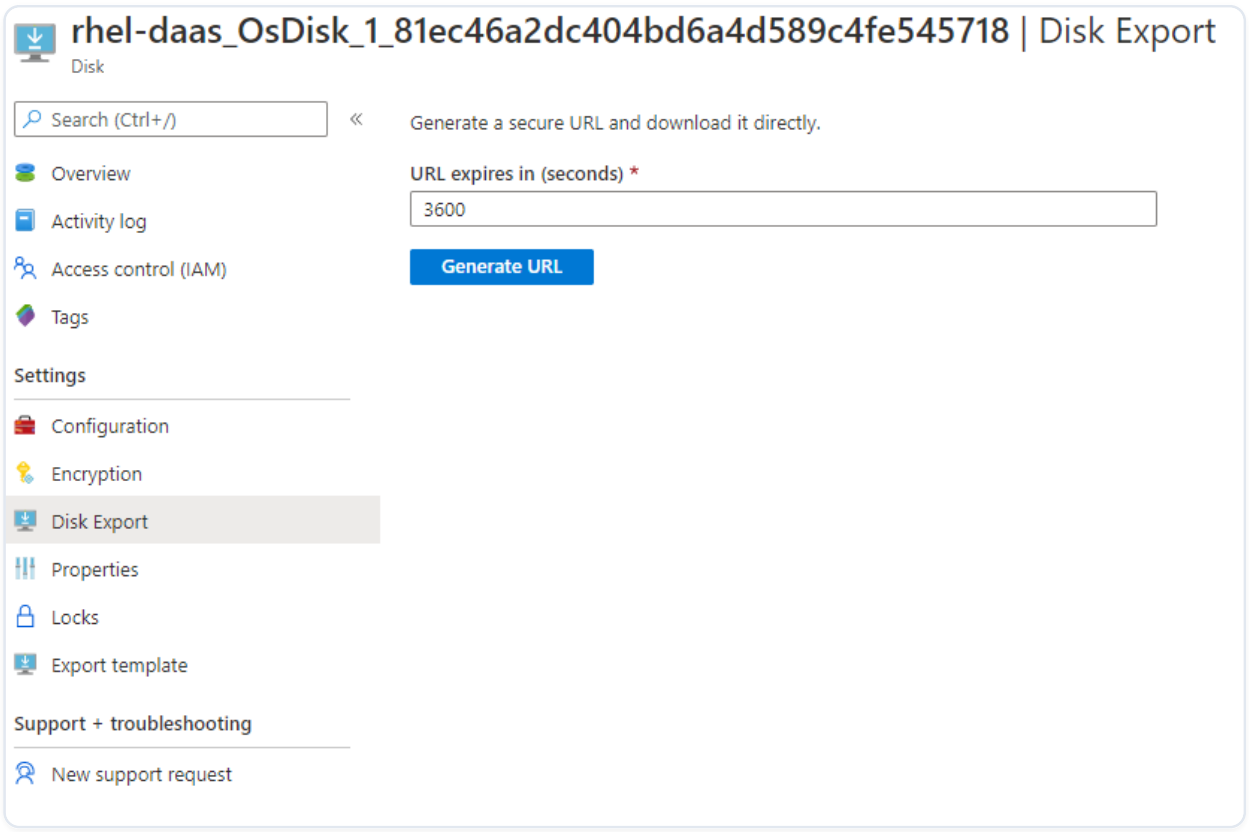
> **Hinweis:**
>
> Lassen Sie die Variable `dns` unspezifiziert. Wenn Sie beim Erstellen eines Maschinenkatalogs den Typ **Static** oder **Random** auswählen, legen Sie `VDI_MODE=Y` fest.

> 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 **Deploy**.



Nachdem Sie in der GUI auf **Deploy** geklickt haben, überschreiben die in der GUI festgelegten Variablen die in der Datei `/etc/xdl/mcs/mcs.conf` festgelegten Variablen.

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



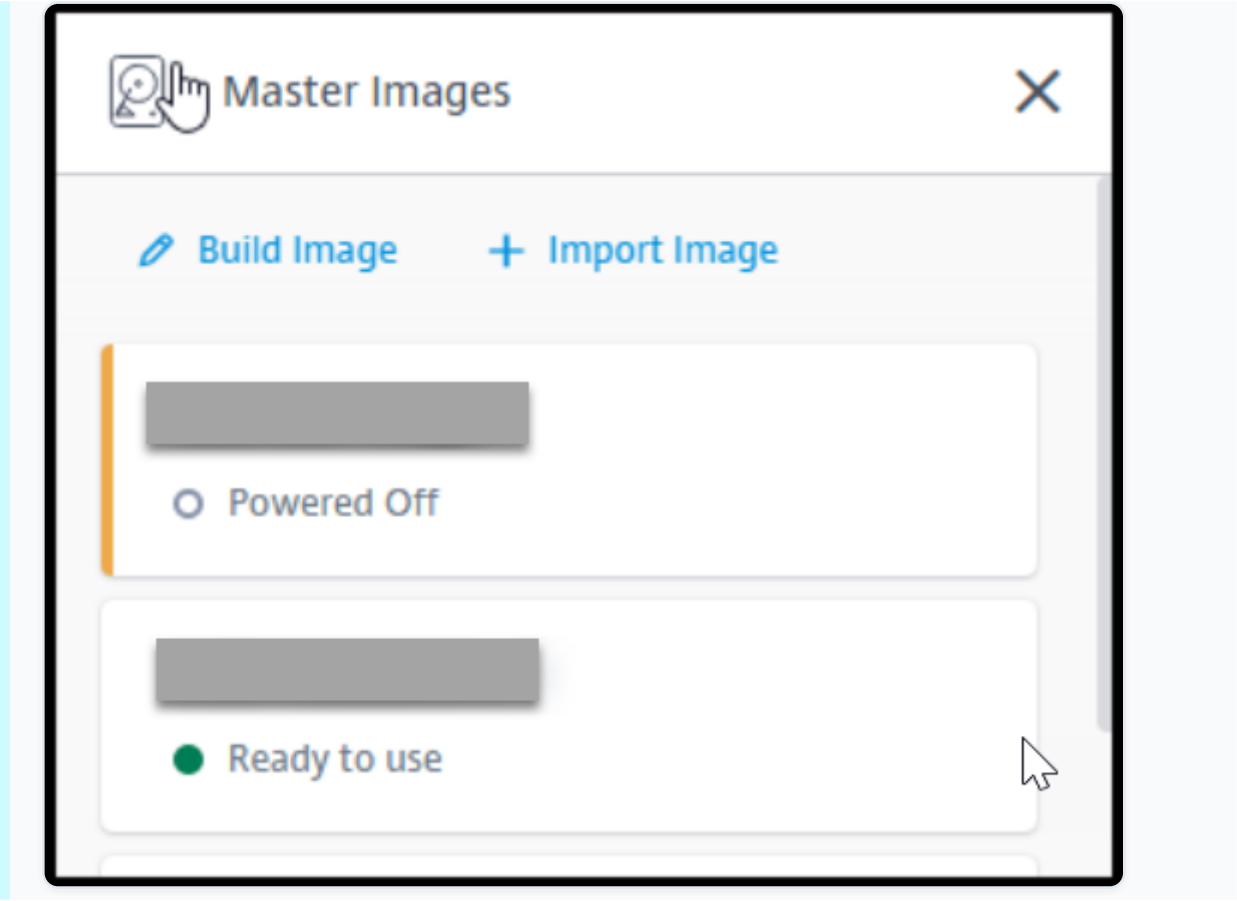
10. (Optional) Nehmen Sie Gruppenrichtlinieneinstellungen am Masterimage vor. Sie können das Tool `ctxreg` verwenden, um Gruppenrichtlinieneinstellungen vorzunehmen. Der folgende Befehl aktiviert beispielsweise die Richtlinie **Auto-create PDF Universal Printer** für den PDF-Druck.

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

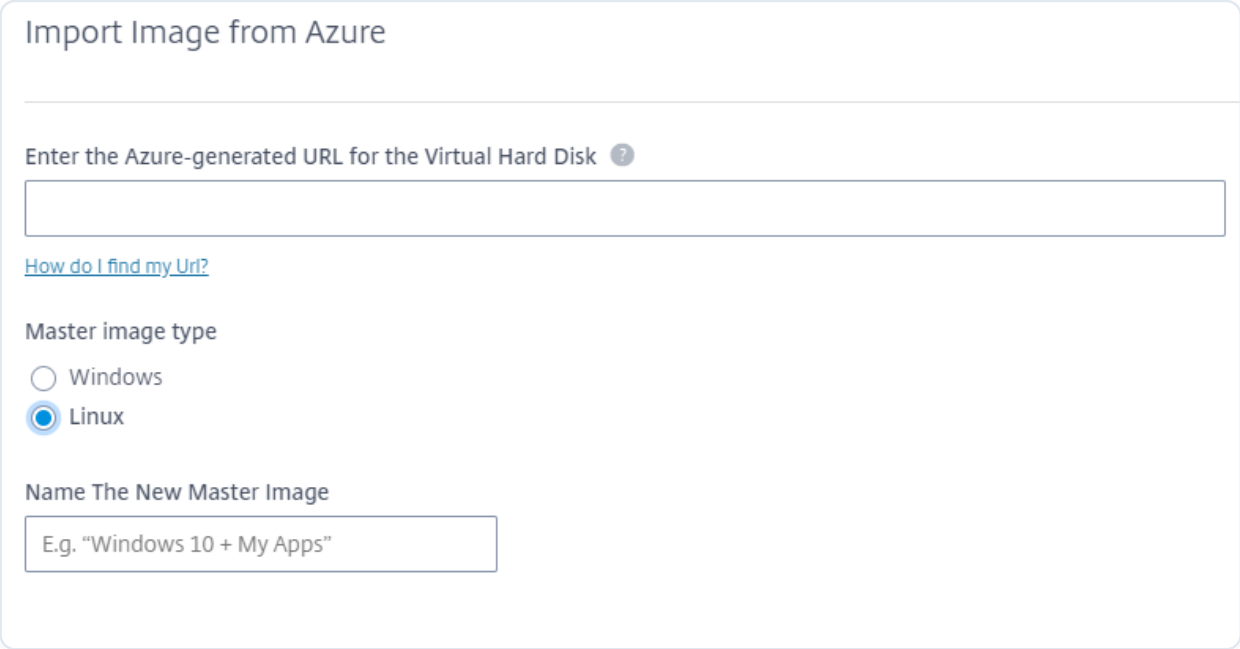
Schritt 2: Masterimage aus Azure importieren

1. Im Manage-Dashboard, erweitern Sie rechts **Master Images**. Die Anzeige listet die von Citrix bereitgestellten Master-Images sowie die von Ihnen erstellten und importierten Images auf.

> **Tipp:**
>
> Die meisten Administratoraktivitäten für diesen Dienst werden über die Dashboards **Manage** und **Monitor** verwaltet. Nachdem Sie Ihren ersten Katalog erstellt haben, wird das Dashboard **Manage** automatisch gestartet, nachdem 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 VHD-Datei ein, die Sie in Azure generiert haben. Wählen Sie **Linux** als Master-Image-Typ aus.



4. Befolgen Sie die Anweisungen im Assistenten, um den Import des Master-Images abzuschließen.

Schritt 3: Maschinenkatalog erstellen

Greifen Sie auf das Verwalten-Dashboard zu und klicken Sie auf **Katalog erstellen**. Wählen Sie beim Erstellen des Maschinenkatalogs das zuvor erstellte Master-Image aus.

> **Hinweis:**
>
> Die als Master-Image verwendete VM ist nicht über SSH oder RDP zugänglich. Um auf die VM zuzugreifen, verwenden Sie die serielle Konsole im Azure-Portal.

Installieren Sie den Linux VDA manuell

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

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

Installieren Sie den Linux VDA manuell auf Amazon Linux 2, CentOS, RHEL und Rocky Linux

> **Wichtig:**
>
> Für Neuinstallationen empfehlen wir Ihnen, easy install für eine schnelle Installation zu verwenden. Easy install spart Zeit und Arbeit und ist weniger fehleranfällig als die in diesem Artikel beschriebene manuelle Installation.

Schritt 1: Konfigurationsinformationen und die Linux-Maschine vorbereiten

Schritt 1a: Netzwerkkonfiguration überprüfen

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

Schritt 1b: Hostnamen festlegen

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

```
hostname
```

Schritt 1c: Eine Loopback-Adresse dem Hostnamen zuweisen

Um sicherzustellen, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine korrekt zurückgemeldet werden, ändern Sie die folgende Zeile der Datei `/etc/hosts`, um den FQDN und den Hostnamen als die ersten beiden Einträge aufzunehmen:

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

Zum Beispiel:

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

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

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

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

Schritt 1d: Hostnamen überprüfen

Überprüfen Sie, ob der Hostname korrekt festgelegt ist:

```
hostname
```

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

Überprüfen Sie, ob der FQDN korrekt eingestellt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN des Computers zurück.

Schritt 1e: Namensauflösung und Dienstverfügbarkeit prüfen

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

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

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

Schritt 1f: Taktsynchronisierung konfigurieren

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

Eine RHEL-Standardumgebung verwendet den Chrony-Daemon (`chronyd`) zur Taktsynchronisierung.

CHRONY-DIENST KONFIGURIEREN

Bearbeiten Sie als Root-Benutzer **/etc/chrony.conf** und fügen Sie einen Servereintrag für jeden externen Zeitserver hinzu:

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



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

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

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

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

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

Schritt 1g: PulseAudio installieren (Nur für 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
```

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

```
autospawn = yes
```

Schritt 1h: OpenJDK 11 installieren

Der Linux VDA erfordert die Anwesenheit von OpenJDK 11.

- Wenn Sie CentOS oder RHEL verwenden, wird OpenJDK 11 automatisch als Abhängigkeit installiert, wenn Sie den Linux VDA installieren.
- 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
```

Bestätigen Sie die korrekte Version:

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

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

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

Schritt 1i: Eine zu verwendende Datenbank installieren und angeben

Sie können SQLite oder PostgreSQL zur Verwendung angeben, indem Sie **/etc/xdl/db.conf** nach der Installation des Linux VDA-Pakets bearbeiten. Für manuelle Installationen müssen Sie SQLite und PostgreSQL manuell installieren, bevor Sie sie angeben können.

Dieser Abschnitt beschreibt, wie die PostgreSQL- und SQLite-Datenbanken installiert werden und wie eine zu verwendende Datenbank angegeben wird.

> **Hinweis:**
>
> Wir empfehlen die Verwendung von SQLite nur für den VDI-Modus.

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 die folgenden Befehle aus, um PostgreSQL zu installieren:

```
sudo yum -y install postgresql-server
```

```
sudo yum -y install postgresql-jdbc
```

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

```
sudo yum -y install libpq
```

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

```
sudo postgresql-setup initdb
```

Führen Sie die folgenden Befehle aus, um PostgreSQL jeweils beim Maschinenstart oder sofort zu starten:

```
sudo systemctl enable postgresql



sudo systemctl start postgresql
```

Überprüfen Sie die Version von PostgreSQL mit:

```
psql --version
```

(Nur für RHEL 7 und Amazon Linux 2) Vergewissern Sie sich, dass das Datenverzeichnis mithilfe des Befehlszeilendienstprogramms **psql** festgelegt ist:

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

SQLITE INSTALLIEREN

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

```
sudo yum -y install sqlite
```

DATENBANK ANGEBEN

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

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Überspringen Sie diesen Schritt, 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: Hypervisor vorbereiten

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

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

Wenn die Zeitsynchronisierungsfunktion von Citrix Hypervisor aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und Citrix Hypervisor auf. Beide versuchen, die Systemuhr zu verwalten. Um zu vermeiden, dass die Uhr mit anderen Servern asynchron wird, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit dem NTP synchronisiert ist. Dieser Fall erfordert die Deaktivierung der Host-Zeitsynchronisierung. Im HVM-Modus sind keine Änderungen erforderlich.

Wenn Sie einen paravirtualisierten Linux-Kernel mit installierten Citrix VM Tools ausführen, können Sie überprüfen, ob die Zeitsynchronisierungsfunktion von Citrix Hypervisor in der Linux-VM vorhanden und aktiviert ist:

```
su -
```

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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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

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

`xen.independent_wallclock = 1`

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

```
su -



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

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

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

Vom Verwaltungsbetriebssystem aus:

1. Öffnen Sie die Hyper-V-Manager-Konsole.

2. Wählen Sie für die Einstellungen einer Linux-VM **Integrationsdienste** aus.
3. Stellen Sie sicher, dass **Zeitsynchronisierung** ausgewählt ist.

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

Zeitsynchronisierung auf ESX und ESXi beheben

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

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

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

Schritt 3: Hinzufügen der Linux-VM zur Windows-Domäne

Die folgenden Methoden stehen zum Hinzufügen von Linux-Maschinen zur Active Directory (AD)-Domäne zur Verfügung:

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

Befolgen Sie die Anweisungen entsprechend der von Ihnen gewählten Methode.

Hinweis:

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

Samba Winbind

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 Besitz des Stammverzeichnisses ändert:

```
usermod -d /nonexistent nobody
```

Installieren oder aktualisieren Sie die erforderlichen Pakete:

Für 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
```

Für Amazon Linux 2, CentOS 7 und RHEL 7:

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

WINBIND-DAEMON BEIM MASCHINENSTART AKTIVIEREN

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

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

WINBIND-AUTHENTIFIZIERUNG KONFIGURIEREN

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

1. Führen Sie den folgenden Befehl aus.

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

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

Für 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
```

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

Wenn eine DNS-basierte Suche des KDC-Servers und des Realm-Namens erforderlich ist, fügen Sie die folgenden beiden Optionen zum vorherigen Befehl hinzu:

`--enablekrb5kdcdns --enablekrb5realmdns`

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

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

   `kerberos method = secrets and keytab`

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

3. (Nur für 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 System-Keytab-Datei /etc/krb5.keytab, um sich beim Delivery Controller zu authentifizieren und zu registrieren. Die vorherige Kerberos-Methodeneinstellung zwingt Winbind dazu, die System-Keytab-Datei zu erstellen, wenn die Maschine zum ersten Mal der Domäne beigetreten wird.

WINDOWS-DOMÄNE BEITRETEN

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

Um eine Linux-VM zur Windows-Domäne hinzuzufügen, führen Sie den folgenden Befehl aus:

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

Tipp:

Für die Linux-VMs, die auf Amazon Linux 2, RHEL 7.9 und CentOS 7.9 ausgeführt werden, können Sie auch den folgenden Befehl verwenden, um sie zur Windows-Domäne hinzuzufügen:

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

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

PAM FÜR WINBIND KONFIGURIEREN

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

`krb5_auth = yes`

`krb5_ccache_type = FILE` `mkhomedir = yes`

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

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

Tipp:

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

Öffnen Sie **/etc/krb5.conf** und ändern Sie die folgende Einstellung unter dem Abschnitt „\[libdefaults\]“ von KEYRING in den FILE-Typ:

`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 beheben:

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



semodule -X 300 -i my-winbindd.pp
```

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

KERBEROS-KONFIGURATION ÜBERPRÜFEN

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

```
sudo klist -ke
```

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

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

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

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

```
sudo klist
```

Überprüfen Sie die Kontodetails des Computers mit:

```
sudo net ads status
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

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

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

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

```
ssh localhost -l domain\\username

id -u
```

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

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

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

Quest Authentication Services

QUEST AUF DEM DOMÄNENCONTROLLER KONFIGURIEREN

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

DOMÄNENBENUTZERN DIE ANMELDUNG AN LINUX-VDA-MASCHINEN ERMÖGLICHEN

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

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

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

QUEST AUF LINUX-VDA KONFIGURIEREN

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

Die bequemste Methode, dieses Problem zu umgehen, ist das Deaktivieren von SELinux. Bearbeiten Sie als Root-Benutzer die Datei **/etc/selinux/config** und ändern Sie die Einstellung für **SELinux**:

`SELINUX=permissive`

Diese Änderung erfordert einen Neustart des Computers:

```
reboot
```

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

VAS-DAEMON KONFIGURIEREN

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

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

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

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

PAM UND NSS KONFIGURIEREN

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

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



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

WINDOWS-DOMÄNE BEITRETEN

Fügen Sie die Linux-Maschine der Active Directory-Domäne mithilfe des Quest **vastool**-Befehls hinzu:

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

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

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl den Domänennamen zurück. Wenn die Maschine keiner Domäne beigetreten ist, wird der folgende Fehler angezeigt:

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

```
ssh localhost -l domain\\username

id -u
```

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

```
ls /tmp/krb5cc_uid
```

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

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

Beenden Sie die Sitzung.

```
exit
```

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

Centrify DirectControl

EINER WINDOWS-DOMÄNE BEITRETEN

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

```
su –

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

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

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

```
su –

adinfo
```

Vergewissern Sie sich, dass der Wert „Joined to domain“ gültig ist und der CentrifyDC-Modus „connected“ zurückgibt. Bleibt der Modus im Startzustand hängen, hat der Centrify-Client Probleme mit der Serververbindung oder Authentifizierung.

Umfassendere System- und Diagnoseinformationen sind verfügbar über:

```
adinfo --sysinfo all

adinfo –diag
```

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

```
adinfo --test
```

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

SSSD

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

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

1. Der Domäne beitreten und Host-Keytab erstellen
2. SSSD einrichten

3. SSSD aktivieren
4. Kerberos-Konfiguration überprüfen
5. Benutzerauthentifizierung überprüfen

DER DOMÄNE BEITRETEN UND HOST-KEYTAB ERSTELLEN

SSSD bietet keine Active Directory-Clientfunktionen zum Beitreten zur Domäne und zur Verwaltung der System-Keytab-Datei. Stattdessen können Sie **adcli**, **realmd** oder **Samba** verwenden.

Dieser Abschnitt beschreibt den **Samba**-Ansatz für Amazon Linux 2 und RHEL 7 sowie den `adcli`-Ansatz für RHEL 8.x/9.x und Rocky Linux 8.x/9.x. Informationen zu **realmd** finden Sie in der RHEL- oder CentOS-Dokumentation. Diese Schritte müssen vor der Konfiguration von SSSD ausgeführt werden.

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

  Erforderliche Pakete installieren oder aktualisieren:

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

  Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

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

  Konfigurieren Sie den Computer für die **Samba**- und Kerberos-Authentifizierung:

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

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

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

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

`--enablekrb5kdcdns --enablekrb5realmdns`

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

`kerberos method = secrets and keytab`

`winbind offline logon = no`

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

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

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

- **Adcli (RHEL 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
  ```

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

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

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

  Unter dem Abschnitt :

  `REALM = {`

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

Unter dem Abschnitt :

`realm = REALM` `.realm = REALM`

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

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

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

SSSD EINRICHTEN

Die Einrichtung von SSSD umfasst die folgenden Schritte:

- Installieren Sie das Paket **sssd-ad** auf dem Linux VDA, indem Sie den Befehl `sudo yum -y install sssd` ausführen.
- Nehmen Sie Konfigurationsänderungen an verschiedenen Dateien vor (zum Beispiel sssd.conf).
- Starten Sie den Dienst **sssd**.

Eine Beispielkonfiguration für **sssd.conf** für RHEL 7 (zusätzliche Optionen können bei Bedarf hinzugefügt werden):

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

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

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

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

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

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

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

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

Ersetzen Sie **ad.example.com**, **server.ad.example.com** durch die entsprechenden Werte. Weitere Informationen finden Sie unter sssd-ad(5) - Linux 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 die folgenden Einträge unter dem Abschnitt hinzu:

`ad_gpo_access_control = permissive`

`full_name_format = %2$s\%1$s` `fallback_homedir = /home/%d/%u`

`# Kerberos settings` `krb5_ccachedir = /tmp`

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

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

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

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

SSSD AKTIVIEREN

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

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

```
sudo systemctl restart sssd

sudo systemctl enable sssd.service

sudo chkconfig sssd on
```

Für Amazon Linux 2, CentOS 7 und RHEL 7:

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

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



sudo service sssd start



sudo chkconfig sssd on
```

KERBEROS-KONFIGURATION ÜBERPRÜFEN

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

```
sudo klist -ke
```

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

```
sudo kinit –k MACHINE\$@REALM
```

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

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

Überprüfen Sie, ob das TGT-Ticket für das Maschinenkonto mit folgender Methode zwischengespeichert wurde:

```
sudo klist
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

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

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

Die unterstützten Anmeldeformate sind:

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

Um zu überprüfen, ob das SSSD PAM-Modul korrekt konfiguriert ist, melden Sie sich mit einem bisher unbenutzten Domänenbenutzerkonto am Linux VDA an.

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



id -u
```

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

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

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

```
klist
```

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

PBIS

ERFORDERLICHES PBIS-PAKET HERUNTERLADEN

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

PBIS-INSTALLATIONSSKRIPT AUSFÜHRBAR MACHEN

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

PBIS-INSTALLATIONSSKRIPT AUSFÜHREN

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

WINDOWS-DOMÄNE BEITRETEN

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

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

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

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

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

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

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

Um zu überprüfen, ob PBIS Domänenbenutzer über PAM authentifizieren kann, melden Sie sich mit einem bisher unbenutzten Domänenbenutzerkonto am Linux-VDA an.

```
ssh localhost -l domain\\user



id -u
```

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

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

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

Schritt 4: .NET Runtime 6.0 installieren

Bevor Sie den Linux VDA installieren, installieren Sie .NET Runtime 6.0 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

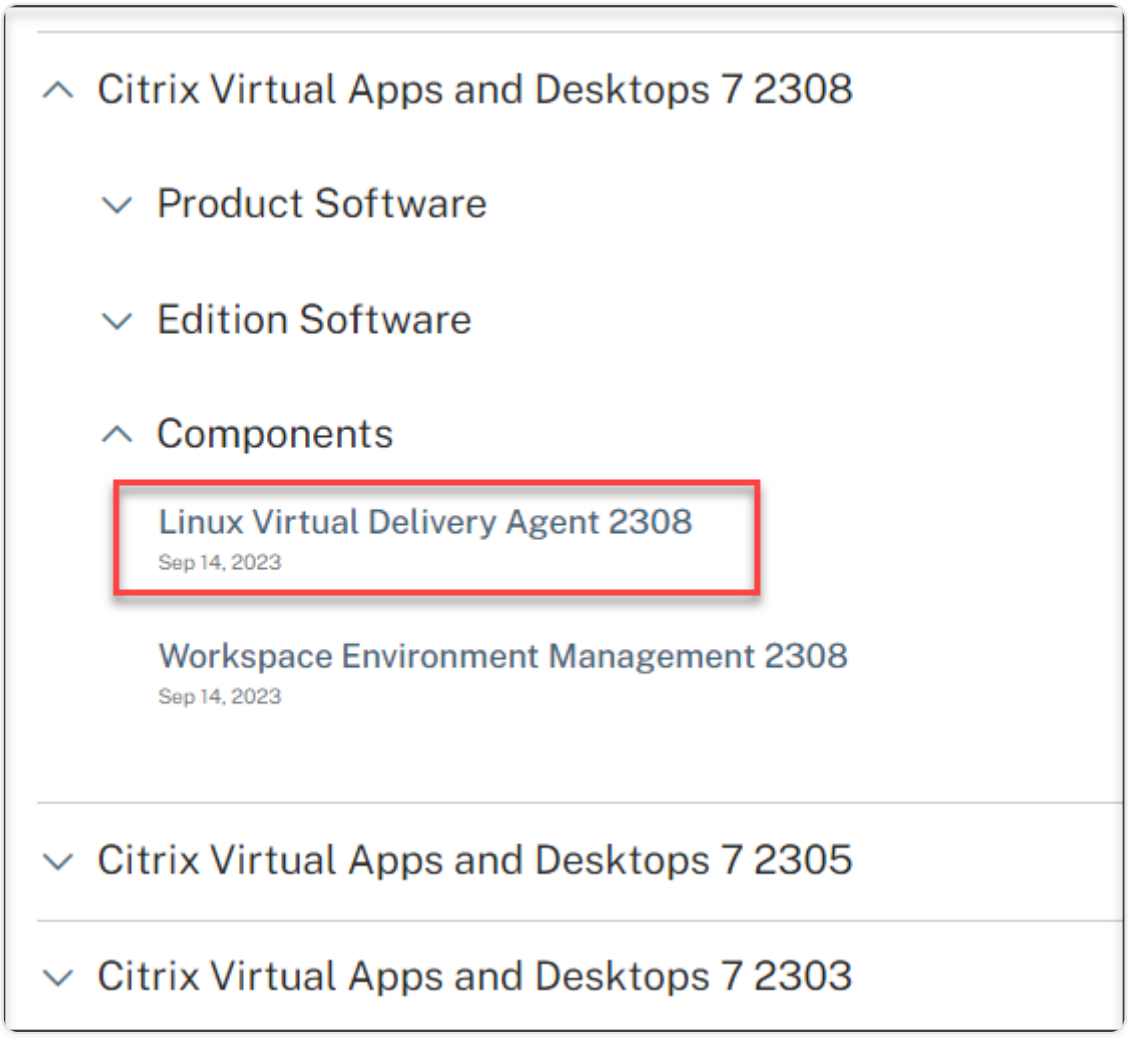
Nach der Installation von .NET Runtime 6.0 führen Sie den Befehl **which dotnet** aus, um Ihren Runtime-Pfad zu finden.

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

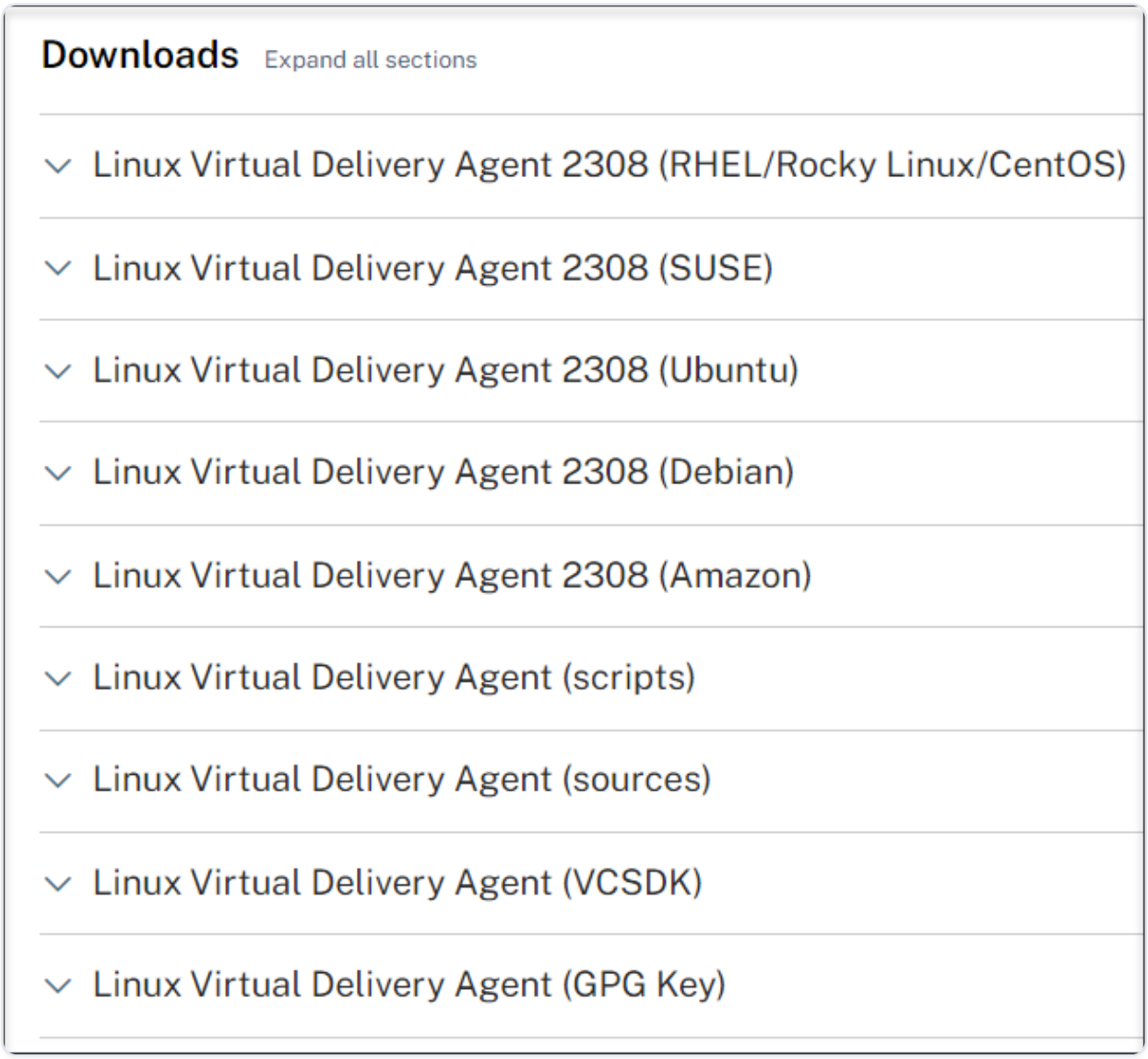
Schritt 5: Linux VDA-Paket herunterladen

1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.

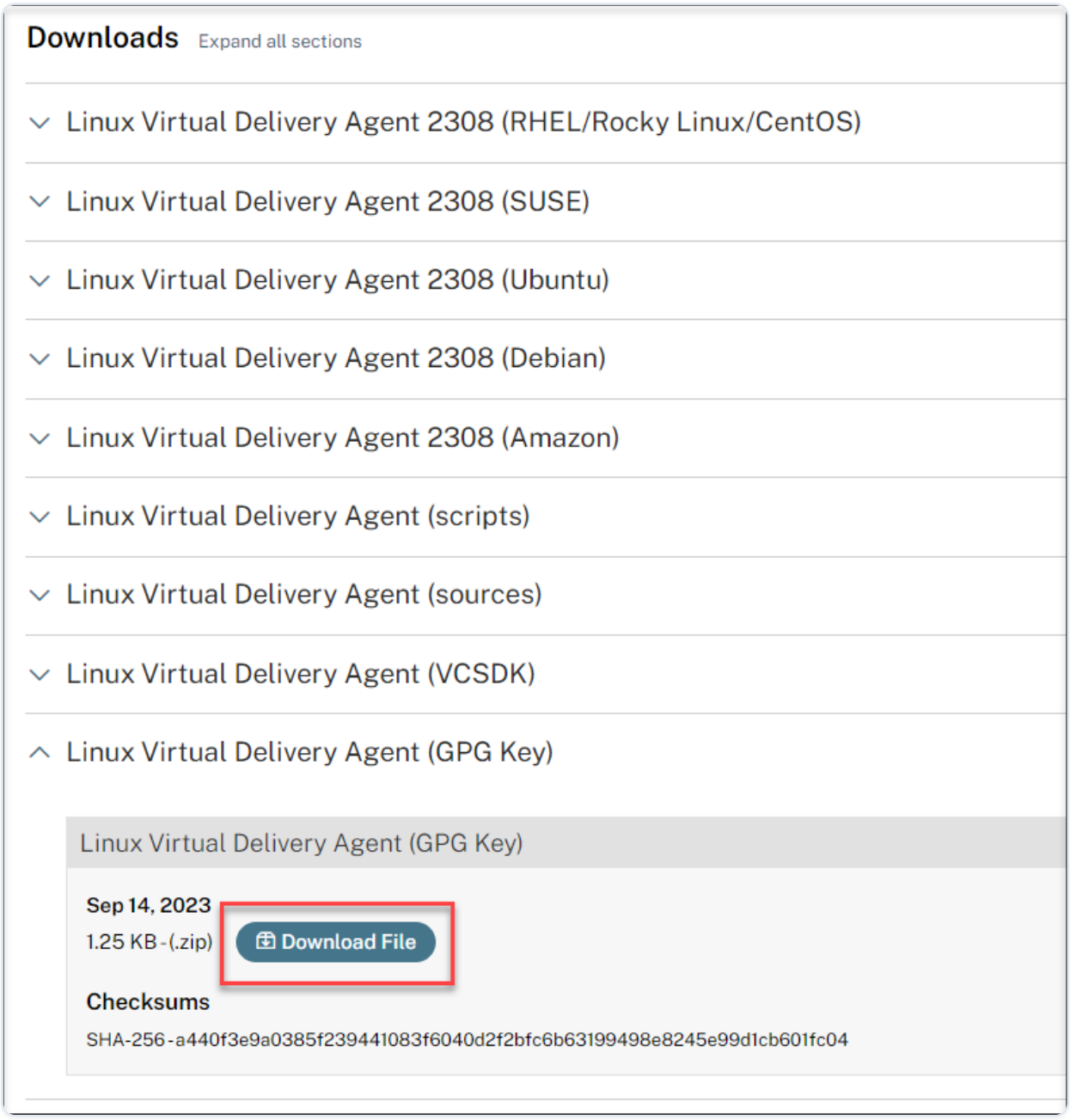
2. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. erweitern Sie **Components**, um den Linux VDA zu finden. Zum Beispiel:



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. Zum 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 Paketintegrität zu überprüfen:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

Schritt 6: Linux VDA installieren

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

Schritt 6a: Neuinstallation durchführen

1. (Optional) Alte Version deinstallieren

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

   a. Beenden Sie die Linux VDA-Dienste:

   ```
   sudo /sbin/service ctxvda stop



   sudo /sbin/service ctxhdx stop
   ```

   Hinweis:

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

   b. Deinstallieren Sie das Paket:

   ```
   sudo rpm -e XenDesktopVDA
   ```

Hinweis:

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

2. Linux VDA-Paket herunterladen

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

3. Linux VDA installieren

Hinweis:

- Für CentOS, RHEL und Rocky Linux müssen Sie das EPEL-Repository installieren, bevor Sie den Linux VDA erfolgreich installieren können. Informationen zur Installation von EPEL finden Sie in den Anweisungen unter `<https://docs.fedoraproject.org/de-de/epel/>`.
- Bevor Sie den Linux VDA unter RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 installieren, aktualisieren Sie das Paket **libsepol** auf Version 3.4 oder höher.

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

  Für Amazon Linux 2:

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

  Für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

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

  Für RHEL 8.x und Rocky Linux 8.x:

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

  Für CentOS 7 und RHEL 7:

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

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

  Für Amazon Linux 2:

  ```
  sudo rpm -i XenDesktopVDA-<version>.amzn2.x86_64.rpm
  ```

  RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

```
sudo rpm -i XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

Für RHEL 8.x und Rocky Linux 8.x:

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

Für CentOS 7 und RHEL 7:

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

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


 policycoreutils-python-utils >= 2.8


 python3-policycoreutils >= 2.8


 dbus >= 1.12.8
```

```
dbus-common >= 1.12.8

dbus-daemon >= 1.12.8

dbus-tools >= 1.12.8

dbus-x11 >= 1.12.8

xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.4

libXpm >= 3.5.12

libXrandr >= 1.5.1

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1
```

```
util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3

findutils >= 4.6

gawk >= 4.2

sed >= 4.5

cups >= 1.6.0

foomatic-filters >= 4.0.9

cups-filters >= 1.20.0

ghostscript >= 9.25

libxml2 >= 2.9
```

```
libmspack >= 0.7

krb5-workstation >= 1.13

ibus >= 1.5

nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9
```

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

libXtst >= 1.2.3

pam >= 1.3.1

util-linux >= 2.32.1

util-linux-user >= 2.32.1

xorg-x11-utils >= 7.5

bash >= 4.3
```

```
findutils >= 4.6


gawk >= 4.2


sed >= 4.5


cups >= 1.6.0


foomatic-filters >= 4.0.9


cups-filters >= 1.20.0


ghostscript >= 9.25


libxml2 >= 2.9


libmspack >= 0.7


krb5-workstation >= 1.13


ibus >= 1.5
```

```
nss-tools >= 3.44.0

gperftools-libs >= 2.4

cyrus-sasl-gssapi >= 2.1

python3 >= 3.6~

qt5-qtbase >= 5.5~

qt5-qtbase-gui >= 5.5~

qrencode-libs >= 3.4.4

imlib2 >= 1.4.9
```

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

qt5-qtbase >= 5.5~

qt5-qtbase >= 5.5~

imlib2 >= 1.4.5
```

RPM-Abhängigkeitsliste für Amazon Linux 2:

```
java-11-openjdk >= 11

ImageMagick >= 6.7.8.9

firewalld >= 0.3.9

policycoreutils-python >= 2.0.83

dbus >= 1.6.12

dbus-x11 >= 1.6.12
```

```
xorg-x11-server-utils >= 7.7

xorg-x11-xinit >= 1.3.2

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

gperftools-libs >= 2.4

nss-tools >= 3.44.0

qt5-qtbase >= 5.5~

qrencode-libs >= 3.4.1
```

```
imlib2 >= 1.4.5
```

Hinweis:

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

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

Schritt 6b: Vorhandene Installation aktualisieren (optional)

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

Hinweis:

- Beim Upgrade einer vorhandenen Installation werden die Konfigurationsdateien unter /etc/xdl überschrieben. Bevor Sie ein Upgrade durchführen, stellen Sie sicher, dass Sie die Dateien sichern.
- Bevor Sie den Linux VDA auf RHEL 9.2/9.0 und Rocky Linux 9.2/9.0 aktualisieren, aktualisieren Sie das **libsepol**-Paket auf Version 3.4 oder höher.

- So aktualisieren Sie Ihre Software mit `Yum`:

  Für Amazon Linux 2:

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

  Für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

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

Für RHEL 8.x und Rocky Linux 8.x:

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

Für CentOS 7 und RHEL 7:

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

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

Für Amazon Linux 2:

```
sudo rpm -U XenDesktopVDA-<version>.amzn2.x86_64.rpm
```

Für RHEL 9.2/9.0 und Rocky Linux 9.2/9.0:

```
sudo rpm -U XenDesktopVDA-<version>.el9_x.x86_64.rpm
```

Für RHEL 8.x und Rocky Linux 8.x:

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

Für CentOS 7 und RHEL 7:

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

Hinweis:

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

1. 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 `ctxvda`-Dienst neu.

Wichtig:

Starten Sie die Linux VDA-Maschine neu, nachdem Sie die Software aktualisiert haben.

Schritt 7: NVIDIA GRID-Treiber installieren

Um HDX 3D Pro zu aktivieren, 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 zur Installation und Konfiguration des NVIDIA GRID Virtual GPU Manager (Hosttreiber) auf den jeweiligen Hypervisoren finden Sie in den folgenden Anleitungen:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Führen Sie die folgenden Schritte aus, um die NVIDIA GRID-Gast-VM-Treiber zu installieren und zu konfigurieren:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie in XenCenter® der VM 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
```

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

Hinweis:

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

Wichtig:

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

```
nvidia-smi

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

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

Legen Sie die korrekte Konfiguration für die Karte fest:

`etc/X11/ctx-nvidia.sh`

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

Schritt 8: Konfigurieren des Linux VDA

> **Hinweis:**

> Bevor Sie die Laufzeitumgebung einrichten, stellen Sie sicher, dass das Gebietsschema **en_US.UTF-8** auf Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema auf Ihrem Betriebssystem nicht verfügbar ist, führen Sie den Befehl **sudo locale-gen en_US.UTF-8** aus. Bearbeiten Sie für Debian die Datei **/etc/locale.gen**, indem Sie die Zeile # **en_US.UTF-8 UTF-8** auskommentieren, und führen Sie dann den Befehl **sudo locale-gen** aus.

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

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

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

Geführte Konfiguration

Führen Sie eine manuelle Konfiguration mit geführten Fragen aus:

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

Automatisierte Konfiguration

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

Unterstützte Umgebungsvariablen sind:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags. Standardmäßig auf N festgelegt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste von Fully Qualified Domain Names (FQDNs) des Delivery Controllers, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** – Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** - Die Linux VDA-Dienste werden nach dem Maschinenstart gestartet. Der Wert ist standardmäßig auf Y festgelegt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux VDA-Dienste erfordern, dass eingehende Netzwerkverbindungen durch die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) automatisch in der System-Firewall für den Linux Virtual Desktop öffnen. Standardmäßig auf Y festgelegt.
- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd \| pbis** – Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird vom installierten und konfigurierten Active Directory-Integrationstool auf dem System bestimmt.
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung grafikintensiver Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für den VDI-Desktop-Modus (Einzelsitzung) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Legt fest, ob die Maschine als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie diese Variable auf Y. Diese Variable ist standardmäßig auf N gesetzt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf einen lokalen Standort zu beschränken, geben Sie einen DNS-Standortnamen an. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum 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. Um schnellere LDAP-Abfragen innerhalb einer Active Directory-Gesamtstruktur zu ermöglichen, aktivieren Sie den **Globalen Katalog** auf einem Domänencontroller und geben Sie die entsprechende LDAP-Portnummer als 3268 oder als 3269 an, wenn Sie LDAPS verwenden. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.

- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne gesetzt ist (z. B. DC=mycompany,DC=com). Um die Suchleistung zu verbessern, können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit 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 zur Installation der .NET Runtime 6.0 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – Gibt die GNOME-, GNOME Classic- oder MATE-Desktop-Umgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

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

  a. Erstellen Sie eine `.xsession`- oder `.Xclients`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA. Wenn Sie Amazon Linux 2 verwenden, erstellen Sie eine `.Xclients`-Datei. Wenn Sie andere Distributionen verwenden, erstellen Sie eine `.xsession`-Datei.

2\. Bearbeiten Sie die `.xsession`- oder `.Xclients`-Datei, um eine Desktop-Umgebung anzugeben.

- **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
```

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

Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebungen anpassen. Um diese Funktion zu aktivieren, müssen Sie im Voraus umschaltbare Desktopumgebungen auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen durch Sitzungsbenutzer.

- **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 Socket-Port zum Abhören von Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT** – Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=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
```

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

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \


CTX_XDL_REGISTER_SERVICE=Y|N \


CTX_XDL_ADD_FIREWALL_RULES=Y|N \


CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \


CTX_XDL_HDX_3D_PRO=Y|N \


CTX_XDL_VDI_MODE=Y|N \
```

```
CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \

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

Konfigurationsänderungen entfernen

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

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

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

So entfernen Sie Konfigurationsänderungen:

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

Wichtig:

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

Konfigurationsprotokolle

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

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

Schritt 9: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um nach häufigen Konfigurationsproblemen in einer Linux VDA-Umgebung zu suchen. Weitere Informationen finden Sie unter XDPing.

Schritt 10: Linux VDA ausführen

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

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start
```

```
sudo /sbin/service ctxvda start
```

Linux VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

Hinweis:

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

Linux VDA neu starten:

So starten Sie die Linux VDA-Dienste neu:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx restart



sudo /sbin/service ctxvda start
```

Status des Linux VDA überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status



sudo /sbin/service ctxhdx status
```

Schritt 11: Maschinenkataloge erstellen

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

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

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

Hinweis:

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

Tipp:

Wenn Sie eine entfernte Maschine wieder der Active Directory-Domäne hinzufügen, entfernen Sie die Maschine aus ihrem Maschinenkatalog und fügen Sie sie wieder hinzu.

Schritt 12: Bereitstellungsgruppen erstellen

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

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

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

> **Wichtig:**

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

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

Installation des Linux VDA auf SUSE manuell

> **Wichtig:**

> Für Neuinstallationen empfehlen wir die Verwendung der einfachen Installation für eine schnelle Installation. Die einfache Installation spart Zeit und Arbeit und ist weniger fehleranfällig als die in diesem Artikel beschriebene manuelle Installation.

Schritt 1: Konfigurationsinformationen und die Linux-Maschine vorbereiten

Schritt 1a: YaST-Tool starten

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

So starten Sie das textbasierte YaST-Tool:

```
su -


yast
```

So starten Sie das UI-basierte YaST-Tool:

```
su -


yast2 &
```

Schritt 1b: Netzwerk konfigurieren

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

HOSTNAMEN UND DOMAIN NAME SYSTEM (DNS) KONFIGURIEREN

1. Starten Sie das UI-basierte YaST-Tool.
2. Wählen Sie **System** und dann **Netzwerkeinstellungen**.
3. Öffnen Sie die Registerkarte **Hostname/DNS**.
4. Wählen Sie die Option **Nein** für **Hostname über DHCP festlegen**.
5. Wählen Sie die Option **Benutzerdefinierte Richtlinie verwenden** für **DNS-Konfiguration ändern**.
6. Bearbeiten Sie Folgendes, um Ihre Netzwerkkonfiguration widerzuspiegeln:

- **Statischer Hostname** – Fügen Sie den DNS-Hostnamen des Computers hinzu.
- **Nameserver** – Fügen Sie die IP-Adresse des DNS-Servers hinzu. Dies ist typischerweise die IP-Adresse des AD-Domänencontrollers.
- **Domänensuchliste** – Fügen Sie den DNS-Domänennamen hinzu.

7. Ändern Sie die folgende Zeile der Datei `/etc/hosts`, um den FQDN und den Hostnamen als erste zwei Einträge aufzunehmen:

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

> **Hinweis:**
>
> Der Linux VDA unterstützt derzeit keine NetBIOS-Namenskürzung. Daher darf der Hostname 15 Zeichen nicht überschreiten. **Tipp:**
>
> Verwenden Sie nur die Zeichen a–z, A–Z, 0–9 und Bindestriche (-). Vermeiden Sie Unterstriche (_), Leerzeichen und andere Symbole. Beginnen Sie einen Hostnamen nicht mit einer Zahl und beenden Sie ihn nicht mit einem Bindestrich. Diese Regel gilt auch für Delivery Controller-Hostnamen.

HOSTNAMEN ÜBERPRÜFEN

Überprüfen Sie, ob der Hostname korrekt eingestellt ist:

```
hostname
```

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

Überprüfen Sie, ob der FQDN korrekt eingestellt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN des Computers zurück.

NAMENSAUFLÖSUNG UND DIENSTVERFÜGBARKEIT PRÜFEN

Überprüfen Sie, ob Sie den FQDN auflösen und den Domänencontroller und den Delivery Controller™ anpingen können:

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

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

Schritt 1c: NTP-Dienst konfigurieren

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

Für SUSE 15.4:

1. Starten Sie das UI-basierte YaST-Tool.
2. Wählen Sie **Netzwerkdienste** und dann **NTP-Konfiguration**.
3. Wählen Sie im Abschnitt **NTP-Daemon starten** die Option **Jetzt und beim Start**.
4. Wählen Sie **Dynamisch** für **Konfigurationsquelle**.
5. Fügen Sie bei Bedarf NTP-Server hinzu. Der NTP-Dienst wird normalerweise auf dem Active Directory-Domänencontroller gehostet.
6. Löschen oder kommentieren Sie die folgende Zeile in /etc/chrony.conf, falls sie vorhanden ist.

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

   Nach der Bearbeitung von chrony.conf starten Sie den `chronyd` Dienst neu.

   ```
   sudo systemctl restart chronyd.service
   ```

Schritt 1d: Linux VDA-abhängige Pakete installieren

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

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

REPOSITORYS HINZUFÜGEN

Die meisten erforderlichen Pakete außer ImageMagick erhalten Sie aus den offiziellen Repositorys. Um die ImageMagick-Pakete zu erhalten, aktivieren Sie das `sle-module-desktop-applications` Repository mit YaST oder dem folgenden Befehl:

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

KERBEROS-CLIENT INSTALLIEREN

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

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

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

OPENJDK 11 INSTALLIEREN

Der Linux VDA erfordert die Installation von OpenJDK 11.

Führen Sie zum Installieren von OpenJDK 11 den folgenden Befehl aus:

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

ZU VERWENDENDE DATENBANK INSTALLIEREN UND ANGEBEN

Sie können SQLite oder PostgreSQL zur Verwendung angeben, indem Sie nach der Installation des Linux VDA-Pakets die Datei **/etc/xdl/db.conf** bearbeiten. Bei manuellen Installationen müssen Sie SQLite und PostgreSQL manuell installieren, bevor Sie sie angeben können.

Dieser Abschnitt beschreibt, wie die PostgreSQL- und SQLite-Datenbanken installiert und wie eine zu verwendende Datenbank angegeben wird.

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

PostgreSQL installieren

Führen Sie zum Installieren von `Postgresql` die folgenden Befehle aus:

```
sudo zypper install postgresql-server



sudo zypper install postgresql-jdbc
```

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

```
sudo systemctl enable postgresql



sudo systemctl restart postgresql
```

SQLite installieren

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

```
sudo zypper install sqlite3
```

Zu verwendende Datenbank angeben

Nachdem Sie SQLite, PostgreSQL oder beides installiert haben, können Sie eine zu verwendende Datenbank angeben, indem Sie nach der Installation des Linux VDA-Pakets die Datei **/etc/xdl/db.conf** bearbeiten. Gehen Sie dazu wie folgt vor:

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Überspringen Sie diesen Schritt bei einer Neuinstallation.
2. Bearbeiten Sie **/etc/xdl/db.conf**, um eine zu verwendende Datenbank anzugeben.
3. Führen Sie **ctxsetup.sh** aus.

> **Hinweis:**

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

Schritt 2: Hypervisor vorbereiten

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

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

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

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

```
su -



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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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

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

`xen.independent_wallclock = 1`

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

```
reboot
```

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

```
su -



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

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

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

Vom Verwaltungsbetriebssystem aus:

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

> **Hinweis:**

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

Zeitsynchronisierung auf ESX und ESXi beheben

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

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

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

Schritt 3: Hinzufügen der Linux-VM zur Windows-Domäne

Die folgenden Methoden stehen zum Hinzufügen von Linux-Maschinen zur Active Directory (AD)-Domäne zur Verfügung:

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Befolgen Sie die Anweisungen entsprechend der von Ihnen gewählten Methode.

> **Hinweis:**

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

Samba Winbind

WINDOWS-DOMÄNE BEITRETEN

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

1. Starten Sie YaST, wählen Sie **Netzwerkdienste** und dann **Windows-Domänenmitgliedschaft**.
2. Nehmen Sie die folgenden Änderungen vor:
   - Legen Sie die **Domäne oder Arbeitsgruppe** auf den Namen Ihrer Active Directory-Domäne oder die IP-Adresse des Domänencontrollers fest. Stellen Sie sicher, dass der Domänenname in Großbuchstaben geschrieben ist.
   - Aktivieren Sie **SMB-Informationen für Linux-Authentifizierung verwenden**.
     - Aktivieren Sie **Home-Verzeichnis bei Anmeldung erstellen**.
     - Aktivieren Sie **Single Sign-on für SSH**.
     - Stellen Sie sicher, dass **Offline-Authentifizierung** nicht aktiviert ist. Diese Option ist nicht mit dem Linux VDA kompatibel.
3. Klicken Sie auf **OK**. Wenn Sie aufgefordert werden, Pakete zu installieren, klicken Sie auf **Installieren**.
4. Wenn ein Domänencontroller gefunden wird, werden Sie gefragt, ob Sie der Domäne beitreten möchten. Klicken Sie auf **Ja**.
5. Geben Sie bei Aufforderung die Anmeldeinformationen eines Domänenbenutzers mit Berechtigung zum Hinzufügen von Maschinen zur Domäne ein und klicken Sie auf **OK**.
6. Starten Sie Ihre Dienste manuell neu oder starten Sie die Maschine neu. Wir empfehlen Ihnen, die Maschine neu zu starten:

```
su -

reboot
```

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

KERBEROS-KONFIGURATION ÜBERPRÜFEN

Stellen Sie sicher, dass die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist –ke
```

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

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

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

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

```
sudo klist
```

Überprüfen Sie die Details des Maschinenkontos mit:

```
sudo net ads status
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

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

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

Überprüfen Sie, ob das Winbind PAM-Modul korrekt konfiguriert ist. Melden Sie sich dazu am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username

id -u
```

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

```
ls /tmp/krb5cc_uid
```

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

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

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

Quest-Authentifizierungsdienst

QUEST AUF DOMÄNENCONTROLLER KONFIGURIEREN

Gehen Sie davon aus, dass Sie die Quest-Software auf den Domänencontrollern installiert und konfiguriert haben und über administrative Berechtigungen verfügen, um Computerobjekte in `Active Directory` zu erstellen.

DOMÄNENBENUTZERN DIE ANMELDUNG AN LINUX VDA-MASCHINEN ERMÖGLICHEN

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

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

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

QUEST AUF LINUX VDA KONFIGURIEREN

VAS-Daemon konfigurieren

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

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



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

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

PAM und NSS konfigurieren

Um Domänenbenutzeranmeldungen über HDX und andere Dienste wie su, ssh und RDP zu ermöglichen, konfigurieren Sie PAM und NSS manuell:

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



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

WINDOWS-DOMÄNE BEITRETEN

Fügen Sie die Linux-Maschine der Active Directory-Domäne mithilfe des Quest `vastool` Befehls hinzu:

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

Der **Benutzer** ist ein beliebiger Domänenbenutzer, der die Berechtigung hat, Maschinen der Active Directory-Domäne hinzuzufügen. Der **Domänenname** ist der DNS-Name der Domäne, zum Beispiel example.com.

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl den Domänennamen zurück. Wenn die Maschine keiner Domäne beigetreten ist, wird der folgende Fehler angezeigt:

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

Überprüfen Sie, ob Quest Domänenbenutzer über PAM authentifizieren kann. Melden Sie sich dazu am Linux-VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username

id -u
```

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

```
ls /tmp/krb5cc_uid
```

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

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

Beenden Sie die Sitzung.

```
exit
```

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

Centrify DirectControl

WINDOWS-DOMÄNE BEITRETEN

Nachdem der Centrify DirectControl Agent installiert wurde, fügen Sie die Linux-Maschine der Active Directory-Domäne mit dem Centrify-Befehl **adjoin** hinzu:

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

Der **Benutzer** ist ein beliebiger Active Directory-Domänenbenutzer, der die Berechtigung hat, Maschinen der Active Directory-Domäne hinzuzufügen. Der **Domänenname** ist der Name der Domäne, der die Linux-Maschine hinzugefügt werden soll.

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

```
sudo adinfo
```

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

Umfassendere System- und Diagnoseinformationen sind verfügbar mit:

```
adinfo --sysinfo all



adinfo –diag
```

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

```
adinfo --test
```

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

SSSD

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

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

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

DER DOMÄNE BEITRETEN UND EINEN HOST-KEYTAB ERSTELLEN

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

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

```
sudo systemctl stop nscd

sudo systemctl disable nscd
```

2. Den Hostnamen und die Chrony-Zeitsynchronisierung überprüfen.

```
hostname

hostname -f

chronyc traking
```

3. Die erforderlichen Pakete installieren oder aktualisieren:

```
sudo zypper install samba-client sssd-ad
```

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

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

```
[libdefaults]


    dns_canonicalize_hostname = false


    rdns = false
```

```
    default_realm = REALM


    forwardable = true


[realms]


    REALM = {


        kdc = fqdn-of-domain-controller


        default_domain = realm


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


    .realm = REALM
```

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

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

```
[global]

    workgroup = domain



    client signing = yes



    client use spnego = yes



    kerberos method = secrets and keytab



    realm = REALM



    security = ADS
```

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

6. Ändern Sie die **passwd**- und **group**-Einträge in der Datei **/etc/nsswitch.conf**, um auf SSSD zu verweisen, wenn Benutzer und Gruppen aufgelöst werden.

```
passwd: compat sss



group: compat sss
```

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

```
kinit administrator
```

8. Verwenden Sie das **net**-Dienstprogramm, um das System der Domäne beizutreten und eine System-Keytab-Datei zu generieren.

```
net ads join osname="SUSE Linux Enterprise Server" osVersion=15 -U
administrator
```

PAM FÜR SSSD KONFIGURIEREN

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

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

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

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

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

SSSD EINRICHTEN

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

```
[sssd]

    config_file_version = 2

    services = nss,pam

    domains = domain-dns-name



[domain/domain-dns-name]

    id_provider = ad

    auth_provider = ad
```

```
    access_provider = ad

    ad_domain = domain-dns-name

    ad_server = fqdn-of-domain-controller

    ldap_id_mapping = true

    ldap_schema = ad



# Kerberos settings

    krb5_ccachedir = /tmp

    krb5_ccname_template = FILE:%d/krb5cc_%U



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



    fallback_homedir = /home/%d/%u

    default_shell = /bin/bash



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



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



    ad_gpo_access_control = permissive
```

```
```

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

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

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

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

SSSD AKTIVIEREN

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

```
sudo systemctl enable sssd

sudo systemctl start sssd
```

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

KERBEROS-KONFIGURATION ÜBERPRÜFEN

Stellen Sie sicher, dass die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der verfügbaren Schlüssel für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten an.

Führen Sie den Kerberos-Befehl **kinit** aus, um den Computer mit diesen Schlüsseln beim Domänencontroller zu authentifizieren:

```
sudo kinit –k MACHINE\$@REALM
```

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

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

```
sudo klist
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

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

```
ssh localhost -l domain\\username



id -u
```

```
klist



exit
```

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

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

```
ls /tmp/krb5cc_uid
```

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

PBIS

ERFORDERLICHES PBIS-PAKET HERUNTERLADEN

Zum Beispiel:

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

PBIS-INSTALLATIONSSKRIPT AUSFÜHRBAR MACHEN

Zum Beispiel:

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

PBIS-INSTALLATIONSSKRIPT AUSFÜHREN

Zum Beispiel:

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

EINER WINDOWS-DOMÄNE BEITRETEN

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

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

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

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

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

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

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

Überprüfen Sie, ob PBIS Domänenbenutzer über PAM authentifizieren kann. Melden Sie sich dazu am Linux-VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\user



id -u
```

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

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit (/de-de/linux-virtual-delivery-agent/2308/installation-overview/manual-installation-overview/suse.html#step-6-install-the-linux-vda) fort.

Schritt 4: .NET Runtime 6.0 installieren

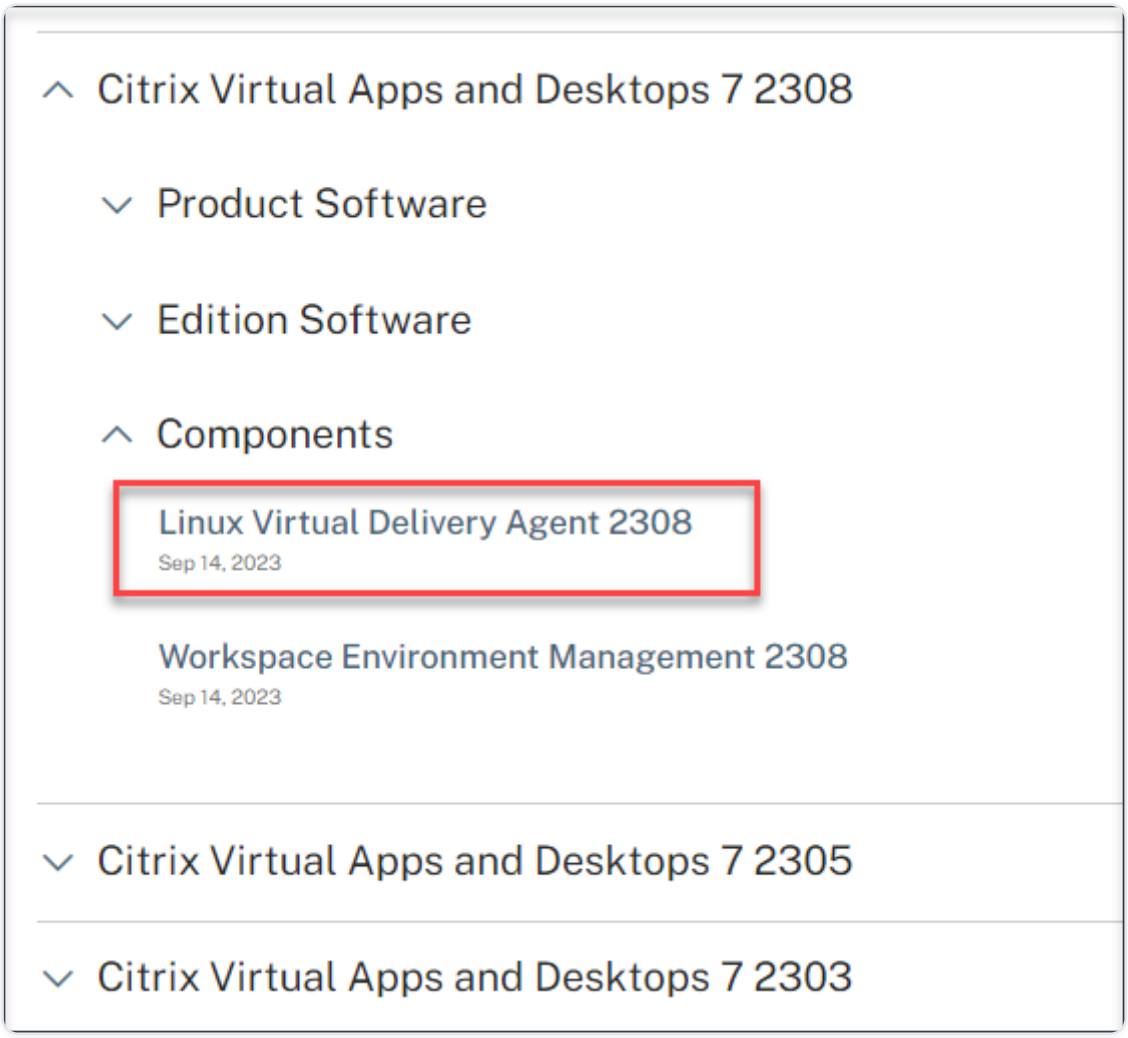
Vor der Installation des Linux VDA installieren Sie .NET Runtime 6.0 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

Nach der Installation von .NET Runtime 6.0 führen Sie den Befehl **which dotnet** aus, um Ihren Runtime-Pfad zu finden.

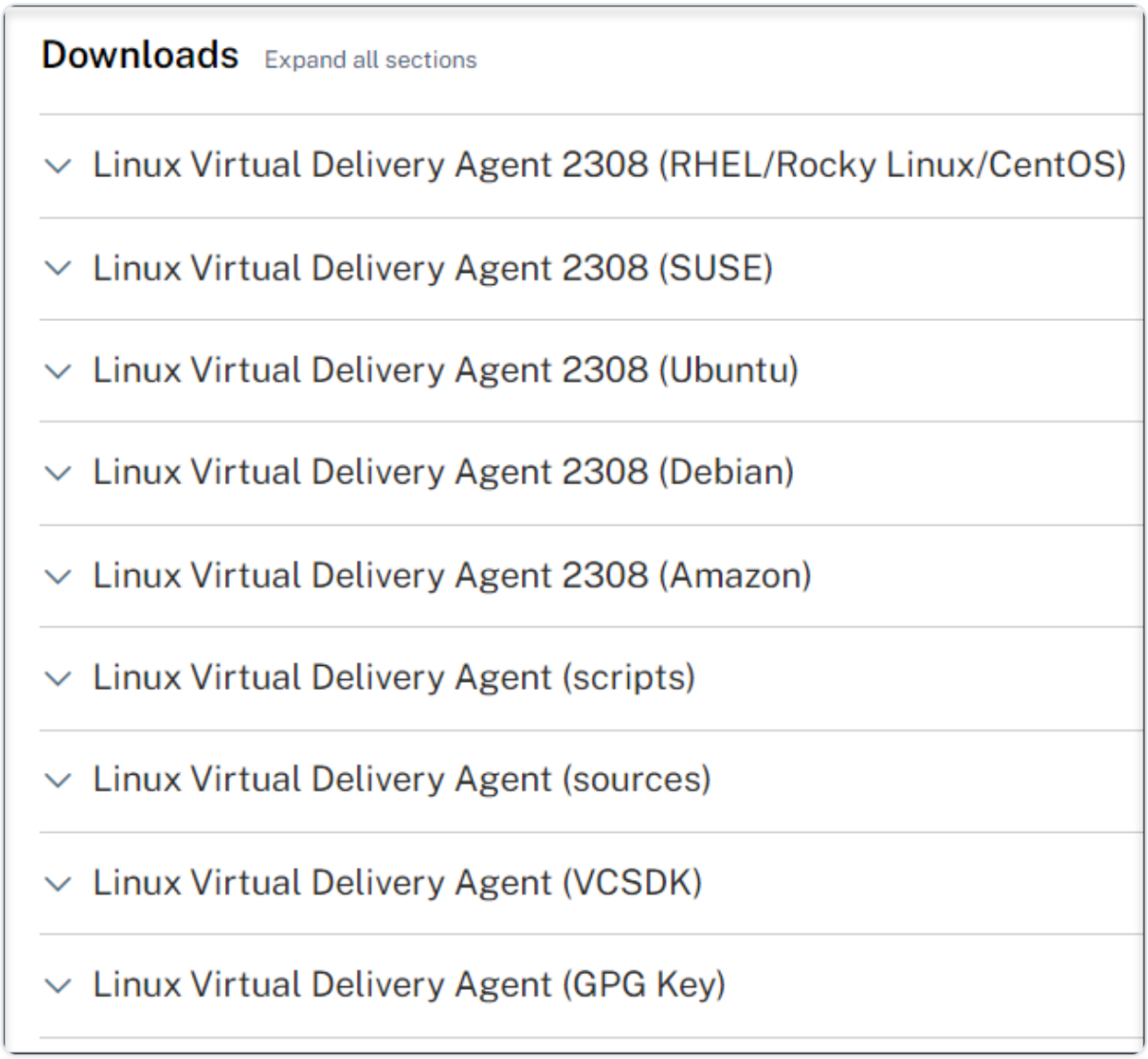
Basierend auf der Befehlsausgabe legen Sie den .NET-Runtime-Binärpfad fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Linux VDA-Paket herunterladen

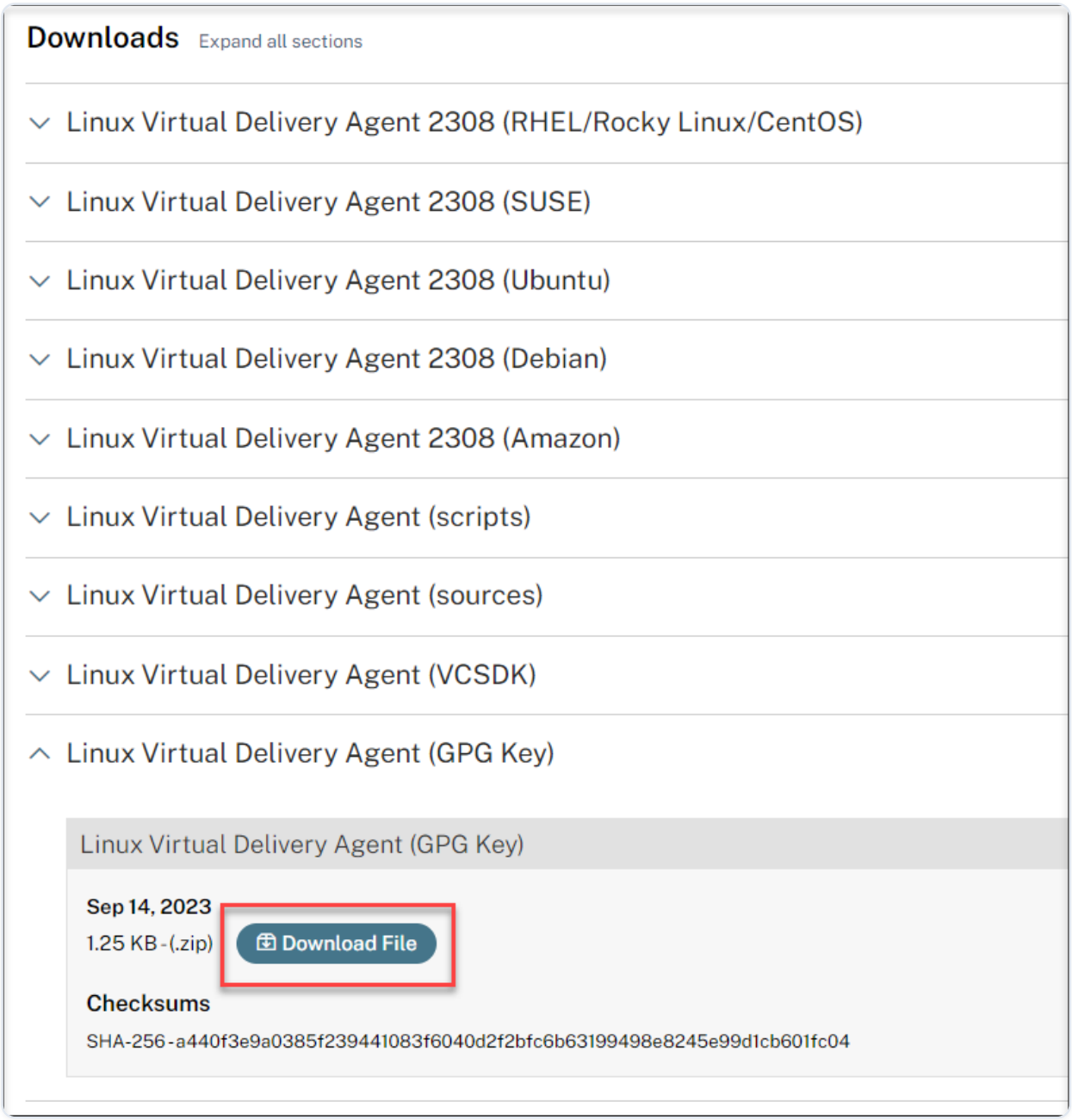
1. Gehen Sie zur Downloadseite für Citrix Virtual Apps and Desktops.
2. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. erweitern Sie **Komponenten**, um den Linux VDA zu finden. Zum Beispiel:



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, den Sie verwenden können, um die Integrität des Linux VDA-Pakets zu überprüfen. Zum 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 Paketintegrität zu überprüfen:

```
rpmkeys --import <path to the public key>

rpm --checksig --verbose <path to the Linux VDA package>
```

Schritt 6: Installieren Sie den Linux VDA

Schritt 6a: Deinstallieren Sie die alte Version

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

1. Beenden Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

Hinweis:

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

2. Deinstallieren Sie das Paket:

```
sudo rpm -e XenDesktopVDA
```

Wichtig:

Ein Upgrade von den letzten beiden Versionen wird unterstützt.

Hinweis:

Installierte Komponenten finden Sie unter **/opt/Citrix/VDA/**.

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

Schritt 6b: Installieren Sie den Linux VDA

Installieren Sie die Linux VDA-Software mit Zypper:

```
sudo zypper install XenDesktopVDA-<version>.sle15_x.x86_64.rpm
```

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

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

Schritt 6c: Upgrade des Linux VDA (optional)

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

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

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

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
```

Wichtig:

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

Schritt 7: NVIDIA GRID-Treiber installieren

Für die Aktivierung 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 (des Hosttreibers) auf den jeweiligen Hypervisoren finden Sie in den folgenden Anleitungen:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

Führen Sie die folgenden allgemeinen Schritte aus, um die NVIDIA GRID-Gast-VM-Treiber zu installieren und zu konfigurieren:

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

Schritt 8: Linux VDA konfigurieren

> **Hinweis:**

> Stellen Sie vor dem Einrichten der Laufzeitumgebung sicher, dass das Gebietsschema **en_US.UTF-8** auf Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema auf Ihrem Betriebssystem nicht verfügbar ist, führen Sie den Befehl **sudo locale-gen en_US.UTF-8** aus. Bearbeiten Sie für Debian die Datei **/etc/locale.gen**, indem Sie die Zeile # **en_US.UTF-8 UTF-8** auskommentieren, und führen Sie dann den Befehl **sudo locale-gen** aus.

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

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

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

Geführte Konfiguration

Führen Sie eine manuelle Konfiguration mit Abfragen durch:

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

Automatisierte Konfiguration

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

Unterstützte Umgebungsvariablen sind:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags. Standardmäßig auf N festgelegt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA benötigt eine durch Leerzeichen getrennte Liste von Fully Qualified Domain Names (FQDNs) der Delivery Controller, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** – Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux VDA-Dienste werden nach dem Start des Computers gestartet. Der Wert ist standardmäßig auf Y festgelegt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux VDA-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) automatisch in der System-Firewall für den Linux VDA öffnen. Standardmäßig auf Y festgelegt.
- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd** – Der Linux VDA benötigt Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird vom installierten und konfigurierten Active Directory-Integrationstool auf dem System bestimmt.

- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung grafikintensiver Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für den VDI-Desktop-Modus (Einzelsitzung) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Ob der Computer als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie diese Variable auf Y. Diese Variable ist standardmäßig auf N festgelegt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf einen lokalen Standort zu beschränken, geben Sie einen DNS-Standortnamen an. Diese Variable ist standardmäßig auf **\<none\>** festgelegt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum Beispiel ad1.mycompany.com:389 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. Um schnellere LDAP-Abfragen innerhalb einer Active Directory-Gesamtstruktur zu ermöglichen, aktivieren Sie den **Global Catalog** auf einem Domänencontroller und geben Sie die entsprechende LDAP-Portnummer als 3268 oder als 3269 an, wenn Sie LDAPS verwenden. Diese Variable ist standardmäßig auf **\<none\>** festgelegt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über einen Suchbasis-Satz ab, der auf das Stammverzeichnis der Active Directory-Domäne (z. B. DC=mycompany,DC=com) festgelegt ist. Um die Suchleistung zu verbessern, können Sie eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen 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 zur Installation der .NET Runtime 6.0 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – Gibt die in Sitzungen zu verwendende GNOME-, GNOME Classic- oder MATE-Desktopumgebung an. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

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

  a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.

  2\. Bearbeiten Sie die `.xsession`-Datei, um eine Desktopumgebung anzugeben.

  - **Für MATE-Desktop unter SUSE 15**

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



if [ -n "$MSESSION" ]; then

  exec mate-session



fi
```

  - **Für GNOME Classic-Desktop unter 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 unter SUSE 15**

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



if [ -n "$GSESSION" ]; then

exec gnome-session



fi
```

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

Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebungen anpassen. Um diese Funktion zu aktivieren, müssen Sie im Voraus umschaltbare Desktopumgebungen auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen durch Sitzungsbenutzer.

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

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N



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

```
export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=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
```

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

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \


CTX_XDL_REGISTER_SERVICE=Y|N \
```

```
CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \
```

```
CTX_XDL_TELEMETRY_PORT=port-number \


CTX_XDL_START_SERVICE=Y|N \


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

Konfigurationsänderungen entfernen

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

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

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

So entfernen Sie Konfigurationsänderungen:

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

Wichtig:

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

Konfigurationsprotokolle

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

`/tmp/xdl.configure.log`

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

Schritt 9: XDPing ausführen

Führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus, um nach häufigen Konfigurationsproblemen in einer Linux VDA-Umgebung zu suchen. Weitere Informationen finden Sie unter **XDPing**.

Schritt 10: Linux VDA ausführen

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

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxhdx start



sudo /sbin/service ctxvda start
```

Linux VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo /sbin/service ctxvda stop



sudo /sbin/service ctxhdx stop
```

> **Hinweis:**

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

> **Linux VDA neu starten:**

So starten Sie die Linux VDA-Dienste neu:

```
sudo /sbin/service ctxvda stop


sudo /sbin/service ctxhdx restart


sudo /sbin/service ctxvda start
```

Linux VDA-Status überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo /sbin/service ctxvda status


sudo /sbin/service ctxhdx status
```

Schritt 11: Maschinenkataloge erstellen

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

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

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

> **Hinweis:**

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

Tipp:

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

Schritt 12: Bereitstellungsgruppen erstellen

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

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

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

Wichtig:

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

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

Installieren Sie den Linux VDA unter Ubuntu manuell

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

Schritt 1: Konfigurationsinformationen und die Linux-Maschine vorbereiten

Schritt 1a: Netzwerkkonfiguration überprüfen

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

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

```
preserve_hostname: true
```

Schritt 1b: Hostnamen festlegen

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

```
hostname
```

Schritt 1c: Loopback-Adresse zum Hostnamen zuweisen

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

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

Zum Beispiel:

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

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

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

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

Schritt 1d: Hostnamen überprüfen

Überprüfen Sie, ob der Hostname korrekt festgelegt ist:

```
hostname
```

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

Überprüfen Sie, ob der FQDN korrekt eingestellt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN des Computers zurück.

Schritt 1e: Multicast-DNS deaktivieren

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

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

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

Zu:

`hosts: files dns`

Schritt 1f: Namensauflösung und Dienstverfügbarkeit prüfen

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

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

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

Schritt 1g: Taktsynchronisation konfigurieren (chrony)

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

Chrony installieren:

```
apt-get install chrony
```

Bearbeiten Sie als Root-Benutzer **/etc/chrony/chrony.conf** und fügen Sie einen Servereintrag für jeden externen Zeitserver hinzu:

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

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

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

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

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

```
sudo systemctl restart chrony
```

Schritt 1h: OpenJDK 11 installieren

Der Linux VDA erfordert die Installation von OpenJDK 11.

Ubuntu 22.04 enthält OpenJDK 11.

Um OpenJDK 11 unter Ubuntu 20.04 zu installieren, führen Sie den folgenden Befehl aus:

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

Schritt 1i: Eine zu verwendende Datenbank installieren und angeben

Sie können SQLite oder PostgreSQL zur Verwendung angeben, indem Sie nach der Installation des Linux VDA-Pakets die Datei **/etc/xdl/db.conf** bearbeiten. Bei manuellen Installationen müssen Sie SQLite und PostgreSQL manuell installieren, bevor Sie sie angeben können.

Dieser Abschnitt beschreibt, wie die PostgreSQL- und SQLite-Datenbanken installiert und wie eine zu verwendende Datenbank angegeben wird.

Hinweis:

Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.

POSTGRESQL INSTALLIEREN

Führen Sie die folgenden Befehle aus, um PostgreSQL zu installieren:

```
sudo apt-get install -y postgresql



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

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

```
sudo systemctl enable postgresql



sudo systemctl restart postgresql
```

SQLITE INSTALLIEREN

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

```
sudo apt-get install -y sqlite3
```

ANZUGEBENDE DATENBANK

Nachdem Sie SQLite, PostgreSQL oder beides installiert haben, können Sie eine zu verwendende Datenbank angeben, indem Sie nach der Installation des Linux VDA-Pakets die Datei **/etc/xdl/db.conf** bearbeiten. Gehen Sie dazu wie folgt vor:

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Überspringen Sie diesen Schritt bei einer Neuinstallation.
2. Bearbeiten Sie **/etc/xdl/db.conf**, um eine zu verwendende Datenbank anzugeben.
3. Führen Sie **ctxsetup.sh** aus.

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

Schritt 1j: Motif installieren

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

Schritt 1k: Andere Pakete installieren

Für 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
```

Für 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
```

Schritt 2: Hypervisor vorbereiten

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

Zeitliche Synchronisierung auf Citrix Hypervisor™ korrigieren

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

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

```
su -


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

Dieser Befehl gibt 0 oder 1 zurück:

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

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

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

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

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

`xen.independent_wallclock = 1`

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

```
su -


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

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

Linux-VMs mit installierten Hyper-V Linux Integration Services können die Hyper-V-Zeitsynchronisierungsfunktion verwenden, um die Zeit des Host-Betriebssystems zu nutzen. Um

sicherzustellen, dass die Systemuhr genau bleibt, aktivieren Sie diese Funktion zusammen mit den NTP-Diensten.

Vom Verwaltungsbetriebssystem aus:

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

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

Zeitsynchronisierung auf ESX und ESXi beheben

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

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

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

Schritt 3: Hinzufügen der Linux-VM zur Windows-Domäne

Die folgenden Methoden stehen zum Hinzufügen von Linux-Maschinen zur Active Directory (AD)-Domäne zur Verfügung:

- Samba Winbind
- Quest-Authentifizierungsdienst

- Centrify DirectControl
- SSSD
- PBIS

Befolgen Sie die Anweisungen entsprechend der von Ihnen gewählten Methode.

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

Samba Winbind

ERFORDERLICHE PAKETE INSTALLIEREN ODER AKTUALISIEREN

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

WINBIND-DAEMON FÜR DEN START BEIM MASCHINENSTART AKTIVIEREN

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

```
sudo systemctl enable winbind
```

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

KERBEROS KONFIGURIEREN

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

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

```
[libdefaults]
```

`default_realm = REALM`

`dns_lookup_kdc = false`

`[realms]`

`REALM = {`

`admin_server = domain-controller-fqdn`

`kdc = domain-controller-fqdn`

`}`

`[domain_realm]`

`domain-dns-name = REALM`

`.domain-dns-name = REALM`

Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. **example.com**. Der **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. **EXAMPLE.COM**.

WINBIND-AUTHENTIFIZIERUNG KONFIGURIEREN

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

Öffnen Sie **/etc/samba/smb.conf**, indem Sie den Befehl **vim /etc/samba/smb.conf** ausführen, 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-Realm-Name in Großbuchstaben.

NSSWITCH KONFIGURIEREN

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

`passwd: compat winbind`

`group: compat winbind`

WINDOWS-DOMÄNE BEITRETEN

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

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

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

`WINBIND` NEU STARTEN

```
sudo systemctl restart winbind
```

PAM FÜR WINBIND KONFIGURIEREN

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

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

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

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

```
sudo net ads testjoin
```

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

```
sudo net ads info
```

KERBEROS-KONFIGURATION ÜBERPRÜFEN

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

```
sudo klist -ke
```

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

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

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

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

```
sudo klist
```

Überprüfen Sie die Kontodetails des Computers mit:

```
sudo net ads status
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

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

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

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

```
ssh localhost -l domain\\username



id -u
```

Hinweis:

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

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

```
ls /tmp/krb5cc_uid
```

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

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

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

Tipp:

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

Quest-Authentifizierungsdienst

QUEST AUF DOMÄNENCONTROLLER KONFIGURIEREN

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

DOMÄNENBENUTZERN DIE ANMELDUNG AN LINUX VDA-MASCHINEN ERMÖGLICHEN

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

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

Hinweis:

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

QUEST AUF LINUX VDA KONFIGURIEREN

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

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

`SELINUX=disabled`

Diese Änderung erfordert einen Neustart des Computers:

```
reboot
```

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

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

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



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

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

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

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



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

WINDOWS-DOMÄNE BEITRETEN

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

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

Der Benutzer ist ein beliebiger Domänenbenutzer mit Berechtigungen, Computer der Active Directory-Domäne hinzuzufügen. Der **Domänenname** ist der DNS-Name der Domäne, zum Beispiel example.com.

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl den Domänennamen zurück. Wenn die Maschine keiner Domäne beigetreten ist, wird der folgende Fehler angezeigt:

`ERROR: No domain could be found.`

`ERROR: VAS_ERR_CONFIG: at ctx.c:414 in _ctx_init_default_realm` `default_realm not configured in vas.conf. Computer may not be joined to domain`

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

```
ssh localhost -l domain\\username



id -u
```

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

```
ls /tmp/krb5cc_uid
```

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

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

Beenden Sie die Sitzung.

```
exit
```

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

Centrify DirectControl

WINDOWS-DOMÄNE BEITRETEN

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

```
su –

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

Der Parameter **user** ist ein beliebiger Active Directory-Domänenbenutzer mit Berechtigungen, Computer der **Active Directory**-Domäne hinzuzufügen. Der Parameter **domain-name** ist der Name der Domäne, der die Linux-Maschine hinzugefügt werden soll.

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

```
su –



adinfo
```

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

Umfassendere System- und Diagnoseinformationen sind verfügbar über:

```
adinfo --sysinfo all



adinfo --diag
```

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

```
adinfo --test
```

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

SSSD

KERBEROS KONFIGURIEREN

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

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

Um Kerberos zu konfigurieren, öffnen Sie **/etc/krb5.conf** als Root und legen Sie die Parameter fest:

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

`[libdefaults]`

`default_realm = REALM`

`dns_lookup_kdc = false`

`[realms]`

`REALM = {`

`admin_server = domain-controller-fqdn`

`kdc = domain-controller-fqdn`

`}`

`[domain_realm]`

`domain-dns-name = REALM`

`.domain-dns-name = REALM`

Der `domain-dns-name` Parameter ist in diesem Kontext der DNS-Domänenname, z. B. example.com. Das *REALM* ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM.

DER DOMÄNE BEITRETEN

SSSD muss so konfiguriert werden, dass es Active Directory als Identitätsanbieter und Kerberos zur Authentifizierung verwendet. SSSD bietet jedoch keine AD-Client-Funktionen zum Beitreten zur Domäne und zur Verwaltung der System-Keytab-Datei. Stattdessen können Sie **adcli**, **realmd** oder **Samba** verwenden.

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

- **Wenn Sie adcli verwenden, um der Domäne beizutreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie **adcli**.

```
sudo apt-get install adcli
```

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

   Entfernen Sie die alte System-Keytab-Datei und treten Sie der Domäne bei mit:

```
su -



rm -rf /etc/krb5.keytab



adcli join domain-dns-name -U user -H hostname-fqdn
```

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

   Die Option **-H** ist für **adcli** erforderlich, um SPN im Format host/hostname-fqdn@REALM zu generieren, was der Linux VDA benötigt.

3. Überprüfen Sie die Domänenmitgliedschaft.

   Führen Sie für Ubuntu 22.04- und Ubuntu 20.04-Maschinen den Befehl `adcli testjoin` aus, um zu testen, ob die Maschinen der Domäne beigetreten sind.

- **Wenn Sie Samba verwenden, um der Domäne beizutreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.

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

2. Konfigurieren Sie **Samba**.

   Öffnen Sie **/etc/samba/smb.conf**, und nehmen Sie die folgenden Einstellungen vor:

`[global]`

`workgroup =` *`WORKGROUP`*

`security = ADS`

`realm =` *`REALM`*

`client signing = yes`

`client use spnego = yes`

`kerberos method = secrets and keytab`

WORKGROUP ist das erste Feld in **REALM**, und **REALM** ist der Kerberos-Realm-Name in Großbuchstaben.

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

   Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Windows-Konto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen.

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

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

SSSD EINRICHTEN

Erforderliche Pakete installieren oder aktualisieren:

Installieren Sie die erforderlichen SSSD- und Konfigurationspakete, falls diese noch nicht installiert sind:

```
sudo apt-get install sssd
```

Wenn die Pakete bereits installiert sind, wird ein Update empfohlen:

```
sudo apt-get install --only-upgrade sssd
```

Hinweis:

> Standardmäßig konfiguriert der Installationsprozess in Ubuntu **nsswitch.conf** und das PAM-Anmeldemodul automatisch.

SSSD KONFIGURIEREN

SSSD-Konfigurationsänderungen sind erforderlich, bevor der SSSD-Daemon gestartet wird. Bei einigen SSSD-Versionen ist die Konfigurationsdatei **/etc/sssd/sssd.conf** standardmäßig nicht installiert und muss manuell erstellt werden. Erstellen oder öffnen Sie als Root **/etc/sssd/sssd.conf** und nehmen Sie die folgenden Einstellungen vor:

```
[sssd]

services = nss, pam

config_file_version = 2

domains = domain-dns-name

[domain/domain-dns-name]

id_provider = ad

access_provider = ad

auth_provider = krb5

krb5_realm = REALM

# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days

krb5_renewable_lifetime = 14d

# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours

krb5_renew_interval = 1h

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U

# This ldap_id_mapping setting is also the default value

ldap_id_mapping = true
```

`override_homedir = /home/%d/%u`

`default_shell = /bin/bash`

`ad_gpo_map_remote_interactive = +ctxhdx`

> **Hinweis:**

> ldap_id_mapping ist auf **true** gesetzt, damit SSSD selbst die Zuordnung von Windows SIDs zu Unix UIDs übernimmt. Andernfalls muss das Active Directory POSIX-Erweiterungen bereitstellen können. Der PAM-Dienst `ctxhdx` wird zu ad_gpo_map_remote_interactive hinzugefügt.

> Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. example.com. Der **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM. Es ist nicht erforderlich, den NetBIOS-Domänennamen zu konfigurieren.

> Informationen zu den Konfigurationseinstellungen finden Sie in den Manpages für sssd.conf und `sssd-ad`.

> Der SSSD-Daemon erfordert, dass die Konfigurationsdatei nur Leseberechtigungen für den Besitzer haben darf:

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

SSSD-DAEMON STARTEN

Führen Sie die folgenden Befehle aus, um den SSSD-Daemon jetzt zu starten und ihn so zu konfigurieren, dass er beim Systemstart automatisch gestartet wird:

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

PAM-KONFIGURATION

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

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

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

KERBEROS-KONFIGURATION ÜBERPRÜFEN

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

```
sudo klist -ke
```

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

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

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

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

```
sudo klist
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

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

```
ssh localhost -l domain\\username



id -u



klist



exit
```

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

Vergewissern Sie sich als Root-Benutzer, dass eine entsprechende Ticket-Cache-Datei für die UID erstellt wurde, die vom vorherigen Befehl **id -u** zurückgegeben wurde:

```
ls /tmp/krb5cc_uid
```

Ein ähnlicher Test kann durch Anmelden bei KDE oder Gnome Display Manager durchgeführt werden. Fahren Sie nach der Überprüfung der Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

ERFORDERLICHES PBIS-PAKET HERUNTERLADEN

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

PBIS-INSTALLATIONSSKRIPT AUSFÜHRBAR MACHEN

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

PBIS-INSTALLATIONSSKRIPT AUSFÜHREN

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

WINDOWS-DOMÄNE BEITRETEN

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

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

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

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

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

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

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

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

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

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

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



id -u
```

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

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

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

Schritt 4: .NET Runtime 6.0 installieren

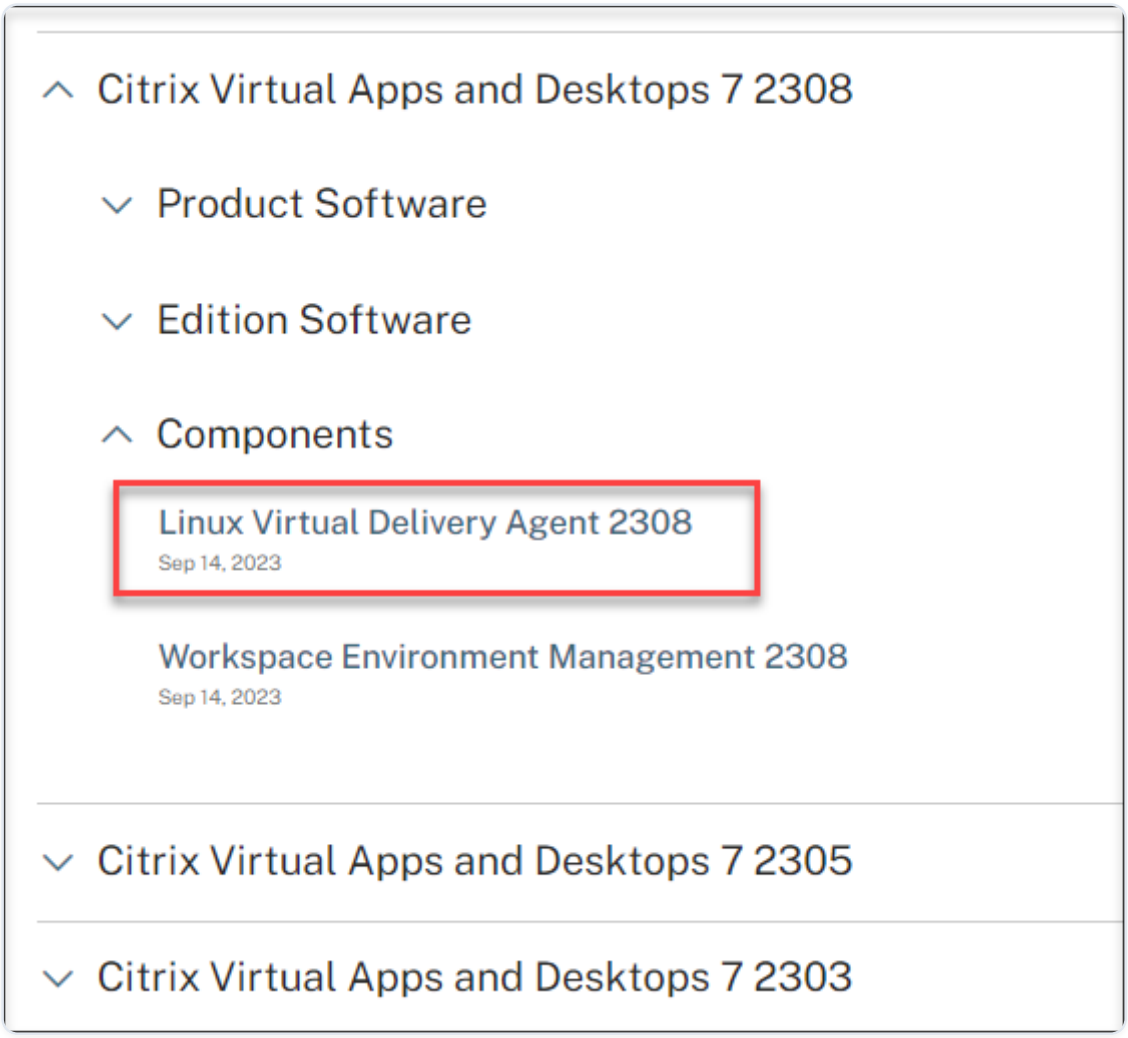
Bevor Sie den Linux VDA installieren, installieren Sie .NET Runtime 6.0 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

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

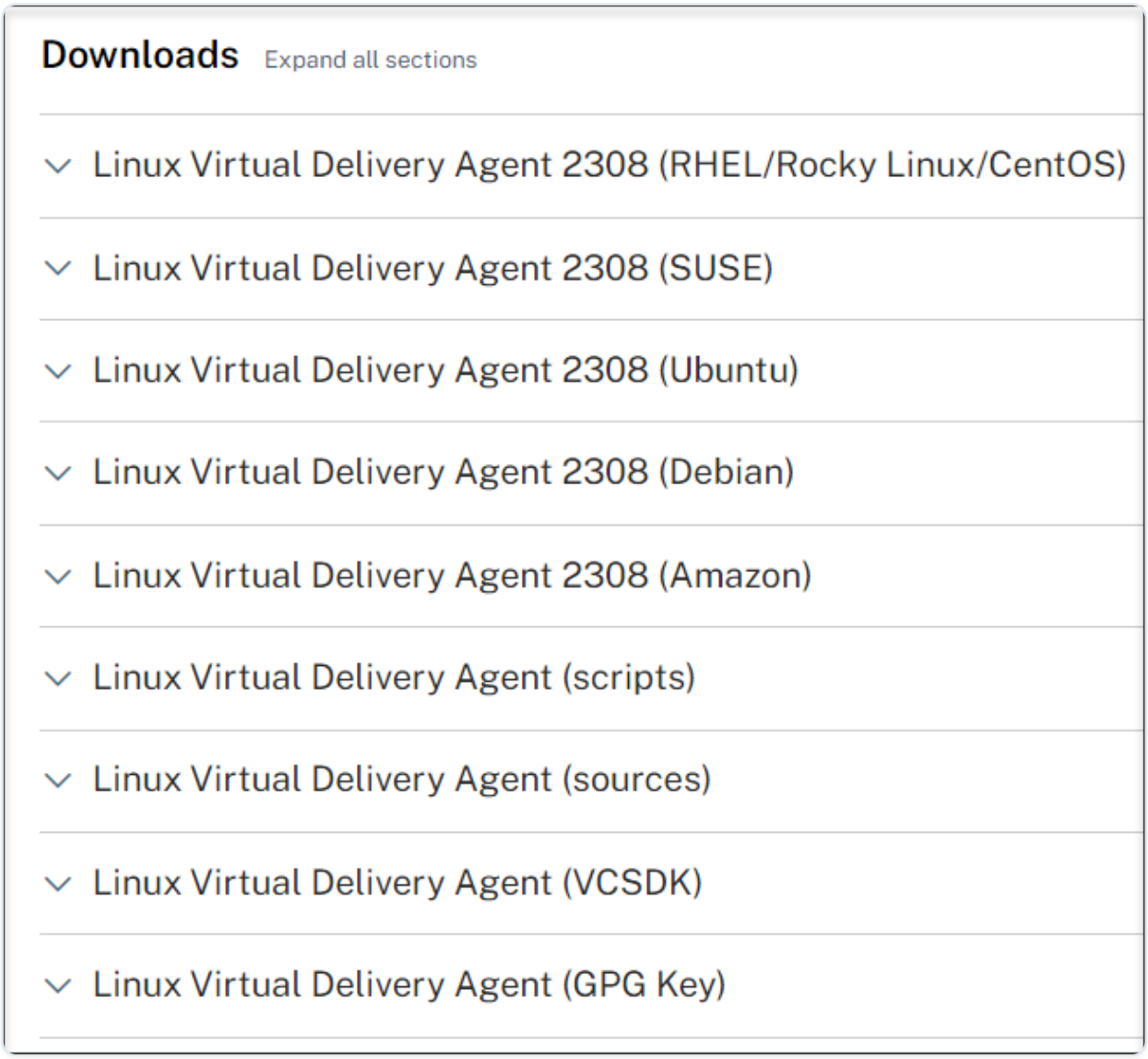
Basierend auf der Befehlsausgabe legen Sie den Binärpfad der .NET-Laufzeit fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Linux VDA-Paket herunterladen

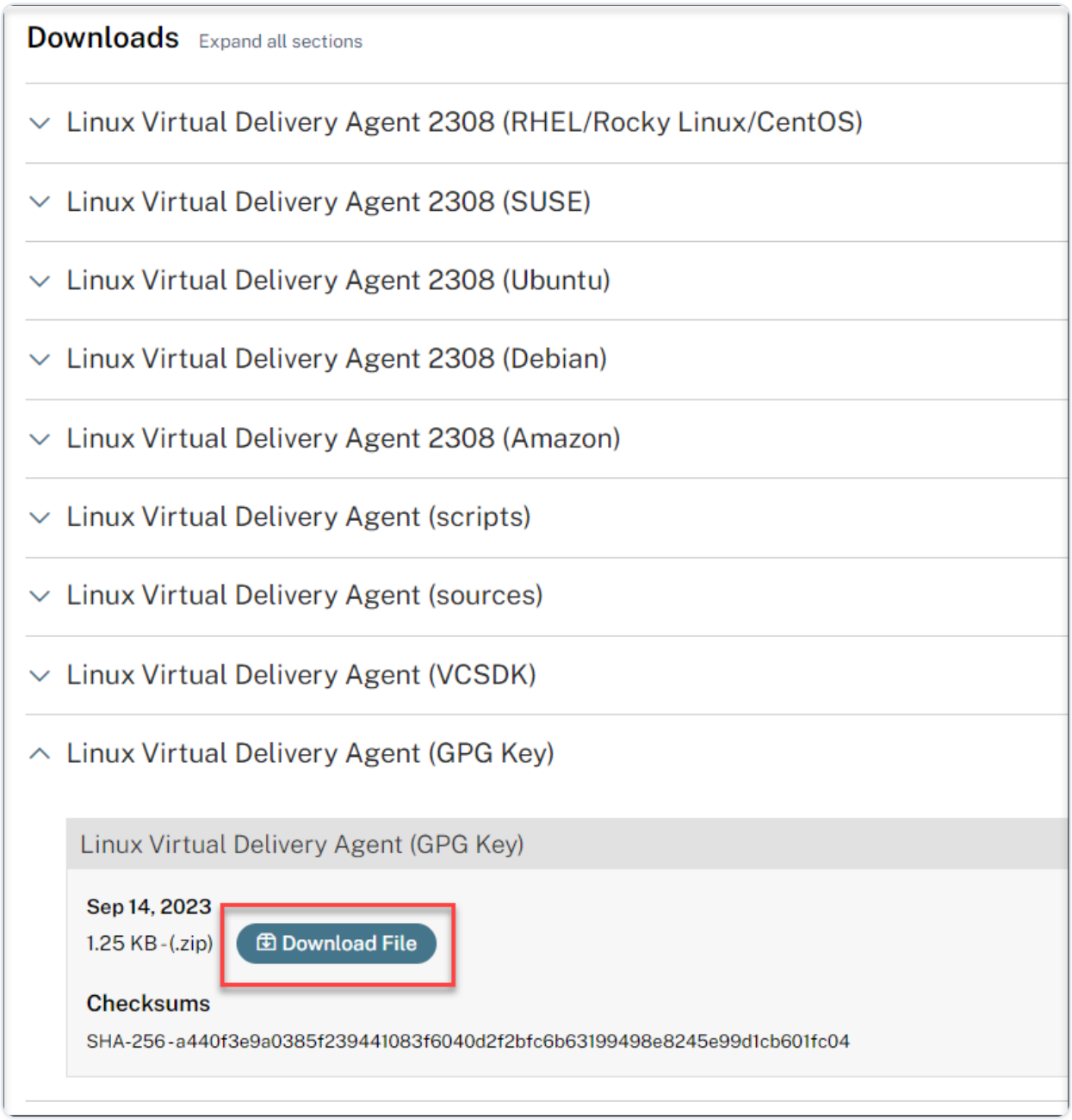
1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
2. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. erweitern Sie **Components**, um den Linux VDA zu finden. Beispiel:



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 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>
```

Schritt 6: Linux VDA installieren

Schritt 6a: Linux VDA installieren

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

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

apt-get install -f
```

Hinweis:

Für Ubuntu 20.04 auf GCP deaktivieren Sie RDNS. Fügen Sie dazu die Zeile **rdns = false** unter in /etc/krb5.conf 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
```

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
```

Hinweis:

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

Schritt 6b: Linux VDA aktualisieren (optional)

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

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

Hinweis:

Beim Aktualisieren einer vorhandenen Installation werden die Konfigurationsdateien unter /etc/xdl überschrieben. Sichern Sie die Dateien, bevor Sie ein Upgrade durchführen.

Schritt 7: NVIDIA GRID-Treiber installieren

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 Anleitungen:

- Citrix Hypervisor
- VMware ESX
- Nutanix AHV

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

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie im Hypervisor-Bedienfeld der VM 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:

Bevor Sie die Laufzeitumgebung einrichten, stellen Sie sicher, dass das Gebietsschema **en_US.UTF-8** auf Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema auf Ihrem Betriebssystem nicht verfügbar ist, führen Sie den Befehl **sudo locale-gen en_US.UTF-8** aus. Bearbeiten Sie für Debian die Datei **/etc/locale.gen**, indem Sie die Zeile # **en_US.UTF-8 UTF-8** auskommentieren, und führen Sie dann den Befehl **sudo locale-gen** aus.

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

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

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

Geführte Konfiguration

Führen Sie eine manuelle Konfiguration mit gestellten Fragen aus:

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

Automatisierte Konfiguration

Für eine automatisierte Installation können die vom Setup-Skript benötigten Optionen über Umgebungsvariablen bereitgestellt werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript den Benutzer nicht zur Eingabe von Informationen auf, was einen skriptgesteuerten Installationsprozess ermöglicht.

Unterstützte Umgebungsvariablen sind:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags. Standardmäßig auf N festgelegt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste von Fully Qualified Domain Names (FQDNs) der Delivery Controller, die für die Registrierung bei einem Delivery Controller verwendet werden sollen. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** – Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux VDA-Dienste werden nach dem Start der Maschine gestartet. Standardmäßig auf Y festgelegt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux VDA-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können

die erforderlichen Ports (standardmäßig Port 80 und 1494) automatisch in der System-Firewall für den Linux VDA öffnen. Standardmäßig auf Y festgelegt.

- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd \| pbis** – Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird anhand des installierten und konfigurierten Active Directory-Integrationstools auf dem System bestimmt.
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung grafikintensiver Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für VDI-Desktops (Einzelsitzung) konfiguriert (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Gibt an, ob die Maschine als dediziertes Desktopbereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie diese Variable auf Y. Diese Variable ist standardmäßig auf N gesetzt.
- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf einen lokalen Standort zu beschränken, geben Sie einen DNS-Standortnamen an. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum 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. Um schnellere LDAP-Abfragen innerhalb einer Active Directory-Gesamtstruktur zu ermöglichen, aktivieren Sie den **Globalen Katalog** auf einem Domänencontroller und geben Sie die relevante LDAP-Portnummer als 3268 oder als 3269 an, wenn Sie LDAPS verwenden. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne gesetzt ist (z. B. DC=mycompany,DC=com). Um die Suchleistung zu verbessern, können Sie jedoch eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt die AD-Gruppenrichtlinie nicht, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit

der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen 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 zur Installation der .NET Runtime 6.0 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – Gibt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

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

  a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.

  2\. Bearbeiten Sie die `.xsession`-Datei, um eine Desktopumgebung basierend auf den Distributionen anzugeben.

  - **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
```

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

Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebungen anpassen. Um diese Funktion zu aktivieren, müssen Sie im Voraus umschaltbare Desktopumgebungen auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen durch Sitzungsbenutzer.

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

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

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N

export CTX_XDL_DDC_LIST='list-ddc-fqdns'

export CTX_XDL_VDA_PORT=port-number

export CTX_XDL_REGISTER_SERVICE=Y|N

export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=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
```

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

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \

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

```
CTX_XDL_VDA_PORT=port-number \

CTX_XDL_REGISTER_SERVICE=Y|N \

CTX_XDL_ADD_FIREWALL_RULES=Y|N \

CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \

CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

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

```
CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \


CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \


CTX_XDL_TELEMETRY_PORT=port-number \


CTX_XDL_START_SERVICE=Y|N \


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

Konfigurationsänderungen entfernen

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

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

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

So entfernen Sie Konfigurationsänderungen:

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

Wichtig:

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

Konfigurationsprotokolle

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

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

Deinstallieren der Linux VDA-Software

So überprüfen Sie, ob der Linux VDA installiert ist und welche Version des installierten Pakets vorliegt:

```
dpkg -l xendesktopvda
```

So zeigen Sie detailliertere Informationen an:

```
apt-cache show xendesktopvda
```

So deinstallieren Sie die Linux VDA-Software:

```
dpkg -r xendesktopvda
```

Hinweis:

Durch die Deinstallation der Linux VDA-Software werden die zugehörigen PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden jedoch nicht gelöscht.

Tipp:

Die Informationen in diesem Abschnitt behandeln nicht die Entfernung abhängiger Pakete, einschließlich PostgreSQL.

Schritt 9: XDPing ausführen

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

Schritt 10: Linux VDA ausführen

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

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Linux VDA beenden:

So beenden Sie die Linux VDA-Dienste:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

> **Hinweis:**

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

> **Linux VDA neu starten:**

So starten Sie die Linux VDA-Dienste neu:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx
```

```
sudo systemctl restart ctxvda
```

Linux VDA-Status überprüfen:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda
```

```
sudo systemctl status ctxhdx
```

Schritt 11: Maschinenkataloge erstellen

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

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

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

Hinweis:

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

> **Tipp:**

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

Schritt 12: Bereitstellungsgruppen erstellen

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

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

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

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

Installieren Sie den Linux VDA unter Debian manuell

> **Wichtig:**

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

Schritt 1: Konfigurationsinformationen und die Linux-Maschine vorbereiten

Schritt 1a: Hostnamen festlegen

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

`hostname`

Schritt 1b: Eine Loopback-Adresse dem Hostnamen zuweisen

Stellen Sie sicher, dass der DNS-Domänenname und der vollqualifizierte Domänenname (FQDN) der Maschine korrekt zurückgemeldet werden. Dazu ändern Sie die folgende Zeile der Datei **/etc/hosts** so, dass sie den FQDN und den Hostnamen als erste zwei Einträge enthält:

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

Zum Beispiel:

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

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

> **Hinweis:**

> Der Linux VDA unterstützt derzeit keine NetBIOS-Namenskürzung. Der Hostname darf 15 Zeichen nicht überschreiten.

> **Tipp:**

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

Schritt 1c: Hostnamen überprüfen

Starten Sie die Maschine neu und überprüfen Sie, ob der Hostname korrekt festgelegt ist:

```
hostname
```

Dieser Befehl gibt nur den Hostnamen der Maschine zurück, nicht ihren FQDN.

Überprüfen Sie, ob der FQDN korrekt festgelegt ist:

```
hostname -f
```

Dieser Befehl gibt den FQDN der Maschine zurück.

Schritt 1d: Multicast-DNS deaktivieren

Die Standardeinstellungen haben Multicast-DNS (**mDNS**) aktiviert, was zu inkonsistenten Namensauflösungsergebnissen führen kann.

Um **mDNS** zu deaktivieren, bearbeiten Sie **/etc/nsswitch.conf** und ändern Sie die Zeile:

`hosts: files mdns_minimal [NOTFOUND=return] dns`

Zu:

`hosts: files dns`

Schritt 1e: Namensauflösung und Dienstverfügbarkeit prüfen

Stellen Sie sicher, dass Sie den FQDN auflösen und den Domänencontroller und Delivery Controller™ anpingen können:

```
nslookup domain-controller-fqdn


ping domain-controller-fqdn


nslookup delivery-controller-fqdn


ping delivery-controller-fqdn
```

Wenn Sie den FQDN nicht auflösen oder eine dieser Maschinen nicht anpingen können, überprüfen Sie die Schritte, bevor Sie fortfahren.

Schritt 1f: Taktsynchronisierung konfigurieren (chrony)

Die Aufrechterhaltung einer genauen Taktsynchronisierung zwischen den VDAs, Delivery Controllern und Domänencontrollern ist entscheidend. Das Hosten des Linux VDA als virtuelle

Maschine (VM) kann zu Problemen mit der Taktverschiebung führen. Aus diesem Grund wird die Synchronisierung der Zeit mit einem Remote-Zeitdienst bevorzugt.

Chrony installieren:

```
apt-get install chrony
```

Bearbeiten Sie als Root-Benutzer **/etc/chrony/chrony.conf** und fügen Sie einen Servereintrag für jeden Remote-Zeitserver hinzu:

`server peer1-fqdn-or-ip-address iburst`

`server peer2-fqdn-or-ip-address iburst`

In einer typischen Bereitstellung synchronisieren Sie die Zeit von den lokalen Domänencontrollern und nicht direkt von öffentlichen NTP-Pool-Servern. Fügen Sie einen Servereintrag für jeden Active Directory-Domänencontroller in der Domäne hinzu.

Entfernen Sie alle anderen aufgeführten **server**- oder **pool**-Einträge, einschließlich Loopback-IP-Adresse, Localhost und öffentliche Server-Einträge ***.pool.ntp.org**.

Speichern Sie die Änderungen und starten Sie den Chrony-Daemon neu:

```
sudo systemctl restart chrony
```

Schritt 1g: Pakete installieren

```
sudo apt-get install -y libsasl2-2



sudo apt-get install -y libgtk2.0-0
```

Schritt 1h: Repositories hinzufügen, um notwendige Abhängigkeiten zu installieren

Für Debian 11.3 fügen Sie die `deb http://deb.debian.org/debian/ bullseye main` Zeile zur Datei /etc/apt/sources.list hinzu.

Schritt 1i: Eine zu verwendende Datenbank installieren und angeben

Sie können SQLite oder PostgreSQL zur Verwendung 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, bevor Sie sie angeben können.

Dieser Abschnitt beschreibt, wie die PostgreSQL- und SQLite-Datenbanken installiert und wie eine zu verwendende Datenbank angegeben wird.

> **Hinweis:**
>
> Wir empfehlen, SQLite nur für den VDI-Modus zu verwenden.

POSTGRESQL INSTALLIEREN

Führen Sie die folgenden Befehle aus, um PostgreSQL zu installieren:

```
sudo apt-get update


sudo apt-get install -y postgresql


sudo apt-get install -y libpostgresql-jdbc-java
```

Führen Sie die folgenden Befehle aus, um PostgreSQL beim Systemstart bzw. sofort zu starten:

```
sudo systemctl enable postgresql


sudo systemctl start postgresql
```

SQLITE INSTALLIEREN

Führen Sie für Debian den folgenden Befehl aus, um SQLite zu installieren:

```
sudo apt-get install -y sqlite3
```

EINE ZU VERWENDENDE DATENBANK ANGEBEN

Nach der Installation des Linux VDA-Pakets können Sie eine zu verwendende Datenbank angeben, indem Sie **/etc/xdl/db.conf** bearbeiten. Gehen Sie dazu wie folgt vor:

1. Führen Sie **/opt/Citrix/VDA/sbin/ctxcleanup.sh** aus. Überspringen Sie diesen Schritt, 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: Hypervisor vorbereiten

Einige Änderungen sind erforderlich, wenn der Linux VDA als VM auf einem unterstützten Hypervisor ausgeführt wird. Nehmen Sie die folgenden Änderungen basierend auf der verwendeten Hypervisor-Plattform vor. Es sind keine Änderungen erforderlich, wenn Sie die Linux-Maschine auf Bare-Metal-Hardware ausführen.

Zeitsynchronisierung auf Citrix Hypervisor™ beheben

Wenn die Zeitsynchronisierungsfunktion von Citrix Hypervisor aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und Citrix Hypervisor auf. Beide versuchen, die Systemuhr zu verwalten. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit dem NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden. Im HVM-Modus sind keine Änderungen erforderlich.

Wenn Sie einen paravirtualisierten Linux-Kernel mit installierten Citrix VM Tools ausführen, können Sie überprüfen, ob die Citrix Hypervisor-Zeitsynchronisierungsfunktion in der Linux-VM vorhanden und aktiviert ist:

```
su -

cat /proc/sys/xen/independent_wallclock
```

Dieser Befehl gibt 0 oder 1 zurück:

- 0 – Die Zeitsynchronisierungsfunktion ist aktiviert und muss deaktiviert werden.
- 1 – Die Zeitsynchronisierungsfunktion ist deaktiviert, und es sind keine weiteren Maßnahmen erforderlich.

Wenn die Datei /proc/sys/xen/independent_wallclock nicht vorhanden ist, sind die folgenden Schritte nicht erforderlich.

Falls aktiviert, deaktivieren Sie die Zeitsynchronisierungsfunktion, indem Sie 1 in die Datei schreiben:

```
sudo echo 1 > /proc/sys/xen/independent_wallclock
```

Um diese Änderung dauerhaft und nach einem Neustart beizubehalten, bearbeiten Sie die Datei ***/etc/sysctl.conf*** und fügen Sie die Zeile hinzu:

`xen.independent_wallclock = 1`

Um diese Änderungen zu überprüfen, starten Sie das System neu:

```
su -

cat /proc/sys/xen/independent_wallclock
```

Dieser Befehl gibt den Wert 1 zurück.

Zeitsynchronisierung auf Microsoft Hyper-V beheben

Linux-VMs mit installierten Hyper-V Linux Integration Services können die Hyper-V-Zeitsynchronisierungsfunktion verwenden, um die Zeit des Host-Betriebssystems zu nutzen. Um sicherzustellen, dass die Systemuhr genau bleibt, aktivieren Sie diese Funktion zusammen mit NTP-Diensten.

Vom Verwaltungsbetriebssystem aus:

1. Öffnen Sie die Hyper-V-Manager-Konsole.
2. Wählen Sie für die Einstellungen einer Linux-VM **Integrationsdienste** aus.
3. Stellen Sie sicher, dass **Zeitsynchronisierung** ausgewählt ist.

> **Hinweis:**

> Dieser Ansatz unterscheidet sich von VMware und Citrix Hypervisor, wo die Host-Zeitsynchronisierung deaktiviert ist, um Konflikte mit NTP zu vermeiden. Die Hyper-V-Zeitsynchronisierung kann mit der NTP-Zeitsynchronisierung koexistieren und diese ergänzen.

Zeitsynchronisierung auf ESX und ESXi beheben

Wenn die VMware-Zeitsynchronisierungsfunktion aktiviert ist, treten in jeder paravirtualisierten Linux-VM Probleme mit NTP und dem Hypervisor auf. Beide versuchen, die Systemuhr zu synchronisieren. Um zu vermeiden, dass die Uhr mit anderen Servern nicht mehr synchron ist, stellen Sie sicher, dass die Systemuhr in jedem Linux-Gast mit NTP synchronisiert ist. In diesem Fall muss die Host-Zeitsynchronisierung deaktiviert werden.

Wenn Sie einen paravirtualisierten Linux-Kernel mit installierten VMware Tools ausführen:

1. Öffnen Sie den vSphere Client.
2. Bearbeiten Sie die Einstellungen für die Linux-VM.
3. Öffnen Sie im Dialogfeld **Eigenschaften der virtuellen Maschine** die Registerkarte **Optionen**.
4. Wählen Sie **VMware Tools** aus.
5. Deaktivieren Sie im Feld **Erweitert** die Option **Gastzeit mit Host synchronisieren**.

Schritt 3: Fügen Sie die Linux-VM zur Windows-Domäne hinzu

Die folgenden Methoden stehen zur Verfügung, um Linux-Maschinen zur Active Directory (AD)-Domäne hinzuzufügen:

- Samba Winbind
- Centrify DirectControl
- SSSD
- PBIS

Befolgen Sie die Anweisungen entsprechend der von Ihnen gewählten Methode.

> **Hinweis:**

> Sitzungsstarts können fehlschlagen, wenn derselbe Benutzername für das lokale Konto im Linux VDA und das Konto in AD verwendet wird.

Samba Winbind

ERFORDERLICHE PAKETE INSTALLIEREN ODER AKTUALISIEREN

```
sudo apt-get install winbind samba libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user
```

WINBIND-DAEMON BEIM MASCHINENSTART AKTIVIEREN

Der Winbind-Daemon muss so konfiguriert werden, dass er beim Maschinenstart gestartet wird:

```
sudo systemctl enable winbind
```

> **Hinweis:**
>
> Stellen Sie sicher, dass das Skript `winbind` unter `/etc/init.d` liegt.

KERBEROS KONFIGURIEREN

Öffnen Sie **/etc/krb5.conf** als Root-Benutzer und nehmen Sie die folgenden Einstellungen vor:

> **Hinweis:**
>
> Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Einzeldomänen-, Einzelforst-Modell vorgesehen.

`[libdefaults]`

`default_realm =` *`REALM`*

`dns_lookup_kdc = false`

`[realms]`

`REALM` `= {`

`admin_server =` *`domain-controller-fqdn`*

`kdc =` *`domain-controller-fqdn`*

`}`

`[domain_realm]`

`domain-dns-name` `=` `REALM`

`.domain-dns-name` `=` `REALM`

Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. **example.com**. Das **REALM** ist der Kerberos-Realm-Name in Großbuchstaben, z. B. **EXAMPLE.COM**.

WINBIND-AUTHENTIFIZIERUNG KONFIGURIEREN

Öffnen Sie **/etc/samba/smb.conf**, indem Sie den Befehl **vim /etc/samba/smb.conf** ausführen, 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-Realm-Name in Großbuchstaben.

NSSWITCH KONFIGURIEREN

Öffnen Sie **/etc/nsswitch.conf**, und fügen Sie `winbind` an die folgenden Zeilen an:

`passwd: files systemd winbind`

`group: files systemd winbind`

WINDOWS-DOMÄNE BEITRETEN

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo net ads join <Kerberos realm name in uppercase> -U <domain user with permission to add computers to the domain>
```

WINBIND NEU STARTEN

```
sudo systemctl restart winbind
```

PAM FÜR WINBIND KONFIGURIEREN

Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass die Optionen **Winbind NT/Active Directory-Authentifizierung** und **Home-Verzeichnis bei Anmeldung erstellen** ausgewählt sind:

```
sudo pam-auth-update
```

Tipp:

Der **Winbind**-Daemon bleibt nur aktiv, wenn der Computer einer Domäne beigetreten ist.

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in `Active Directory` haben.

Führen Sie den Befehl **net ads** von **Samba** aus, um zu überprüfen, ob der Computer einer Domäne beigetreten ist:

```
sudo net ads testjoin
```

Führen Sie den folgenden Befehl aus, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen:

```
sudo net ads info
```

KERBEROS-KONFIGURATION ÜBERPRÜFEN

Um zu überprüfen, ob Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, stellen Sie sicher, dass die System-**Keytab**-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der Schlüssel an, die für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten verfügbar sind. Führen Sie den Kerberos-Befehl **kinit** aus, um die Maschine mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Die Maschinen- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Maschinenkonto mit folgendem Befehl zwischengespeichert wurde:

```
sudo klist
```

Überprüfen Sie die Kontodetails des Computers mit:

```
sudo net ads status
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

Verwenden Sie das Tool **wbinfo**, um zu überprüfen, ob Domänenbenutzer sich bei der Domäne authentifizieren können:

```
wbinfo --krb5auth=domain\\username%password
```

Die hier angegebene Domäne ist der AD-Domänenname, nicht der Kerberos-Realm-Name. Für die Bash-Shell muss der Backslash (\\) mit einem weiteren Backslash maskiert werden. Dieser Befehl gibt eine Meldung zurück, die den Erfolg oder Misserfolg anzeigt.

Um zu überprüfen, ob das Winbind PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u
```

Hinweis:

Um einen SSH-Befehl erfolgreich auszuführen, stellen Sie sicher, dass SSH aktiviert ist und ordnungsgemäß funktioniert.

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die von dem Befehl **id -u** zurückgegebene uid erstellt wurde:

```
ls /tmp/krb5cc_uid
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

Beenden Sie die Sitzung.

```
exit
```

Ein ähnlicher Test kann durchgeführt werden, indem Sie sich direkt an der Gnome- oder KDE-Konsole anmelden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Tipp:

Wenn die Benutzerauthentifizierung erfolgreich ist, Sie aber Ihren Desktop beim Anmelden mit einem Domänenkonto nicht anzeigen können, starten Sie den Computer neu und versuchen Sie es erneut.

Centrify DirectControl

WINDOWS-DOMÄNE BEITRETEN

Nach der Installation des Centrify DirectControl Agent fügen Sie den Linux-Computer mit dem Centrify-Befehl `adjoin` der Active Directory-Domäne hinzu:

```
su –

adjoin -w -V -u user domain-name
```

Der Parameter **user** ist ein beliebiger Active Directory-Domänenbenutzer mit Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne. Der Parameter **domain-name** ist der Name der Domäne, der der Linux-Computer beitreten soll.

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

Der Delivery Controller erfordert, dass alle VDA-Maschinen, ob Windows oder Linux, ein Computerobjekt in Active Directory haben. Um zu überprüfen, ob eine mit Centrify verbundene Linux-Maschine in der Domäne ist:

```
su –


adinfo
```

Überprüfen Sie, ob der Wert **Joined to domain** gültig ist und der **CentrifyDC mode** den Wert **connected** zurückgibt. Wenn der Modus im Startzustand hängen bleibt, hat der Centrify-Client Probleme mit der Serververbindung oder Authentifizierung.

Umfassendere System- und Diagnoseinformationen sind verfügbar über:

```
adinfo --sysinfo all


adinfo --diag
```

Testen Sie die Konnektivität zu den verschiedenen Active Directory- und Kerberos-Diensten.

```
adinfo --test
```

Fahren Sie nach der Überprüfung der Domänenverbindung mit Schritt 6: Installieren des Linux VDA fort.

SSSD

KERBEROS KONFIGURIEREN

Führen Sie den folgenden Befehl aus, um Kerberos zu installieren:

```
sudo apt-get install krb5-user
```

Um Kerberos zu konfigurieren, öffnen Sie **/etc/krb5.conf** als Root und legen Sie die Parameter fest:

Hinweis:

Konfigurieren Sie Kerberos basierend auf Ihrer AD-Infrastruktur. Die folgenden Einstellungen sind für das Einzeldomänen-, Einzelforst-Modell vorgesehen.

```
[libdefaults]
```

`default_realm = REALM`

`dns_lookup_kdc = false`

`rdns = false`

`[realms]`

`REALM = {`

`admin_server = domain-controller-fqdn`

`kdc = domain-controller-fqdn`

`}`

`[domain_realm]`

`domain-dns-name` = `REALM`

`.domain-dns-name` = `REALM`

Der `domain-dns-name`-Parameter in diesem Kontext ist der DNS-Domänenname, z. B. example.com. Der *REALM* ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM.

DER DOMÄNE BEITRETEN

SSSD muss so konfiguriert werden, dass es Active Directory als Identitätsanbieter und Kerberos zur Authentifizierung verwendet. SSSD bietet jedoch keine AD-Client-Funktionen für den Domänenbeitritt und die Verwaltung der System-Keytab-Datei. Stattdessen können Sie **adcli**, **realmd** oder **Samba** verwenden.

> **Hinweis:**
>
> Dieser Abschnitt enthält nur Informationen zu **adcli** und **Samba**.

- **Wenn Sie adcli für den Domänenbeitritt verwenden, führen Sie die folgenden Schritte aus:**

1. Installieren Sie **adcli**.

   ```
   sudo apt-get install adcli
   ```

2. Treten Sie der Domäne mit **adcli** bei.

   Entfernen Sie die alte System-Keytab-Datei und treten Sie der Domäne mit Folgendem bei:

   ```
   su -



   rm -rf /etc/krb5.keytab



   adcli join domain-dns-name -U user -H hostname-fqdn
   ```

Der **user** ist ein Domänenbenutzer mit Berechtigungen zum Hinzufügen von Maschinen zur Domäne. Der **hostname-fqdn** ist der Hostname im FQDN-Format für die Maschine.

Die Option **-H** ist für **adcli** erforderlich, um SPN im Format host/hostname-fqdn@REALM zu generieren, was der Linux VDA benötigt.

3. System-Keytab überprüfen.

   Führen Sie den Befehl `sudo klist -ket` aus, um sicherzustellen, dass die System-Keytab-Datei erstellt wurde.

   Stellen Sie sicher, dass der Zeitstempel für jeden Schlüssel mit der Zeit übereinstimmt, zu der die Maschine der Domäne beigetreten ist.

- **Wenn Sie Samba verwenden, um der Domäne beizutreten, führen Sie die folgenden Schritte aus:**

1. Installieren Sie das Paket.

   ```
   sudo apt-get install samba krb5-user
   ```

2. Konfigurieren Sie **Samba**.

   Öffnen Sie **/etc/samba/smb.conf** und nehmen Sie die folgenden Einstellungen vor:

   `[global]`

   `workgroup =` *`WORKGROUP`*

   `security = ADS`

   `realm =` *`REALM`*

   `client signing = yes`

   `client use spnego = yes`

   `kerberos method = secrets and keytab`

   WORKGROUP ist das erste Feld in *REALM*, und *REALM* ist der Kerberos-Realm-Name in Großbuchstaben.

3. Treten Sie der Domäne mit **Samba** bei.

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Windows-Konto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen.

```
sudo net ads join <the Kerberos realm name in uppercase> -U <domain user with permission to add computers to the domain>
```

SSSD EINRICHTEN

Erforderliche Pakete installieren oder aktualisieren:

Installieren Sie die erforderlichen SSSD- und Konfigurationspakete, falls noch nicht geschehen:

```
sudo apt-get install sssd
```

Wenn die Pakete bereits installiert sind, wird ein Update empfohlen:

```
sudo apt-get install --only-upgrade sssd
```

SSSD KONFIGURIEREN

SSSD-Konfigurationsänderungen sind erforderlich, bevor der SSSD-Daemon gestartet wird. Bei einigen SSSD-Versionen ist die Konfigurationsdatei **/etc/sssd/sssd.conf** standardmäßig nicht installiert und muss manuell erstellt werden. Erstellen oder öffnen Sie als Root **/etc/sssd/sssd.conf** und nehmen Sie die folgenden Einstellungen vor:

`[sssd]`

`services = nss, pam`

`config_file_version = 2`

`domains =` *`domain-dns-name`*

`[domain/`*`domain-dns-name`*`]`

`id_provider = ad`

`access_provider = ad`

`auth_provider = krb5`

`krb5_realm =` *`REALM`*

```
# Set krb5_renewable_lifetime higher if TGT renew lifetime is longer than 14 days
```

```
krb5_renewable_lifetime = 14d
```

```
# Set krb5_renew_interval to lower value if TGT ticket lifetime is shorter than 2 hours
```

```
krb5_renew_interval = 1h
```

```
krb5_ccachedir = /tmp
```

```
krb5_ccname_template = FILE:%d/krb5cc_%U
```

```
# This ldap_id_mapping setting is also the default value
```

```
ldap_id_mapping = true
```

```
override_homedir = /home/%d/%u
```

```
default_shell = /bin/bash
```

```
ad_gpo_map_remote_interactive = +ctxhdx
```

> **Hinweis:**

> ldap_id_mapping ist auf **true** gesetzt, damit SSSD selbst die Zuordnung von Windows-SIDs zu Unix-UIDs übernimmt. Andernfalls muss `Active Directory` POSIX-Erweiterungen bereitstellen können. Der PAM-Dienst `ctxhdx` wird zu ad_gpo_map_remote_interactive hinzugefügt.

> Der Parameter **domain-dns-name** ist in diesem Kontext der DNS-Domänenname, z. B. example.com. Das *REALM* ist der Kerberos-Realm-Name in Großbuchstaben, z. B. EXAMPLE.COM. Es ist nicht erforderlich, den NetBIOS-Domänennamen zu konfigurieren.

> Informationen zu den Konfigurationseinstellungen finden Sie in den Manpages für sssd.conf und `sssd-ad`.

> Der SSSD-Daemon erfordert, dass die Konfigurationsdatei nur Leseberechtigungen für den Besitzer hat:

```
sudo chmod 0600 /etc/sssd/sssd.conf
```

SSSD-DAEMON STARTEN

Führen Sie die folgenden Befehle aus, um den SSSD-Daemon jetzt zu starten und ihn so zu konfigurieren, dass er beim Systemstart automatisch gestartet wird:

```
sudo systemctl start sssd



sudo systemctl enable sssd
```

PAM-KONFIGURATION

Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass die Optionen **SSS-Authentifizierung** und **Home-Verzeichnis bei Anmeldung erstellen** ausgewählt sind:

```
sudo pam-auth-update
```

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in `Active Directory` haben.

- Wenn Sie **adcli** zur Überprüfung der Domänenmitgliedschaft verwenden, führen Sie den Befehl `sudo adcli info domain-dns-name` aus, um die Domäneninformationen anzuzeigen.
- Wenn Sie **Samba** zur Überprüfung der Domänenmitgliedschaft verwenden, führen Sie den Befehl `sudo net ads testjoin` aus, um zu überprüfen, ob die Maschine einer Domäne beigetreten ist, und den Befehl `sudo net ads info`, um zusätzliche Domänen- und Computerobjektinformationen zu überprüfen.

KERBEROS-KONFIGURATION ÜBERPRÜFEN

Um zu überprüfen, ob Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, stellen Sie sicher, dass die System-Keytab-Datei erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der Schlüssel an, die für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersammlungen verfügbar sind. Führen Sie den Kerberos-Befehl `kinit` aus, um den Computer mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit -k MACHINE\$@REALM
```

Der Computer- und Realm-Name müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT für das Computerkonto mit folgendem Befehl zwischengespeichert wurde:

```
sudo klist
```

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

SSSD bietet kein Befehlszeilentool zum direkten Testen der Authentifizierung mit dem Daemon und kann nur über PAM erfolgen.

Um zu überprüfen, ob das SSSD PAM-Modul korrekt konfiguriert ist, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
ssh localhost -l domain\\username



id -u



klist



exit
```

Überprüfen Sie, ob die vom Befehl **klist** zurückgegebenen Kerberos-Tickets für diesen Benutzer korrekt sind und nicht abgelaufen sind.

Überprüfen Sie als Root-Benutzer, ob eine entsprechende Ticket-Cache-Datei für die UID erstellt wurde, die vom vorherigen Befehl **id -u** zurückgegeben wurde:

```
ls /tmp/krb5cc_uid
```

Ein ähnlicher Test kann durch Anmeldung bei KDE oder Gnome Display Manager durchgeführt werden. Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

PBIS

ERFORDERLICHES PBIS-PAKET HERUNTERLADEN

```
sudo wget https://github.com/BeyondTrust/pbis-open/releases/download/
9.1.0/pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

PBIS-INSTALLATIONSSKRIPT AUSFÜHRBAR MACHEN

```
sudo chmod +x pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

PBIS-INSTALLATIONSSKRIPT AUSFÜHREN

```
sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
```

WINDOWS-DOMÄNE BEITRETEN

Ihr Domänencontroller muss erreichbar sein, und Sie müssen über ein Active Directory-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo /opt/pbis/bin/domainjoin-cli join domain-name user
```

Der **Benutzer** ist ein Domänenbenutzer, der über Berechtigungen zum Hinzufügen von Computern zur Active Directory-Domäne verfügt. Der **Domänenname** ist der DNS-Name der Domäne, zum Beispiel example.com.

Hinweis: Um Bash als Standardshell festzulegen, führen Sie den Befehl **sudo /opt/pbis/bin/config LoginShellTemplate/bin/bash** aus.

DOMÄNENMITGLIEDSCHAFT ÜBERPRÜFEN

Der Delivery Controller erfordert, dass alle VDA-Maschinen (Windows- und Linux-VDAs) ein Computerobjekt in `Active Directory` haben. Um zu überprüfen, ob eine PBIS-verbundene Linux-Maschine in der Domäne ist:

```
/opt/pbis/bin/domainjoin-cli query
```

Wenn die Maschine einer Domäne beigetreten ist, gibt dieser Befehl die Informationen über die aktuell beigetretene AD-Domäne und OU zurück. Andernfalls wird nur der Hostname angezeigt.

BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

Um zu überprüfen, ob PBIS Domänenbenutzer über PAM authentifizieren kann, melden Sie sich am Linux VDA mit einem Domänenbenutzerkonto an, das zuvor noch nicht verwendet wurde.

```
sudo ssh localhost -l domain\\user



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die UID erstellt wurde, die vom Befehl **id -u** zurückgegeben wird:

```
ls /tmp/krb5cc_uid
```

Beenden Sie die Sitzung.

```
exit
```

Fahren Sie nach der Überprüfung des Domänenbeitritts mit Schritt 6: Installieren des Linux VDA fort.

Schritt 4: .NET Runtime 6.0 installieren

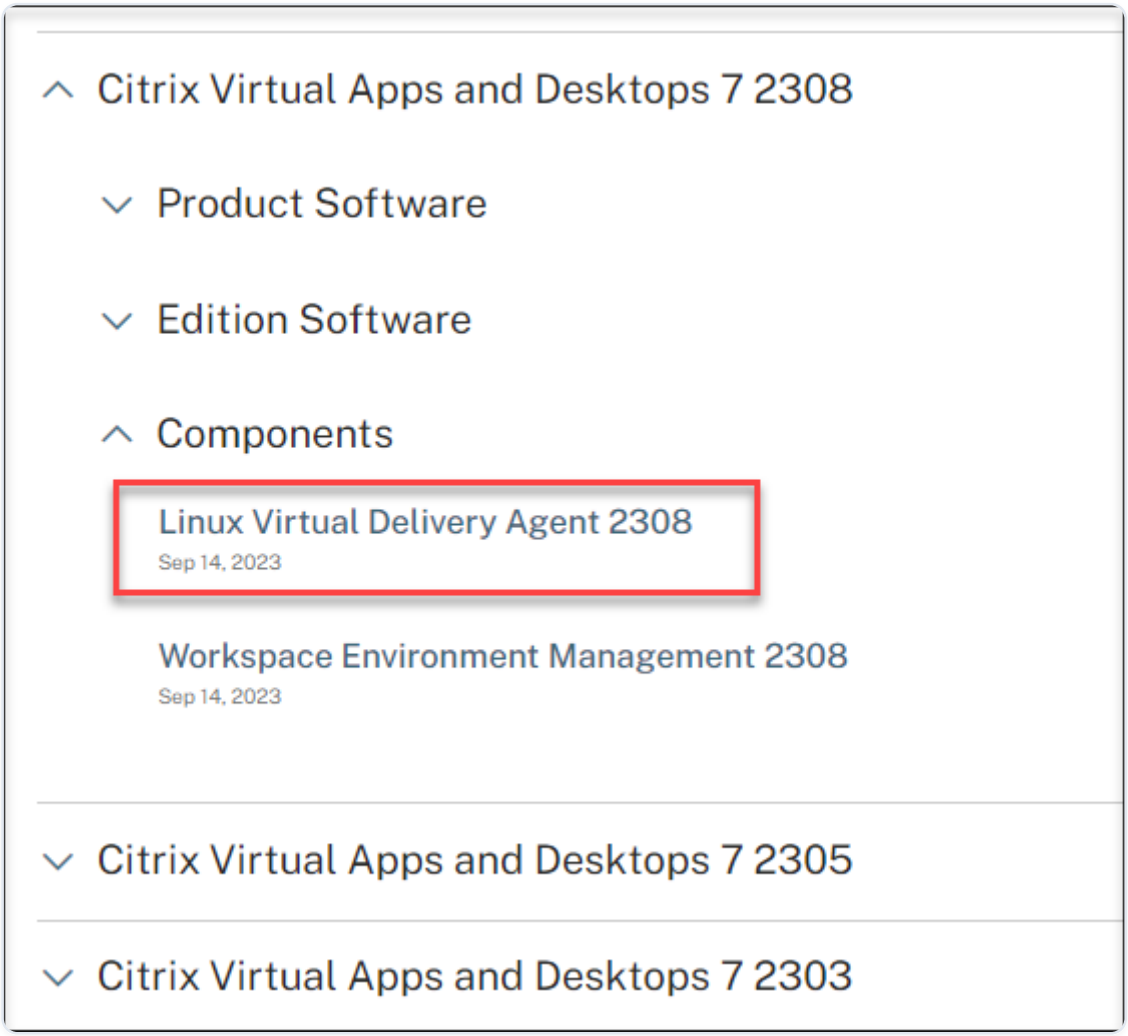
Bevor Sie den Linux VDA installieren, installieren Sie .NET Runtime 6.0 gemäß den Anweisungen unter `<https://docs.microsoft.com/de-de/dotnet/core/install/linux-package-managers>`.

Nach der Installation von .NET Runtime 6.0 führen Sie den Befehl **which dotnet** aus, um Ihren Laufzeitpfad zu finden.

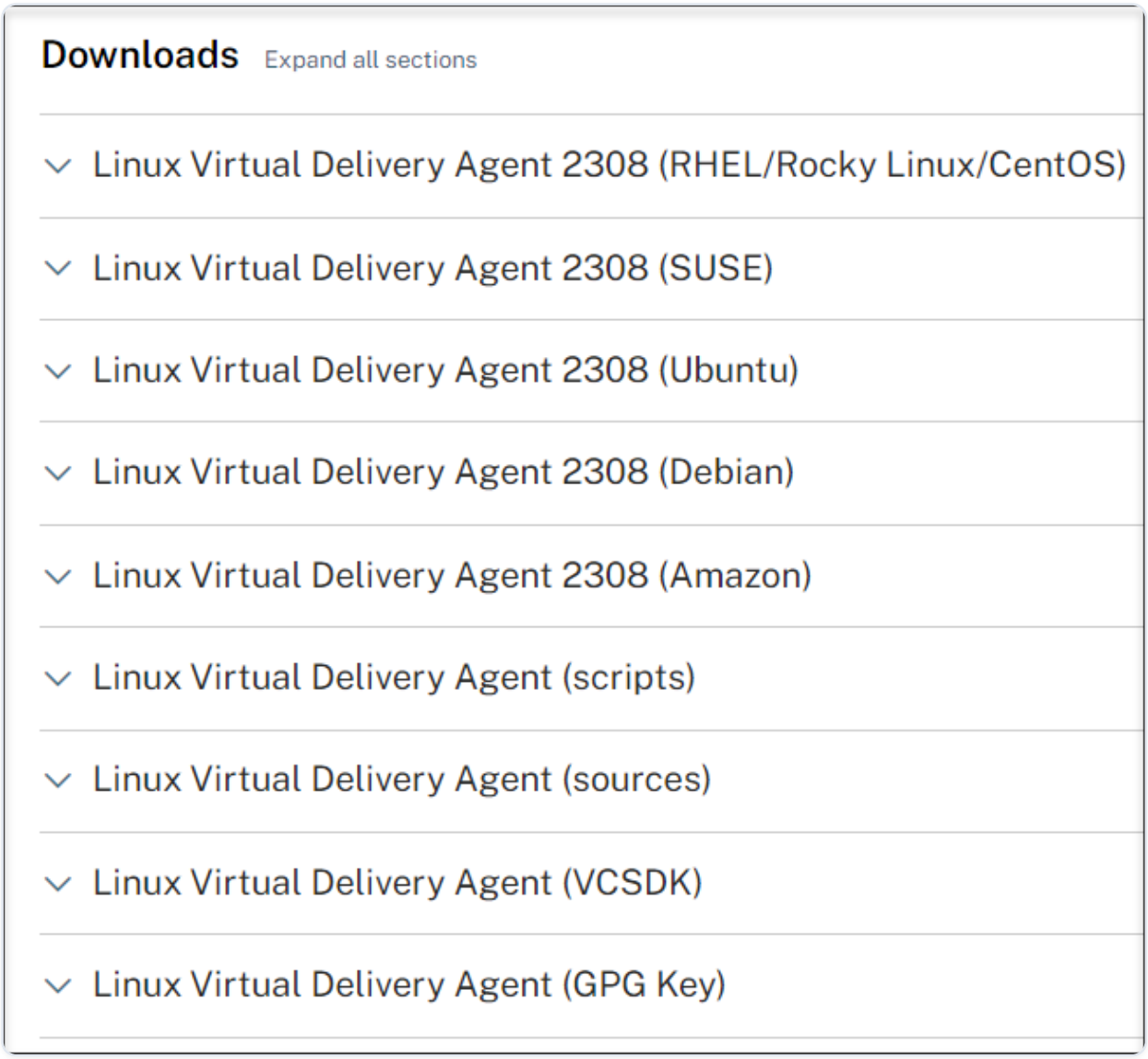
Basierend auf der Befehlsausgabe legen Sie den Binärpfad der .NET-Laufzeitumgebung fest. Wenn die Befehlsausgabe beispielsweise /aa/bb/dotnet lautet, verwenden Sie /aa/bb als .NET-Binärpfad.

Schritt 5: Linux VDA-Paket herunterladen

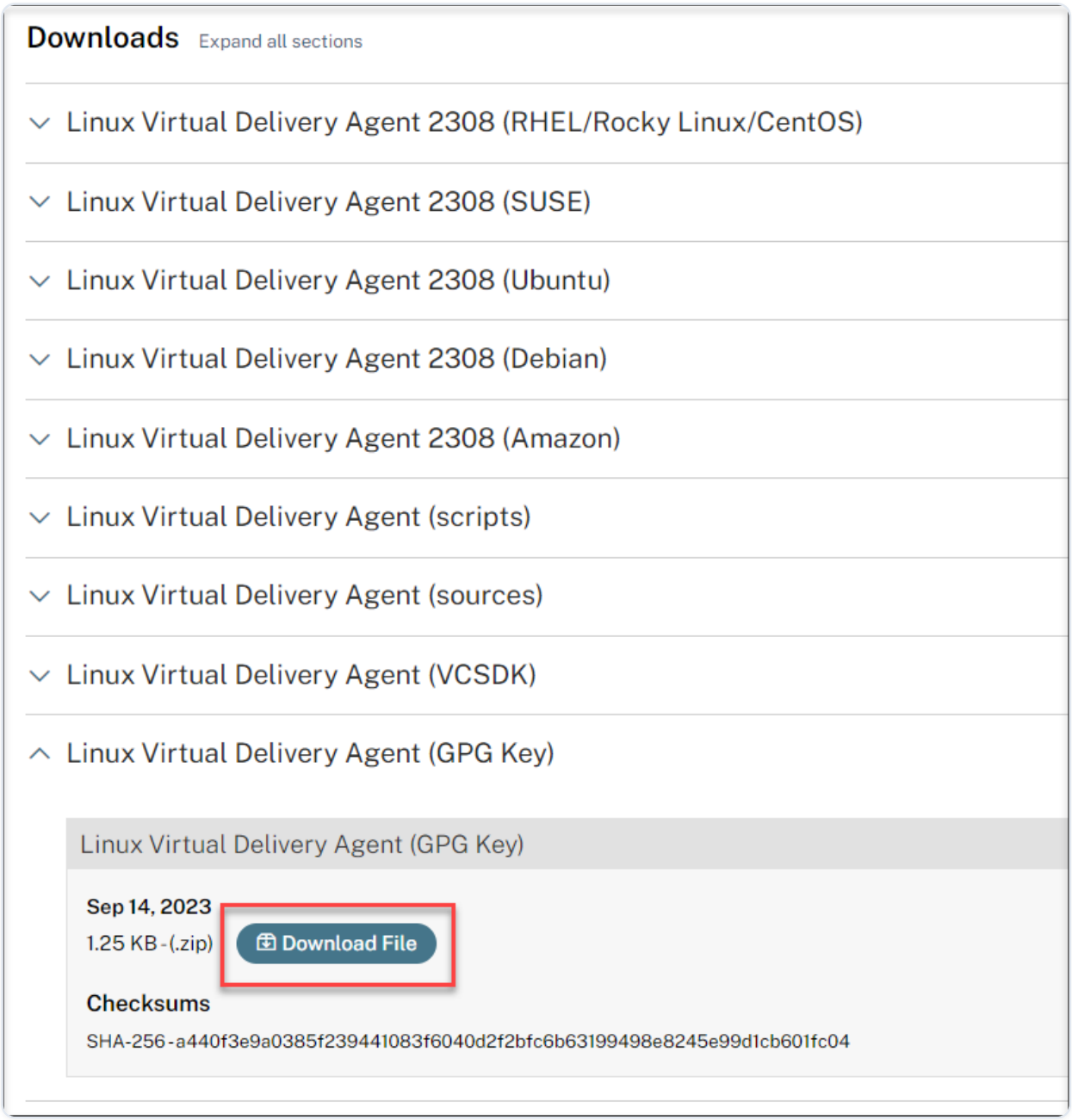
1. Gehen Sie zur Citrix Virtual Apps and Desktops-Downloadseite.
2. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops.
3. erweitern Sie **Components**, um den Linux VDA zu finden. Zum Beispiel:



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. Zum 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 Paketintegrität zu prüfen:

```
sudo apt-get install dpkg-sig

gpg --import <path to the public key>

dpkg-sig --verify <path to the Linux VDA package>
```

Schritt 6: Linux VDA installieren

Schritt 6a: Linux VDA installieren

Installieren Sie die Linux VDA-Software mit dem Debian-Paketmanager:

```
sudo dpkg -i xendesktopvda_<version>.debian10_amd64.deb
```

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
```

Hinweis:

Eine Matrix der Linux-Distributionen und Xorg-Versionen, die diese Version des Linux VDA unterstützt, finden Sie unter Systemanforderungen.

Schritt 6b: Linux VDA aktualisieren (optional)

Sie können eine vorhandene Installation von den beiden vorherigen Versionen und von einer LTSR-Version aktualisieren.

```
sudo dpkg -i <PATH>/<Linux VDA deb>
```

Hinweis:

Beim Aktualisieren einer vorhandenen Installation werden die Konfigurationsdateien unter /etc/xdl überschrieben. Sichern Sie die Dateien, bevor Sie ein Upgrade durchführen.

Schritt 7: NVIDIA GRID-Treiber installieren

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 (des Hosttreibers) auf den jeweiligen Hypervisoren finden Sie in den folgenden Anleitungen:

- Citrix Hypervisor

- VMware ESX
- Nutanix AHV

Führen Sie die folgenden allgemeinen Schritte aus, um die NVIDIA GRID-Gast-VM-Treiber zu installieren und zu konfigurieren:

1. Stellen Sie sicher, dass die Gast-VM heruntergefahren ist.
2. Weisen Sie der VM im Hypervisor-Bedienfeld eine GPU zu.
3. Starten Sie die VM.
4. Installieren Sie den Gast-VM-Treiber auf der VM.

Schritt 8: Linux VDA konfigurieren

> **Hinweis:**
>
> Bevor Sie die Laufzeitumgebung einrichten, stellen Sie sicher, dass das Gebietsschema **en_US.UTF-8** auf Ihrem Betriebssystem installiert ist. Wenn das Gebietsschema auf Ihrem Betriebssystem nicht verfügbar ist, führen Sie den Befehl **sudo locale-gen en_US.UTF-8** aus. Bearbeiten Sie für Debian die Datei **/etc/locale.gen**, indem Sie die Zeile # **en_US.UTF-8 UTF-8** auskommentieren, und führen Sie dann den Befehl **sudo locale-gen** aus.

> Nach der Installation des Pakets müssen Sie den Linux VDA konfigurieren, indem Sie das Skript ctxsetup.sh ausführen. Bevor Änderungen vorgenommen werden, überprüft das Skript die Umgebung und stellt sicher, dass alle Abhängigkeiten installiert sind. Bei Bedarf können Sie das Skript jederzeit erneut ausführen, um Einstellungen zu ändern.

Sie können das Skript manuell mit Abfragen oder automatisch mit vorkonfigurierten Antworten ausführen. Lesen Sie die Hilfe zum Skript, bevor Sie fortfahren:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh --help
```

Konfiguration mit Abfragen

Führen Sie eine manuelle Konfiguration mit Abfragen durch:

```
sudo /opt/Citrix/VDA/sbin/ctxsetup.sh
```

Automatisierte Konfiguration

Für eine automatisierte Installation können die vom Setup-Skript benötigten Optionen über Umgebungsvariablen bereitgestellt werden. Wenn alle erforderlichen Variablen vorhanden sind, fordert das Skript den Benutzer nicht zur Eingabe von Informationen auf, was einen skriptgesteuerten Installationsprozess ermöglicht.

Unterstützte Umgebungsvariablen sind:

- **CTX_XDL_SUPPORT_DDC_AS_CNAME=Y \| N** – Der Linux VDA unterstützt die Angabe eines Delivery Controller-Namens mithilfe eines DNS-CNAME-Eintrags. Standardmäßig auf N festgelegt.
- **CTX_XDL_DDC_LIST='list-ddc-fqdns'** – Der Linux VDA erfordert eine durch Leerzeichen getrennte Liste von Delivery Controller Fully Qualified Domain Names (FQDNs), die für die Registrierung bei einem Delivery Controller verwendet werden sollen. Mindestens ein FQDN oder CNAME-Alias muss angegeben werden.
- **CTX_XDL_VDA_PORT=port-number** – Der Linux VDA kommuniziert mit Delivery Controllern über einen TCP/IP-Port, der standardmäßig Port 80 ist.
- **CTX_XDL_REGISTER_SERVICE=Y \| N** – Die Linux VDA-Dienste werden nach dem Start des Computers gestartet. Standardmäßig auf Y festgelegt.
- **CTX_XDL_ADD_FIREWALL_RULES=Y \| N** – Die Linux VDA-Dienste erfordern, dass eingehende Netzwerkverbindungen über die System-Firewall zugelassen werden. Sie können die erforderlichen Ports (standardmäßig Port 80 und 1494) automatisch in der System-Firewall für den Linux VDA öffnen. Standardmäßig auf Y festgelegt.
- **CTX_XDL_AD_INTEGRATION=winbind \| quest \|centrify \| sssd \| pbis** – Der Linux VDA erfordert Kerberos-Konfigurationseinstellungen zur Authentifizierung bei den Delivery Controllern. Die Kerberos-Konfiguration wird anhand des installierten und konfigurierten Active Directory-Integrationstools auf dem System bestimmt.
- **CTX_XDL_HDX_3D_PRO=Y \| N** – Der Linux VDA unterstützt HDX 3D Pro, eine Reihe von GPU-Beschleunigungstechnologien, die zur Optimierung der Virtualisierung von grafikintensiven Anwendungen entwickelt wurden. Wenn HDX 3D Pro ausgewählt ist, wird der VDA für den VDI-Desktop-Modus (Einzelsitzung) konfiguriert – (d. h. CTX_XDL_VDI_MODE=Y).
- **CTX_XDL_VDI_MODE=Y \| N** – Gibt an, ob die Maschine als dediziertes Desktop-Bereitstellungsmodell (VDI) oder als gehostetes Shared-Desktop-Bereitstellungsmodell konfiguriert werden soll. Für HDX 3D Pro-Umgebungen setzen Sie diese Variable auf Y. Diese Variable ist standardmäßig auf N gesetzt.

- **CTX_XDL_SITE_NAME=dns-name** – Der Linux VDA ermittelt LDAP-Server über DNS. Um die DNS-Suchergebnisse auf einen lokalen Standort zu beschränken, geben Sie einen DNS-Standortnamen an. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_LDAP_LIST='list-ldap-servers'** – Der Linux VDA fragt DNS ab, um LDAP-Server zu ermitteln. Wenn DNS keine LDAP-Dienstdatensätze bereitstellen kann, können Sie eine durch Leerzeichen getrennte Liste von LDAP-FQDNs mit LDAP-Ports angeben. Zum 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. Um schnellere LDAP-Abfragen innerhalb einer Active Directory-Gesamtstruktur zu ermöglichen, aktivieren Sie **Global Catalog** auf einem Domänencontroller und geben Sie die entsprechende LDAP-Portnummer als 3268 oder als 3269 an, wenn Sie LDAPS verwenden. Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_SEARCH_BASE=search-base-set** – Der Linux VDA fragt LDAP über eine Suchbasis ab, die auf das Stammverzeichnis der Active Directory-Domäne gesetzt ist (z. B. DC=mycompany,DC=com). Um die Suchleistung zu verbessern, können Sie jedoch eine Suchbasis angeben (z. B. OU=VDI,DC=mycompany,DC=com). Diese Variable ist standardmäßig auf **\<none\>** gesetzt.
- **CTX_XDL_FAS_LIST='list-fas-servers'** – Die Federated Authentication Service (FAS)-Server werden über die AD-Gruppenrichtlinie konfiguriert. Der Linux VDA unterstützt keine AD-Gruppenrichtlinien, aber Sie können stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Die Reihenfolge muss dieselbe sein wie in der AD-Gruppenrichtlinie konfiguriert. Wenn eine Serveradresse entfernt wird, füllen Sie die Lücke mit der Textzeichenfolge **\<none\>** und ändern Sie nicht die Reihenfolge der Serveradressen. Um ordnungsgemäß mit FAS-Servern zu kommunizieren, stellen Sie sicher, dass Sie eine Portnummer anhängen, die mit der auf den FAS-Servern angegebenen 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 zur Installation der .NET Runtime 6.0 zur Unterstützung des neuen Broker-Agent-Dienstes (`ctxvda`). Der Standardpfad ist /usr/bin.
- **CTX_XDL_DESKTOP _ENVIRONMENT=gnome/gnome-classic/mate** – Gibt die GNOME-, GNOME Classic- oder MATE-Desktopumgebung an, die in Sitzungen verwendet werden soll. Wenn Sie die Variable nicht angeben, wird der aktuell auf dem VDA installierte Desktop verwendet. Wenn der aktuell installierte Desktop jedoch MATE ist, müssen Sie den Variablenwert auf **mate** setzen.

Sie können die Desktopumgebung für einen Ziel-Sitzungsbenutzer auch ändern, indem Sie die folgenden Schritte ausführen:

a. Erstellen Sie eine `.xsession`-Datei im Verzeichnis **$HOME/<username\>** auf dem VDA.

2\. Bearbeiten Sie die `.xsession`-Datei, um eine Desktopumgebung basierend auf den Distributionen anzugeben.

- **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
```

b. Teilen Sie die Dateiberechtigung 700 mit dem Ziel-Sitzungsbenutzer.

Ab Version 2209 können Sitzungsbenutzer ihre Desktopumgebungen anpassen. Um diese Funktion zu aktivieren, müssen Sie im Voraus umschaltbare Desktopumgebungen auf dem VDA installieren. Weitere Informationen finden Sie unter Benutzerdefinierte Desktopumgebungen durch Sitzungsbenutzer.

- **CTX_XDL_START_SERVICE=Y \| N** – Ob die Linux VDA-Dienste gestartet werden, wenn die Linux VDA-Konfiguration abgeschlossen ist. Standardmäßig auf Y gesetzt.
- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Abhören von Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT** – Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

Legen Sie die Umgebungsvariable fest und führen Sie das Konfigurationsskript aus:

```
export CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N



export CTX_XDL_DDC_LIST='list-ddc-fqdns'



export CTX_XDL_VDA_PORT=port-number



export CTX_XDL_REGISTER_SERVICE=Y|N
```

```
export CTX_XDL_ADD_FIREWALL_RULES=Y|N

export CTX_XDL_AD_INTEGRATION=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
```

Wenn Sie den sudo-Befehl ausführen, geben Sie die Option **-E** ein, um die vorhandenen Umgebungsvariablen an die neue Shell zu übergeben, die er erstellt. Wir empfehlen, aus den vorhergehenden Befehlen eine Shell-Skriptdatei mit **#\!/bin/bash** als erster Zeile zu erstellen.

Alternativ können Sie alle Parameter mit einem einzigen Befehl angeben:

```
sudo CTX_XDL_SUPPORT_DDC_AS_CNAME=Y|N \


CTX_XDL_DDC_LIST='list-ddc-fqdns' \


CTX_XDL_VDA_PORT=port-number \


CTX_XDL_REGISTER_SERVICE=Y|N \


CTX_XDL_ADD_FIREWALL_RULES=Y|N \


CTX_XDL_AD_INTEGRATION=winbind | quest |centrify | sssd | pbis \
```

```
CTX_XDL_HDX_3D_PRO=Y|N \

CTX_XDL_VDI_MODE=Y|N \

CTX_XDL_SITE_NAME=dns-name \

CTX_XDL_LDAP_LIST='list-ldap-servers' \

CTX_XDL_SEARCH_BASE=search-base-set \

CTX_XDL_FAS_LIST='list-fas-servers' \

CTX_XDL_DOTNET_RUNTIME_PATH=path-to-install-dotnet-runtime \

CTX_XDL_DESKTOP_ENVIRONMENT=gnome|gnome-classic|mate \

CTX_XDL_TELEMETRY_SOCKET_PORT=port-number \

CTX_XDL_TELEMETRY_PORT=port-number \

CTX_XDL_START_SERVICE=Y|N \
```

```
/opt/Citrix/VDA/sbin/ctxsetup.sh --silent
```

Konfigurationsänderungen entfernen

In einigen Szenarien müssen Sie möglicherweise die durch das Skript **ctxsetup.sh** vorgenommenen Konfigurationsänderungen entfernen, ohne das Linux VDA-Paket zu deinstallieren.

Lesen Sie die Hilfe zu diesem Skript, bevor Sie fortfahren:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh --help
```

So entfernen Sie Konfigurationsänderungen:

```
sudo /opt/Citrix/VDA/sbin/ctxcleanup.sh
```

Wichtig:

Dieses Skript löscht alle Konfigurationsdaten aus der Datenbank und macht den Linux VDA unbrauchbar.

Konfigurationsprotokolle

Die Skripte **ctxsetup.sh** und **ctxcleanup.sh** zeigen Fehler auf der Konsole an, wobei zusätzliche Informationen in die Konfigurationsprotokolldatei **/tmp/xdl.configure.log** geschrieben werden.

Starten Sie die Linux VDA-Dienste neu, damit die Änderungen wirksam werden.

Deinstallieren der Linux VDA-Software

Um zu überprüfen, ob der Linux VDA installiert ist und die Version des installierten Pakets anzuzeigen:

```
dpkg -l xendesktopvda
```

Um detailliertere Informationen anzuzeigen:

```
apt-cache show xendesktopvda
```

Um die Linux VDA-Software zu deinstallieren:

```
dpkg -r xendesktopvda
```

Hinweis:

Durch die Deinstallation der Linux VDA-Software werden die zugehörigen PostgreSQL- und andere Konfigurationsdaten gelöscht. Das PostgreSQL-Paket und andere abhängige Pakete, die vor der Installation des Linux VDA eingerichtet wurden, werden jedoch nicht gelöscht.

Tipp:

Die Informationen in diesem Abschnitt behandeln nicht die Entfernung abhängiger Pakete, einschließlich PostgreSQL.

Schritt 9: XDPing ausführen

`sudo /opt/Citrix/VDA/bin/xdping` ausführen, um häufige Konfigurationsprobleme in einer Linux VDA-Umgebung zu überprüfen. Weitere Informationen finden Sie unter XDPing.

Schritt 10: Den Linux VDA ausführen

Nachdem Sie den Linux VDA mit dem Skript **ctxsetup.sh** konfiguriert haben, verwenden Sie die folgenden Befehle, um den Linux VDA zu steuern.

Linux VDA starten:

So starten Sie die Linux VDA-Dienste:

```
sudo systemctl start ctxhdx



sudo systemctl start ctxvda
```

Linux VDA anhalten:

So halten Sie die Linux VDA-Dienste an:

```
sudo systemctl stop ctxvda



sudo systemctl stop ctxhdx
```

Hinweis:

Bevor Sie die Dienste **ctxvda** und **ctxhdx** anhalten, führen Sie den Befehl **systemctl stop ctxmonitord** aus, um den Überwachungsdienst-Daemon anzuhalten. Andernfalls startet der Überwachungsdienst-Daemon die von Ihnen angehaltenen Dienste neu.

Linux VDA neu starten:

So starten Sie die Linux VDA-Dienste neu:

```
sudo systemctl stop ctxvda



sudo systemctl restart ctxhdx



sudo systemctl restart ctxvda
```

Überprüfen Sie den Linux VDA-Status:

So überprüfen Sie den Ausführungsstatus der Linux VDA-Dienste:

```
sudo systemctl status ctxvda



sudo systemctl status ctxhdx
```

Schritt 11: Maschinenkataloge erstellen

Der Prozess zum Erstellen von Maschinenkatalogen und Hinzufügen von Linux VDA-Maschinen ähnelt dem traditionellen Windows VDA-Ansatz. Eine detailliertere Beschreibung zur Durchführung dieser Aufgaben finden Sie unter Maschinenkataloge erstellen und Maschinenkataloge verwalten.

Beim Erstellen von Maschinenkatalogen, die Linux VDA-Maschinen enthalten, gibt es einige Einschränkungen, die den Prozess von der Erstellung von Maschinenkatalogen für Windows VDA-Maschinen unterscheiden:

- Wählen Sie für das Betriebssystem Folgendes aus:
  - Die Option **Multi-session OS** für ein Bereitstellungsmodell mit gehosteten Shared Desktops.
  - Die Option **Single-session OS** für ein VDI-Bereitstellungsmodell mit dedizierten Desktops.
- Mischen Sie keine Linux- und Windows VDA-Maschinen im selben Maschinenkatalog.

> **Hinweis:**
>
> Frühere Versionen von Citrix Studio unterstützten den Begriff „Linux OS“ nicht. Die Auswahl der Option **Windows Server OS** oder **Server OS** impliziert jedoch ein äquivalentes Bereitstellungsmodell für gehostete Shared Desktops. Die Auswahl der Option **Windows Desktop OS** oder **Desktop OS** impliziert ein Bereitstellungsmodell mit einem Benutzer pro Maschine.

> **Tipp:**
>
> Wenn Sie eine Maschine aus der Active Directory-Domäne entfernen und wieder hinzufügen, müssen Sie die Maschine erneut aus dem Maschinenkatalog entfernen und hinzufügen.

Schritt 12: Bereitstellungsgruppen erstellen

Der Prozess zum Erstellen einer Bereitstellungsgruppe und Hinzufügen von Maschinenkatalogen, die Linux VDA-Maschinen enthalten, ist nahezu identisch mit dem für Windows VDA-Maschinen. Eine detailliertere Beschreibung zur Durchführung dieser Aufgaben finden Sie unter Bereitstellungsgruppen erstellen.

Beim Erstellen von Bereitstellungsgruppen, die Linux VDA-Maschinenkataloge enthalten, gelten die folgenden Einschränkungen:

- Stellen Sie sicher, dass die von Ihnen ausgewählten AD-Benutzer und -Gruppen ordnungsgemäß für die Anmeldung an den Linux VDA-Maschinen konfiguriert wurden.
- Lassen Sie die Anmeldung von nicht authentifizierten (anonymen) Benutzern nicht zu.
- Mischen Sie die Bereitstellungsgruppe nicht mit Maschinenkatalogen, die Windows-Maschinen enthalten.

Informationen zum Erstellen von Maschinenkatalogen und Bereitstellungsgruppen finden Sie unter Citrix Virtual Apps and Desktops 7 2308.

Konfigurieren

Dieser Abschnitt beschreibt die Funktionen des Linux VDA, einschließlich Funktionsbeschreibung, Konfiguration und Fehlerbehebung.

Verwaltung

Dieser Abschnitt enthält die folgenden Themen:

- CEIP
- HDX Insight
- Integration mit dem Citrix Telemetriedienst
- Linux VDA-Selbstaktualisierung für Citrix DaaS Standard für Azure
- Linux-VM- und Linux-Sitzungsmetriken
- Protokollsammlung
- Sitzungsschatten
- Der Monitor-Dienst-Daemon
- Tools und Dienstprogramme
- Sonstiges
    - Unterstützung für Citrix Workspace-App für HTML5
    - Erstellen einer virtuellen **Python3**-Umgebung
    - NIS in Active Directory integrieren
    - **IPv6**
    - LDAPS
    - **Xauthority**

Citrix Programm zur Verbesserung der Kundenerfahrung (CEIP)

Wenn Sie am CEIP teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, um die Qualität und Leistung von Citrix-Produkten zu verbessern. Zusätzlich wird eine

Kopie der anonymen Daten zur schnellen und effizienten Analyse an Google Analytics (GA) gesendet. GA ist standardmäßig deaktiviert.

Registrierungseinstellungen

Standardmäßig nehmen Sie automatisch am CEIP teil, wenn Sie den Linux VDA installieren. Der erste Daten-Upload erfolgt etwa sieben Tage nach der Installation des Linux VDA. Sie können diese Standardeinstellung in der Registrierung ändern.

- **CEIPSwitch**

Registrierungseinstellung, die das CEIP aktiviert oder deaktiviert (Standard = 0):

Location: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Name: **CEIPSwitch**

Wert: 1 = deaktiviert, 0 = aktiviert

Wenn nicht angegeben, ist das CEIP aktiviert.

Sie können den folgenden Befehl auf einem Client ausführen, um das CEIP zu deaktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "CEIPSwitch" -d "1"
```

- **GASwitch**

Registrierungseinstellung, die GA aktiviert oder deaktiviert (Standard = 1):

Location: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Name: **GASwitch**

Wert: 1 = deaktiviert, 0 = aktiviert

Wenn nicht angegeben, ist GA deaktiviert.

Sie können den folgenden Befehl auf einem Client ausführen, um GA zu aktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "GASwitch" -d "0"
```

- **DataPersistPath**

Registrierungseinstellung, die den Datenpersistenzpfad steuert (Standard = /var/xdl/ceip):

Speicherort: HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\CEIP

Name: DataPersistPath

Wert: Zeichenfolge

Sie können den folgenden Befehl ausführen, um diesen Pfad festzulegen:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CEIP" -v "DataPersistPath" -d
"your_path"
```

Wenn der konfigurierte Pfad nicht existiert oder nicht zugänglich ist, werden die Daten im Standardpfad gespeichert.

CEIP-Daten, die vom Linux VDA erfasst werden

Die folgende Tabelle zeigt ein Beispiel für die Arten der gesammelten anonymen Informationen. Die Daten enthalten keine Details, die Sie als Kunden identifizieren.

DATENPUNKT	SCHLÜSSELNAME	BESCHREIBUNG
Maschinen-GUID	**machine_guid**	Eine GUID-Zeichenfolge, die den Computer identifiziert, von dem die Daten stammen
AD-Lösung	**ad_solution**	Eine Zeichenfolge, die die Domänenbeitrittsmethode des Computers angibt
Linux-Kernel-Version	**kernel_version**	Eine Zeichenfolge, die die Kernel-Version des Computers angibt
LVDA-Version	**vda_version**	Eine Zeichenfolge, die die installierte Version des Linux VDA angibt.
LVDA-Update oder Neuinstallation	**update_or_fresh_install**	Eine Zeichenfolge, die angibt, ob das aktuelle Linux VDA-

DATENPUNKT	SCHLÜSSELNAME	BESCHREIBUNG
		Paket neu installiert oder aktualisiert wird
LVDA-Installationsmethode	install_method	Eine Zeichenfolge, die angibt, dass das aktuelle Linux VDA-Paket mittels MCS, PVS, einfacher Installation oder manueller Installation installiert wurde.
HDX™ 3D Pro aktiviert oder nicht	**hdx_3d_pro**	Eine Zeichenfolge, die angibt, ob HDX 3D Pro auf der Maschine aktiviert ist
VDI-Modus aktiviert oder nicht	**vdi_mode**	Eine Zeichenfolge, die angibt, ob der VDI-Modus aktiviert ist
System-Locale	**system_locale**	Eine Zeichenfolge, die das Gebietsschema dieser Maschine angibt
Letzte Neustartzeit der LVDA-Schlüsseldienste	**ctxhdx, ctxvda**	Die letzte Neustartzeit der Dienste `ctxhdx` und `ctxvda` im Format TT-hh:mm:ss, zum Beispiel 10-17:22:19
GPU-Typ	**gpu_type**	Gibt den GPU-Typ der Maschine an
CPU-Kerne	**cpu_cores**	Eine Ganzzahl, die die Anzahl der CPU-Kerne der Maschine angibt
CPU-Frequenz	**cpu_frequency**	Gleitkommazahl, die die CPU-Frequenz in MHz angibt
Physische Speichergröße	**memory_size**	Eine Ganzzahl, die die physische Speichergröße in KB angibt

DATENPUNKT	SCHLÜSSELNAME	BESCHREIBUNG
Anzahl gestarteter Sitzungen	**session_launch**	Eine Ganzzahl, die die Anzahl der gestarteten Sitzungen (angemeldet oder wieder verbunden) auf der Maschine zum Zeitpunkt der Erfassung dieses Datenpunkts angibt
Name und Version des Linux-Betriebssystems	**os_name_version**	Eine Zeichenfolge, die den Namen und die Version des Linux-Betriebssystems des Computers angibt
Sitzungsschlüssel	**session_key**	Identifiziert die Sitzung, aus der die Daten stammen
Ressourcentyp	**resource_type**	Eine Zeichenfolge, die den Ressourcentyp der gestarteten Sitzung angibt: Desktop oder `<appname>`
Aktive Sitzungszeit	**active_session_time**	Wird verwendet, um die aktiven Zeiten der Sitzung zu speichern. Eine Sitzung kann mehrere aktive Zeiten haben, da die Sitzung die Verbindung trennen/ wiederherstellen kann.
Sitzungsdauer	**session_duration_time**	Wird verwendet, um die Dauer der Sitzung von der Anmeldung bis zur Abmeldung zu speichern.
Receiver-Client-Typ	**receiver_type**	Ein Integer, der den Typ der Citrix Workspace™ App angibt, die zum Starten der Sitzung verwendet wurde
Receiver-Client-Version	**receiver_version**	Eine Zeichenfolge, die die Version der Citrix Workspace

DATENPUNKT	SCHLÜSSELNAME	BESCHREIBUNG
		App angibt, die zum Starten der Sitzung verwendet wurde
Druckanzahl	**printing_count**	Ein Integer, der angibt, wie oft die Sitzung die Druckfunktion verwendet
Anzahl der USB-Umleitungen	**usb_redirecting_count**	Ein Integer, der angibt, wie oft die Sitzung ein USB-Gerät verwendet
Gfx-Anbietertyp	**gfx_provider_type**	Eine Zeichenfolge, die den Grafik-Anbietertyp der Sitzung angibt
Shadowing-Anzahl	**shadow_count**	Eine Ganzzahl, die angibt, wie oft die Sitzung überwacht wurde
Vom Benutzer ausgewählte Sprache	**ctxism_select**	Eine zusammengesetzte lange Zeichenfolge, die alle von Benutzern ausgewählten Sprachen enthält
Anzahl der Smartcard-Umleitungen	**scard_redirecting_count**	Eine Ganzzahl, die angibt, wie oft die Smartcard-Umleitung für Sitzungsanmeldungen und die Benutzerauthentifizierung für In-Session-Apps verwendet wird

HDX™ Insight

Übersicht

Der Linux VDA unterstützt die HDX Insight-Funktion teilweise.

Installation

Es müssen keine abhängigen Pakete installiert werden.

Verwendung

HDX Insight analysiert die ICA®-Nachrichten, die über den Citrix ADC zwischen der Citrix Workspace™-App und dem Linux VDA geleitet werden. Alle HDX Insight-Daten stammen aus dem virtuellen NSAP-Kanal und werden unkomprimiert gesendet. Der virtuelle NSAP-Kanal ist standardmäßig aktiviert.

Die folgenden Befehle deaktivieren bzw. aktivieren den virtuellen NSAP-Kanal:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000000" --force
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v "EnableNSAP"
-d "0x00000001" --force
```

Problembehandlung

Es werden keine Datenpunkte angezeigt

Es kann zwei Ursachen geben:

- HDX Insight ist nicht korrekt konfiguriert.

  Zum Beispiel ist AppFlow® auf dem Citrix ADC nicht aktiviert oder eine falsche Citrix ADC-Instanz ist auf dem Citrix ADM konfiguriert.
- Der virtuelle ICA-Steuerungskanal wird auf dem Linux VDA nicht gestartet.

  `ps aux | grep -i ctxctl`

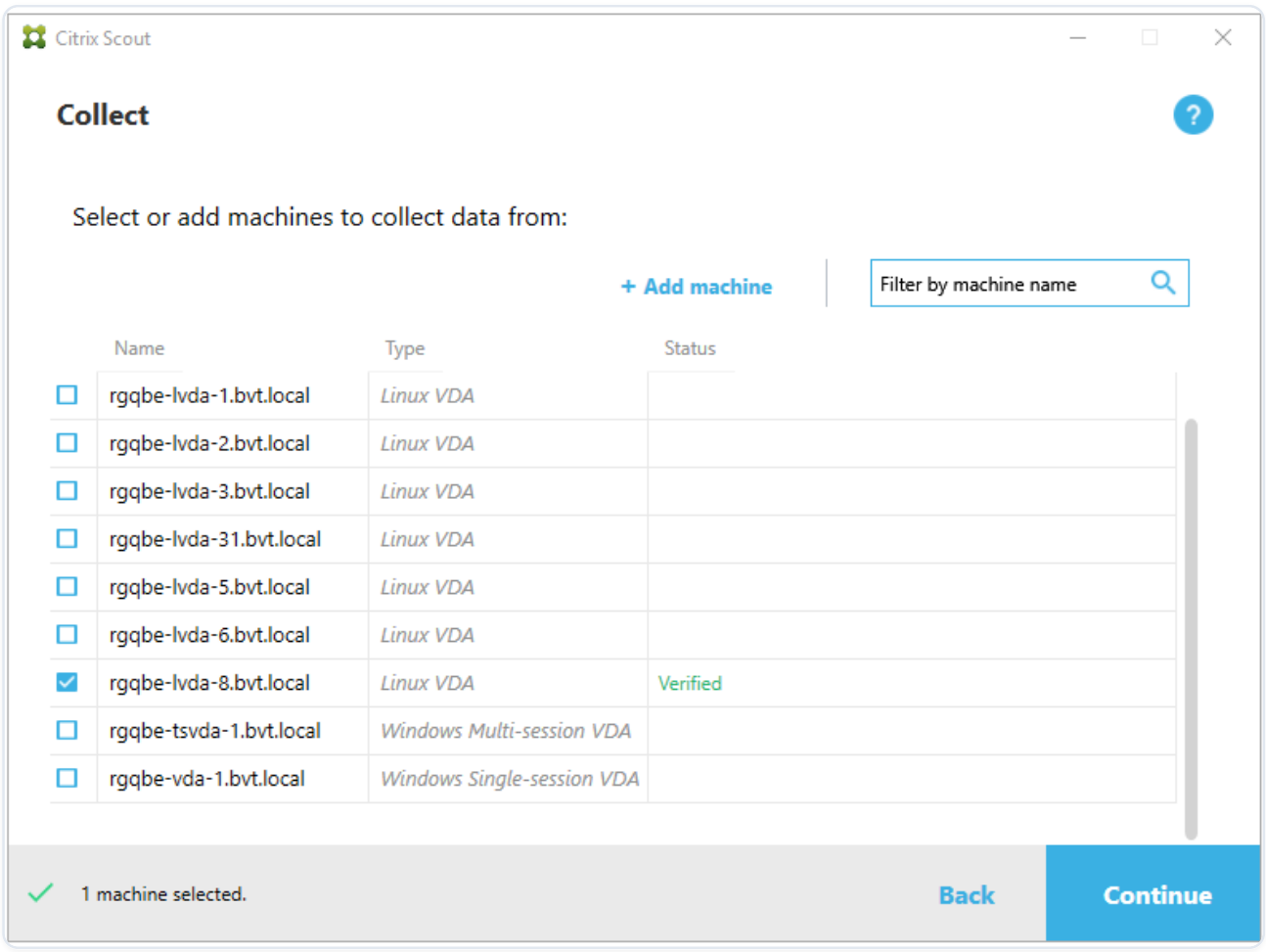
  Wenn `ctxctl` nicht ausgeführt wird, wenden Sie sich an Ihren Administrator, um einen Fehler an Citrix zu melden.

Es werden keine Anwendungsdatenpunkte angezeigt

Stellen Sie sicher, dass der nahtlose virtuelle Kanal aktiviert ist und eine nahtlose Anwendung ausgeführt wird.

Integration mit dem Citrix Telemetriedienst

Da der Citrix Telemetriedienst (`ctxtelemetry`) in die Linux VDA-Software integriert ist, können Sie Citrix Scout ausführen, das dann das Skript /opt/Citrix/VDA/bin/xdlcollect.sh verwendet, um Protokolle über den Linux VDA zu sammeln.



Hinweis:

Nach dem Upgrade von Linux VDA 1912 und früheren Versionen müssen Sie /opt/Citrix/VDA/sbin/ctxsetup.sh erneut ausführen, um die Variablen für den Citrix Telemetriedienst (`ctxtelemetry`) zu konfigurieren. Weitere Informationen zu den Variablen finden Sie unter Easy Install.

Citrix Telemetriedienst aktivieren und deaktivieren

- Um den Dienst zu aktivieren, führen Sie den Befehl **sudo systemctl enable ctxtelemetry.socket** aus.
- Um den Dienst zu deaktivieren, führen Sie **sudo systemctl disable ctxtelemetry.socket** aus.

Ports

Der Citrix Telemetriedienst (`ctxtelemetry`) verwendet standardmäßig den TCP/IP-Port 7503, um auf Citrix Scout zu lauschen. Er verwendet den TCP/IP-Port 7502 auf dem Delivery Controller, um mit Citrix Scout zu kommunizieren.

Sie können die Standardports verwenden oder die Ports über die folgenden Variablen ändern, wenn Sie den Linux VDA installieren.

- **CTX_XDL_TELEMETRY_SOCKET_PORT** – Der Socket-Port zum Lauschen auf Citrix Scout. Der Standardport ist 7503.
- **CTX_XDL_TELEMETRY_PORT** – Der Port für die Kommunikation mit Citrix Scout. Der Standardport ist 7502.

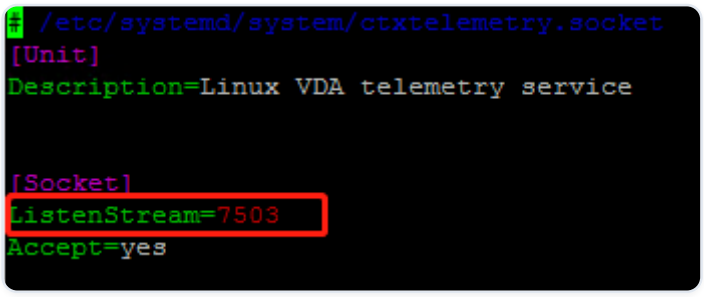
Um die Ports nach der Installation Ihres VDA zu ändern, gehen Sie wie folgt vor:

1. Um einen Port für die Kommunikation mit Scout zu ändern, führen Sie den folgenden Befehl aus.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\Software\Citrix\VirtualDesktopAgent" -v "TelemetryServicePort" -d
   <port number> -t REG_DWORD
   ```

2. Um den Socket-Port zum Lauschen auf Scout zu ändern, führen Sie den folgenden Befehl aus, um die Datei ctxtelemetry.socket zu öffnen und zu bearbeiten.

   ```
   sudo vi /etc/systemd/system/ctxtelemetry.socket
   ```

3. Führen Sie die folgenden Befehle aus, um den Socket-Port neu zu starten.

   ```
   sudo systemctl daemon-reload

   sudo systemctl stop ctxtelemetry.socket
   ```

```
sudo systemctl start ctxtelemetry.socket
```

4. Aktivieren Sie die neuen Ports in Ihrer Firewallkonfiguration.

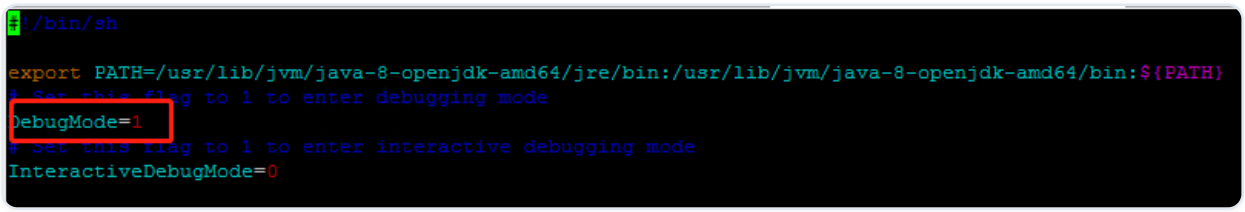
   Wenn Sie beispielsweise Ubuntu verwenden, führen Sie den Befehl **sudo ufw allow 7503** aus, um Port 7503 zu aktivieren.

Debug-Modus

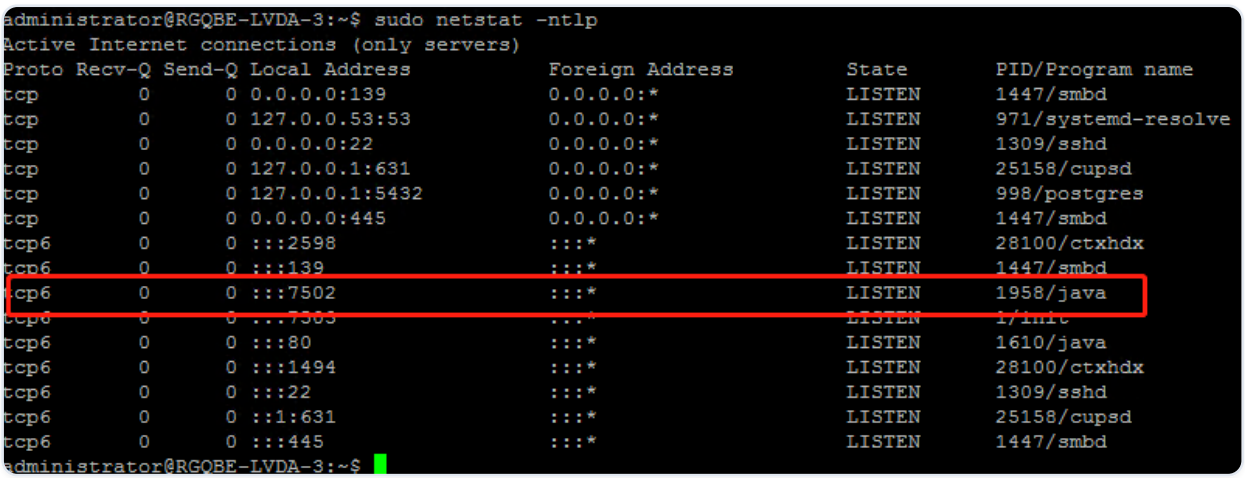
Wenn der Citrix Telemetry Service nicht wie erwartet funktioniert, können Sie den Debug-Modus aktivieren, um die Ursachen zu ermitteln.

1. Um den Debug-Modus zu aktivieren, führen Sie den folgenden Befehl aus, um die Datei `ctxtelemetry` zu öffnen, und ändern Sie dann den Wert von DebugMode in 1.

   ```
   sudo vi /opt/Citrix/VDA/sbin/ctxtelemetry
   ```

2. Stoppen Sie den Citrix Telemetry Service manuell, oder warten Sie 15 Minuten, bis der Dienst automatisch beendet wird.

   In diesem Beispiel können Sie die folgenden Befehle ausführen, um den Citrix Telemetry Service zu beenden.

```
sudo netstat -ntlp

Kill -9 1958
```

3. Um den Citrix Telemetry Service neu zu starten, wählen Sie Ihren Linux VDA in Scout aus und suchen Sie telemetry-debug.log unter /var/log/xdl/.

Dienstwartezeit

Der `systemd`-Daemon, der den Socket-Port öffnet, startet standardmäßig und verbraucht wenige Ressourcen. Der Citrix Telemetry Service wird standardmäßig beendet und startet nur, wenn eine Protokollsammlungsanforderung vom Delivery Controller vorliegt. Nachdem die Protokollsammlung abgeschlossen ist, wartet der Dienst 15 Minuten lang auf neue Sammlungsanforderungen und wird erneut beendet, wenn keine vorhanden sind. Sie können die Wartezeit mit dem folgenden Befehl konfigurieren. Der Mindestwert beträgt 10 Minuten. Wenn Sie einen Wert unter 10 Minuten festlegen, wird der Mindestwert von 10 Minuten wirksam. Nachdem Sie die Wartezeit festgelegt haben, 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
```

Überprüfungstests

Bevor eine Sammlung beginnt, werden für jede ausgewählte Maschine automatisch Überprüfungstests ausgeführt. Diese Tests stellen sicher, dass die Anforderungen erfüllt werden. Wenn ein Test für eine Maschine fehlschlägt, zeigt Scout eine Meldung mit vorgeschlagenen Korrekturmaßnahmen an. Weitere Informationen zu Überprüfungstests finden Sie im Abschnitt Überprüfungstests in der Citrix Scout-Dokumentation.

Linux VDA-Selbstaktualisierung über Azure

Diese Funktion hilft Ihnen, Ihre Linux VDA-Software automatisch zu aktualisieren – sofort oder zu einem geplanten Zeitpunkt. Dies ist von Vorteil, wenn Sie Linux VDAs in Citrix DaaS Standard für Azure (ehemals Citrix Virtual Apps and Desktops Standard für Azure) erstellen. Sie benötigen keine Administratorrechte für die VMs in Azure. Weitere Informationen finden Sie unter Erstellen von Linux VDAs in Citrix DaaS Standard für Azure.

Konfiguration

Um diese Funktion zu verwenden, führen Sie die folgenden Schritte aus:

Schritt 1: Aktualisierungsinformationen und neue VDA-Pakete in Ihren Azure-Container hochladen

Schritt 1a: Erstellen Sie einen Container unter Ihrem Azure-Speicherkonto und legen Sie die Zugriffsebene des Containers auf **Blob (Anonymer Lesezugriff nur für Blobs)** fest.

> **Hinweis:**

> Azure-Container und -Blobs werden ausschließlich von Kunden gehalten und verwaltet. Citrix® haftet nicht für damit verbundene Sicherheitsprobleme. Um Datensicherheit und Kosteneffizienz zu gewährleisten, setzen Sie die Zugriffsebene Ihres Containers nach jedem **Self-Update** auf **Privat (kein anonymer Zugriff)**.

> Schritt 1b: Fügen Sie Ihre VDA-Aktualisierungsinformationen in eine JSON-Datei namens UpdateInfo.json ein. Ein Beispiel für das Dateiformat finden Sie im folgenden Block:

```
{

 "Version": "21.04.200.4",

"Distributions":[

{

"TargetOS": "RHEL7_9",

"PackageName": "",

"PackageHash": ""

},

{

"TargetOS": "UBUNTU20_04",

"PackageName": "",
```

```
"PackageHash": ""

}

]

}
```

Dabei gibt **„Version“** die neue VDA-Version an und **„Distributions“** ist ein Array von Update-Objekten. Jedes Objekt enthält drei Elemente:

- **„TargetOS“**: muss „RHEL7_9“ (für RHEL 7, CentOS 7 und Amazon Linux 2) oder „UBUNTU20_04“ sein. Der **ctxmonitord** erkennt keine anderen Distributionen.
- **„PackageName“**: Vollständiger Name des VDA-Pakets der angegebenen Version.
- **„PackageHash“**: SHA-256-Wert, den Sie mit dem Befehl `shasum -a 256 <pkgname>` berechnen.

Schritt 1c: Laden Sie die JSON-Datei und die neue Version der Linux VDA-Pakete in Ihren Azure-Container hoch.

Schritt 2: Die Selbstaktualisierungsfunktion auf dem Masterimage oder auf jedem VDA aktivieren

Standardmäßig ist das **Self-Update** deaktiviert. Wenn Sie Linux-VDAs in Citrix DaaS Standard für Azure erstellen, muss die Aktivierung der Funktion auf dem Masterimage erfolgen. Andernfalls aktivieren Sie die Funktion direkt auf jedem Ziel-VDA.

Um das **Self-Update** zu aktivieren, führen Sie ähnliche Befehle wie die folgenden aus, um den Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\SelfUpdate zu bearbeiten.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_DWORD"
-v "fEnabled" -d "0x00000001" --force



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"ScheduledTime" -d "Immediately" --force
```

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"Url" -d "<Your-Azure-Container-Url>" --force



/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SelfUpdate" -t "REG_SZ" -v
"CaCertificate" -d "<Local-Certificate-Path-of-PortalAzureCom>" --force
```

Die folgende Tabelle beschreibt die Registrierungseinstellungen.

REGISTRIERUNGSEINSTELLUNG	BESCHREIBUNG
fEnabled	Diese Einstellung ist erforderlich. Standardmäßig ist der Wert 0, was bedeutet, dass die **Selbstaktualisierung** deaktiviert ist. Sie können ihn auf 1 setzen, um die **Selbstaktualisierung** zu aktivieren.
Url	Diese Einstellung ist erforderlich. Sie legt die URL Ihres Azure-Containers fest, um die Update-Informationen und neue VDA-Pakete abzurufen.
ScheduledTime	Diese Einstellung ist erforderlich. Sie können sie auf **Immediately** oder **NextStart** setzen. **Immediately** bedeutet, ein Update sofort nach dem Herunterladen der VDA-Pakete auszuführen. Diese Option ist geeignet, wenn die Download-Geschwindigkeit hoch und Ihr Update dringend ist. Sie kann jedoch die Benutzererfahrung beeinträchtigen, wenn Live-Sitzungen vorhanden sind, während Sie das Paket herunterladen. **NextStart** bedeutet, ein Update beim nächsten Start des **ctxmonitord** auszuführen. Diese Option ist geeignet, wenn die Download-Geschwindigkeit nicht hoch und Ihr Update nicht dringend ist.

REGISTRIERUNGSEINSTELLUNG	BESCHREIBUNG
CaCertificate	Diese Einstellung ist optional. Sie legt den vollständigen Pfad eines PEM-Zertifikats fest, um die URL Ihres Azure-Containers zu überprüfen. Für Azure-Blobs kann es das Zertifikat von portal.azure.com sein, das aus dem Browser abgerufen und dann in PEM konvertiert wird. Aus Sicherheitsgründen empfehlen wir Ihnen, diese Registrierungseinstellung hinzuzufügen, sie wird jedoch nur unter Ubuntu unterstützt. Unter RHEL fehlen einige NSS-Bibliotheken für den `curl`-Befehl. Stellen Sie sicher, dass die geringsten Berechtigungen für das Zertifikat festgelegt sind.

Wenn der **ctxmonitord** neu startet, fragt er zuerst die **Url** ab, um die Datei UpdateInfo.json zu erhalten, und ruft die Update-Version aus der JSON-Datei ab. Anschließend vergleicht der **ctxmonitord** die Update-Version mit der aktuellen Version. Wenn die aktuelle Version älter ist, lädt der Dienst die neue Version des VDA-Pakets von Azure herunter und speichert sie lokal. Danach führt er ein Update gemäß der Einstellung von **ScheduledTime** aus. Für eine lokale Bereitstellung können Sie den **ctxmonitord** direkt neu starten, um das Update auszulösen. In Citrix DaaS Standard für Azure, wo Sie keine Administratorrechte für die VMs haben, kann der **ctxmonitord** jedoch nur nach dem Neustart der VDA-Maschine neu gestartet werden. Wenn ein Update fehlschlägt, wird Ihr VDA auf die vorhandene Version zurückgesetzt.

Hinweis:

- Die Registrierungseinstellungen, die Sie auf dem Master-Image konfiguriert haben, können nicht geändert werden.
- Wenn alle VMs in einer Umgebung gleichzeitig ein Paket herunterladen, kann das lokale Netzwerk überlastet werden.
- Benutzerdaten gehen verloren, wenn sowohl ein Update als auch ein Rollback fehlschlagen.

- Wenn ein Update fehlschlägt, das Rollback jedoch erfolgreich ist, können Benutzer im selben Netzwerk unterschiedliche Versionen des Linux VDA haben. Dieser Fall ist suboptimal.
- Ein Update dauert in der Regel mehrere Minuten. In Citrix Studio gibt es keine Statusanzeige.

Linux-VM- und Linux-Sitzungsmetriken

Die folgende Tabelle listet einige Metriken auf, die für Linux-VMs und Linux-Sitzungen verfügbar sind.

METRIK	MIN. ERFORDERLICHE VDA-VERSION	BESCHREIBUNG	HINWEISE
Anmeldedauer	2109	Sie ist ein Maß für den Anmeldevorgang von dem Zeitpunkt an, zu dem ein Benutzer sich über die Citrix Workspace-App verbindet, bis zu dem Zeitpunkt, an dem eine Sitzung einsatzbereit ist. Um die Metrik einer Sitzung anzuzeigen, wechseln Sie zur Registerkarte Monitor von Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service). Monitor ist als Director-Konsole zum Überwachen und Beheben von Problemen bei Citrix Virtual Apps and Desktops Current	Nur in Monitor verfügbar.

METRIK	MIN. ERFORDERLICHE VDA-VERSION	BESCHREIBUNG	HINWEISE
		Release- und LTSR -Bereitstellungen verfügbar. Auf der Registerkarte Monitor klicken Sie im Abschnitt **Durchschnittliche Anmeldedauer** auf **Historischen Trend anzeigen**. Legen Sie auf der Seite **Anmeldeleistung** Filterbedingungen fest und klicken Sie auf **Anwenden**, um Metriken zu visualisieren.	
Anzahl der automatischen Sitzungswiederverbindungen	2109	Um die Anzahl der automatischen Wiederverbindungen in einer Sitzung anzuzeigen, rufen Sie die Ansicht **Trends** auf. Legen Sie Bedingungen fest und klicken Sie auf **Anwenden**, um die Suchergebnisse einzugrenzen. Die Spalte **Anzahl der automatischen Sitzungswiederverbindungen** zeigt die Anzahl der automatischen Wiederverbindungen in einer Sitzung an.	Sowohl in Citrix Director als auch in Monitor verfügbar.

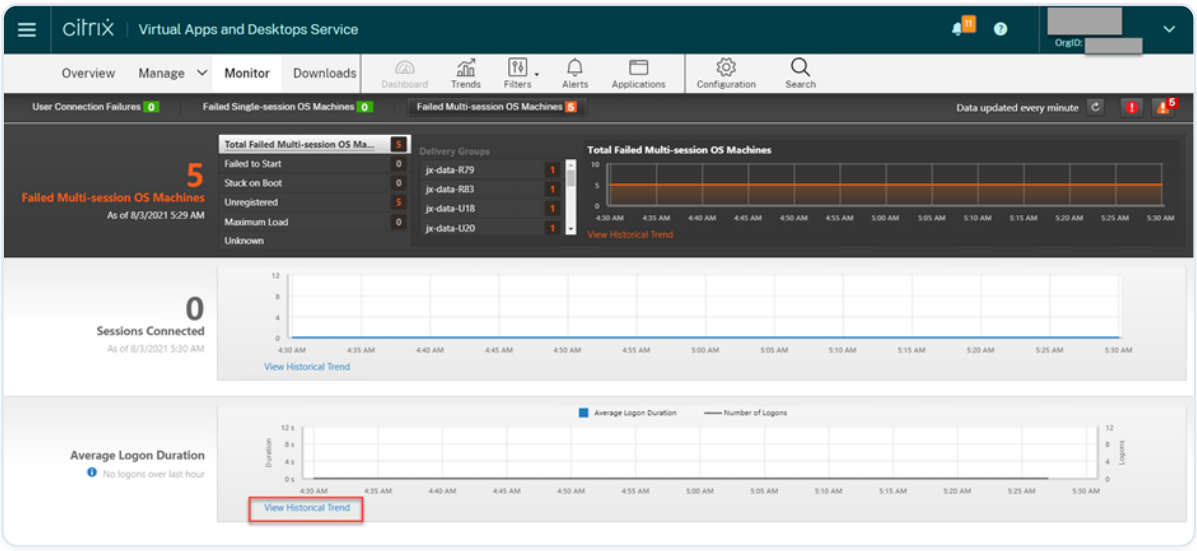
METRIK	MIN. ERFORDERLICHE VDA-VERSION	BESCHREIBUNG	HINWEISE
		Automatische Wiederverbindung ist aktiviert, wenn die Richtlinien **Sitzungszuverlässigkeit** oder **Automatische Client-Wiederverbindung** wirksam sind. Weitere Informationen zu Sitzungswiederverbindungen finden Sie unter Sitzungen. Weitere Informationen zu Richtlinien finden Sie unter Richtlinieneinstellungen für automatische Client-Wiederverbindung und Richtlinieneinstellungen für Sitzungszuverlässigkeit	
Leerlaufzeit	2103	Um auf diese Metrik zuzugreifen, öffnen Sie die Seite **Alle Sitzungen**, indem Sie **Filter > Sitzungen > Alle Sitzungen** auswählen.	Sowohl in Citrix Director als auch in Monitor verfügbar.

METRIK	MIN. ERFORDERLICHE VDA-VERSION	BESCHREIBUNG	HINWEISE
Metriken einer Linux-VM	2103	Die folgenden Metriken für Linux-VMs sind verfügbar: die Anzahl der CPU-Kerne, Speichergröße, Festplattenkapazität sowie die aktuelle und historische CPU- und Speicherauslastung	Sowohl in Citrix Director als auch in Monitor verfügbar.
Protokoll	1909	Das Transportprotokoll einer Linux-Sitzung wird im Bereich **Sitzungsdetails** als UDP oder TCP angezeigt.	Verfügbar sowohl in Citrix Director als auch in Monitor.
ICA® RTT	1903	Die ICA Round Trip Time (RTT) ist die verstrichene Zeit von dem Zeitpunkt, an dem Sie eine Taste drücken, bis die Antwort auf dem Endpunkt angezeigt wird. Um ICA-RTT-Metriken zu erhalten, erstellen Sie die Richtlinien **ICA-Roundtrip-Berechnung** und **ICA-Roundtrip-Berechnungsintervall** in Citrix Studio.	Verfügbar sowohl in Citrix Director als auch in Monitor.

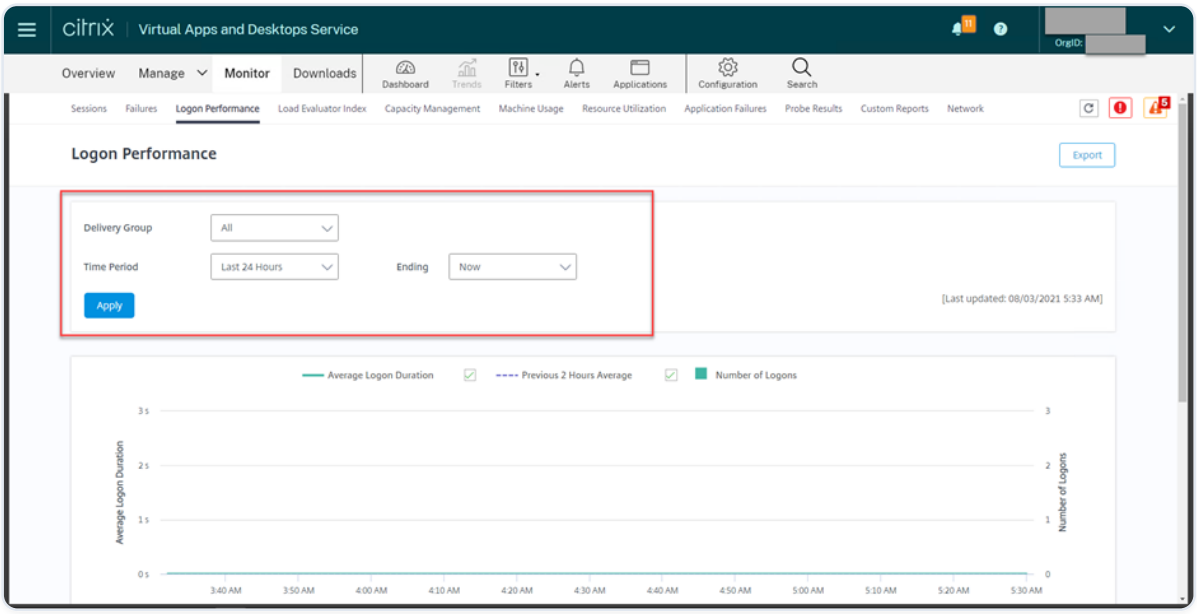
Beispiele für den Zugriff auf die verschiedenen Metriken in Citrix Director und Monitor

- **Anmeldedauer**

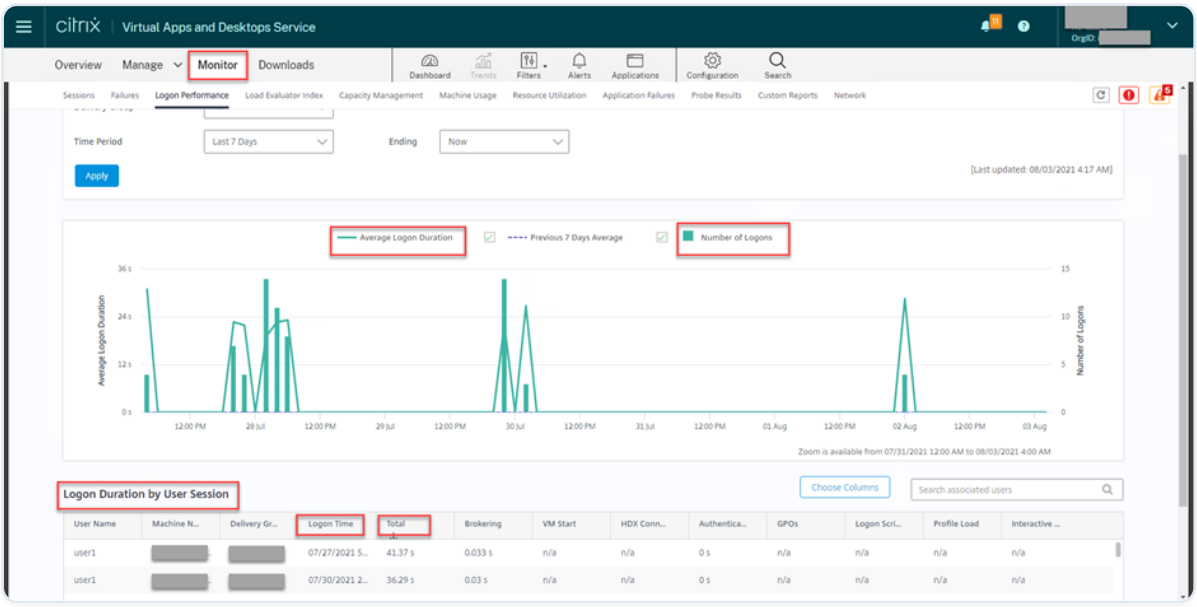
a. Klicken Sie auf der Registerkarte Monitor von Citrix DaaS im Abschnitt **Durchschnittliche Anmeldedauer** auf **Historischen Trend anzeigen**.



b. Legen Sie auf der Seite **Anmeldeleistung** Filterbedingungen fest.

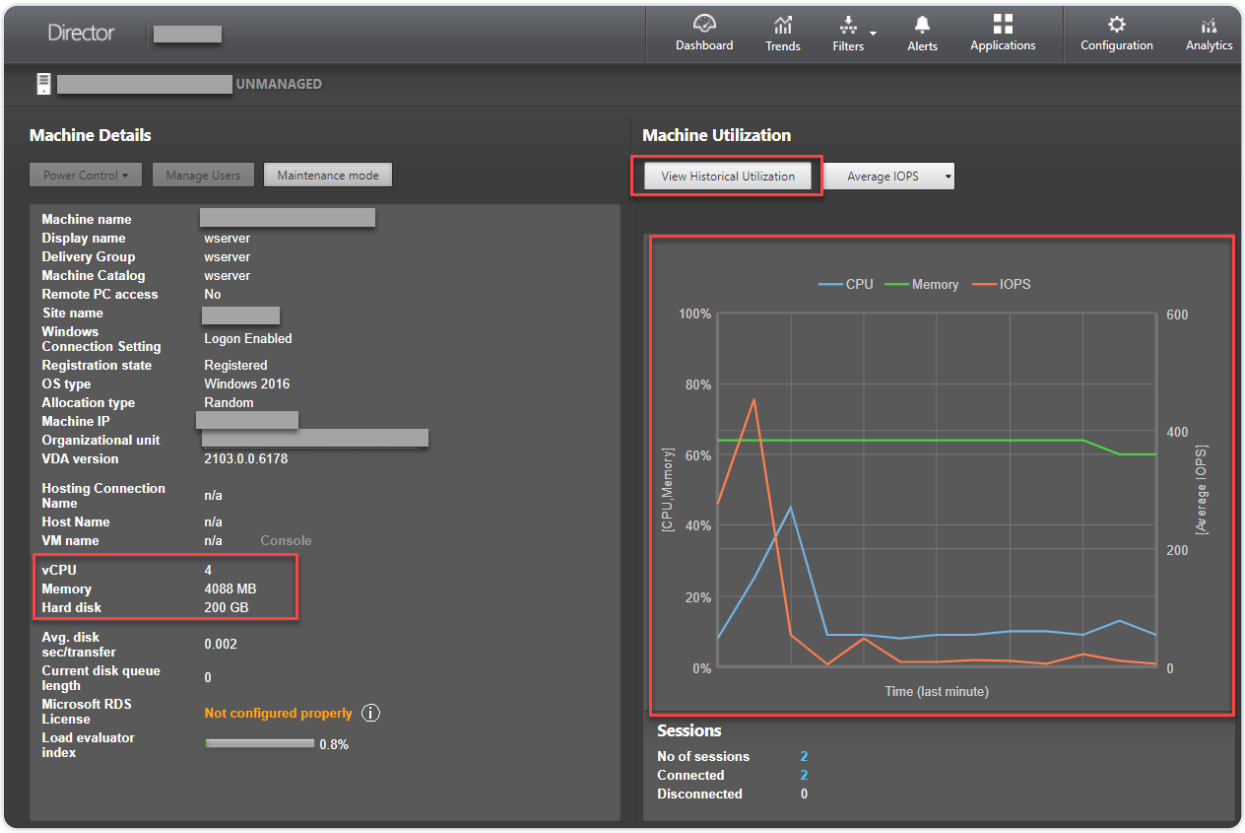


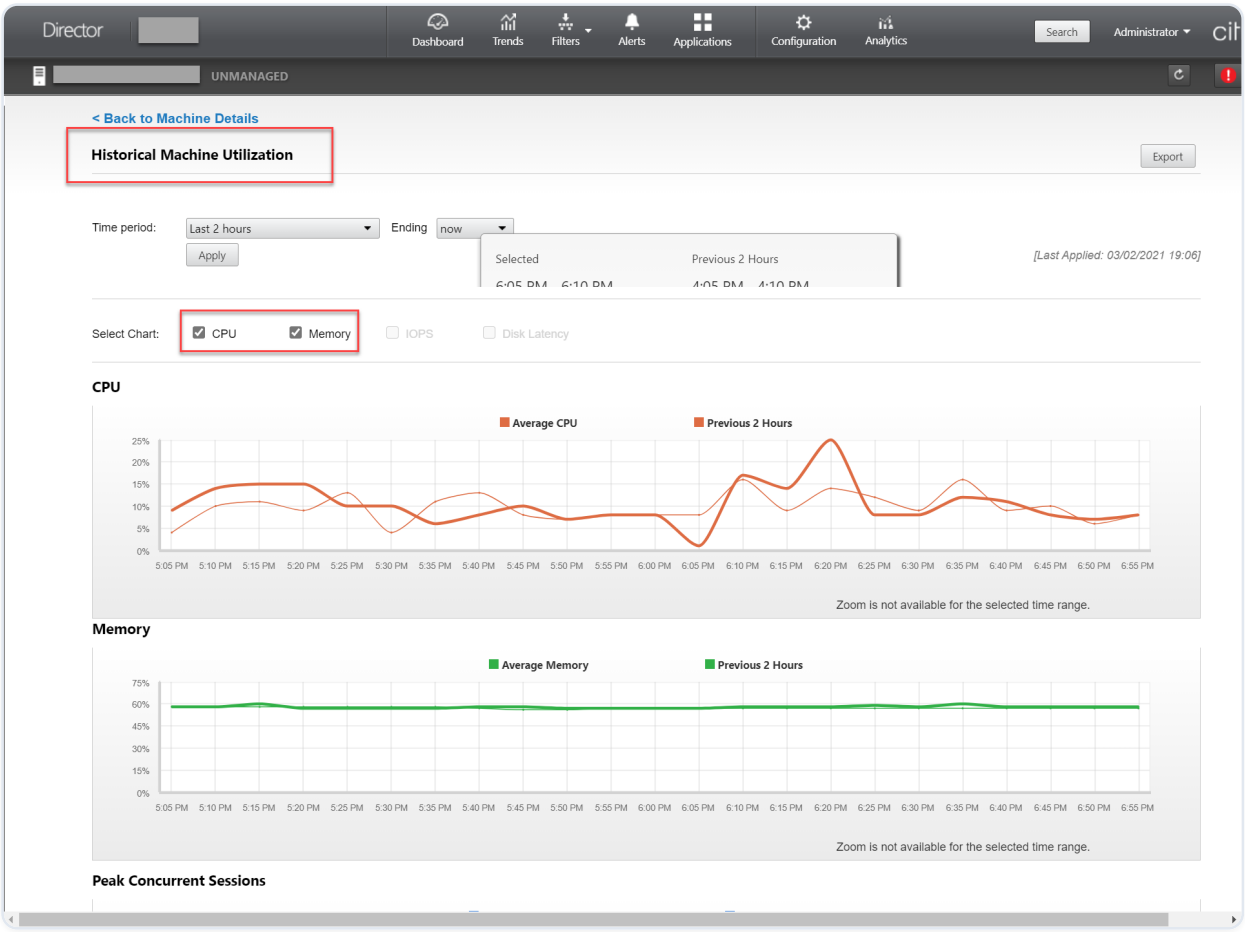
c. Klicken Sie auf **Anwenden**, um die Metriken zur Anmeldedauer zu visualisieren.



- **Die Anzahl der CPU-Kerne, die Speichergröße, die Festplattenkapazität sowie die aktuelle und historische CPU- und Speicherauslastung einer Linux-VM**

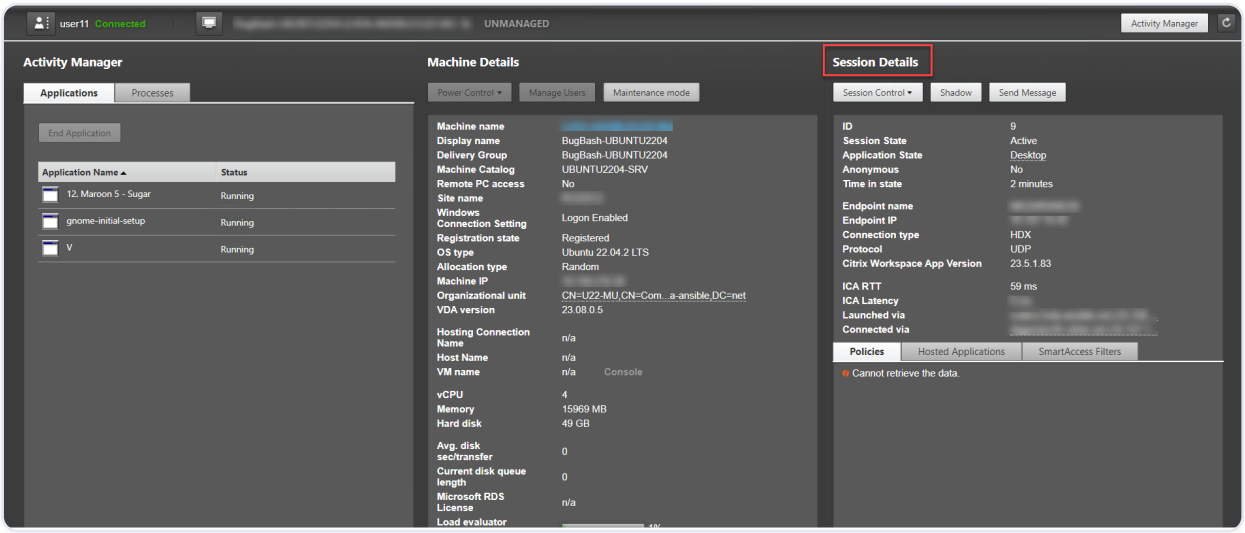
  Um auf diese Metriken einer Linux-VM zuzugreifen, suchen Sie die VM in Citrix Director oder Monitor und überprüfen Sie den Bereich **Maschinendetails**. Zum Beispiel:





- **ICA RTT und Protokoll**

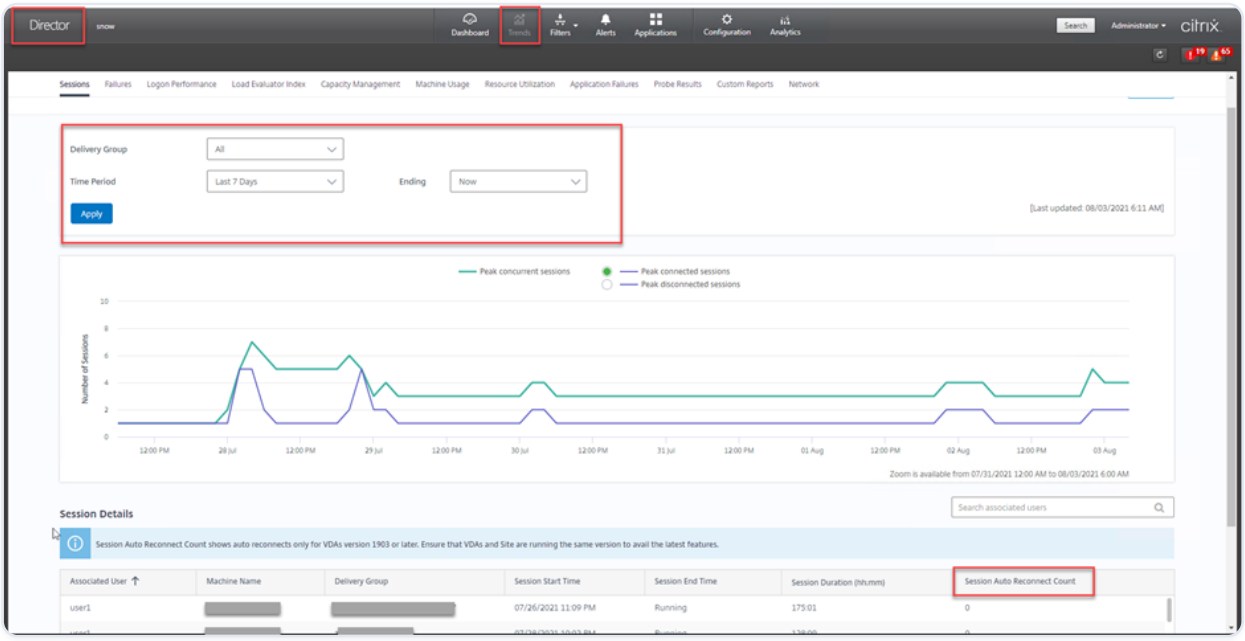
  Um die Metriken einer Linux-Sitzung anzuzeigen, öffnen Sie die Seite **Alle Sitzungen**, indem Sie **Filter > Sitzungen > Alle Sitzungen** auswählen, oder greifen Sie auf das Panel **Sitzungsdetails** zu. Um auf das Panel **Sitzungsdetails** zuzugreifen, öffnen Sie die Seite **Alle Sitzungen** und klicken Sie auf eine Zielsitzung, um deren Ansicht **Aktivitätsmanager** aufzurufen. Beispiel:



- **Anzahl der automatischen Sitzungswiederverbindungen**

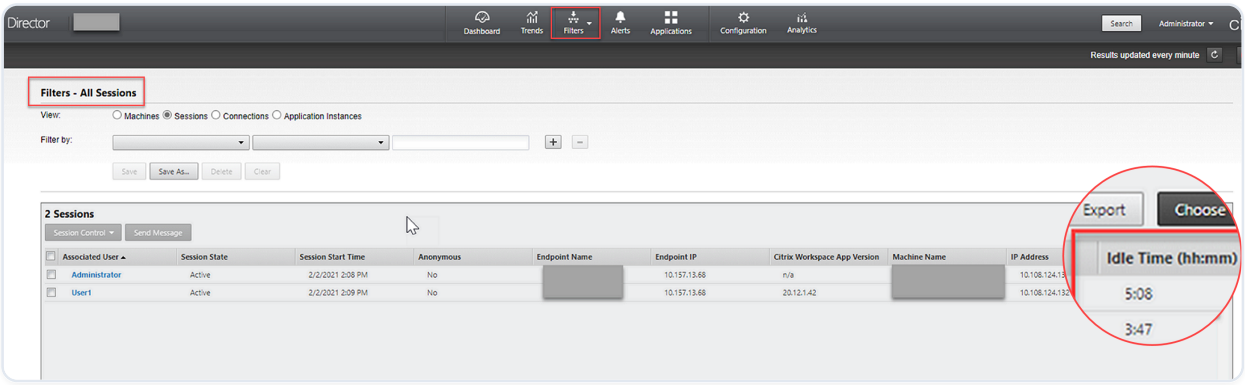
Um die Anzahl der automatischen Wiederverbindungen in einer Sitzung anzuzeigen, rufen Sie die Ansicht **Trends** auf. Legen Sie Bedingungen fest und klicken Sie auf **Anwenden**, um die Suchergebnisse einzugrenzen.

Die Spalte **Anzahl der automatischen Sitzungswiederverbindungen** zeigt die Anzahl der automatischen Wiederverbindungen in einer Sitzung an. Beispiel:



- **Leerlaufzeit**

  Zum Beispiel:



Protokollsammlung

Übersicht

Die Protokollsammlung ist für den Linux VDA standardmäßig aktiviert.

Konfiguration

Der `ctxlogd`-Daemon und das `setlog`-Dienstprogramm sind im Linux VDA-Releasepaket enthalten. Standardmäßig startet der `ctxlogd`-Daemon, nachdem Sie den Linux VDA installiert und konfiguriert haben.

Der Daemon ctxlogd

Alle anderen nachverfolgten Dienste hängen vom `ctxlogd`-Daemon ab. Sie können den `ctxlogd`-Daemon beenden, wenn Sie den Linux VDA nicht nachverfolgen möchten.

Das Dienstprogramm setlog

Die Protokollsammlung wird mit dem Dienstprogramm `setlog` konfiguriert, das sich unter dem Pfad **/opt/Citrix/VDA/bin/** befindet. Nur der Root-Benutzer hat die Berechtigung, es auszuführen. Sie können die GUI verwenden oder Befehle ausführen, um die Konfigurationen anzuzeigen und zu ändern. Führen Sie den folgenden Befehl aus, um Hilfe zum Dienstprogramm `setlog` zu erhalten:

```
setlog help
```

WERTE

Standardmäßig ist **Log Output Path** auf **/var/log/xdl/hdx.log** und **Max Log Size** auf 200 MB festgelegt, und Sie können bis zu zwei alte Protokolldateien unter **Log Output Path** speichern.

Aktuelle `setlog`-Werte anzeigen:

```
setlog values



log_path (Log Output Path) = /var/log/xdl/hdx.log



log_size (Max Log Size (MiB)) = 200



log_count (Max Old Log Files) = 2
```

Einen einzelnen `setlog`-Wert anzeigen oder festlegen:

```
setlog value <name> [<value>]
```

Zum Beispiel:

```
setlog value log_size 100
```

EBENEN

Standardmäßig sind die Protokollebenen auf **warning** (Groß-/Kleinschreibung wird nicht beachtet) eingestellt.

Führen Sie den folgenden Befehl aus, um die für verschiedene Komponenten festgelegten Protokollebenen anzuzeigen:

```
setlog levels
```

Führen Sie den folgenden Befehl aus, um Protokollebenen festzulegen (einschließlich Disabled, Inherited, Verbose, Information, Warnings, Errors und Fatal Errors):

```
setlog level <class> [<level>]
```

PROTOKOLLSTUFE	BEFEHLSPARAMETER (GROSS-/KLEINSCHREIBUNG WIRD NICHT BEACHTET)
Deaktiviert	keine
Geerbt	vererben
Ausführlich	ausführlich
Informationen	Info
Warnungen	Warnung
Fehler	Fehler
Schwerwiegende Fehler	Fatal

Die Variable `<class>` gibt eine Komponente des Linux VDA an. Um alle Komponenten abzudecken, setzen Sie sie auf 'all'. Zum Beispiel:

```
setlog level all error
```

FLAGS

Standardmäßig sind die Flags wie folgt 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
```

Die aktuellen Flags anzeigen:

```
setlog flags
```

Einzelnes Protokoll-Flag anzeigen oder festlegen:

```
setlog flag <flag> [<state>]
```

STANDARDEINSTELLUNGEN WIEDERHERSTELLEN

Alle Ebenen, Flags und Werte auf die Standardeinstellungen zurücksetzen:

```
setlog default
```

Wichtig:

Der `ctxlogd`-Dienst wird über die Datei **/var/xdl/.ctxlog** konfiguriert, die nur Root-Benutzer erstellen können. Andere Benutzer haben keine Schreibberechtigung für diese Datei. Wir empfehlen, dass Root-Benutzer anderen Benutzern keine Schreibberechtigung erteilen. Die Nichteinhaltung kann dazu führen, dass die willkürliche oder bösartige Konfiguration `ctxlogd`, was die Serverleistung und damit die Benutzererfahrung beeinträchtigen kann.

Problembehandlung

Der `ctxlogd`-Daemon schlägt fehl, und Sie können den `ctxlogd`-Dienst nicht neu starten, wenn die Datei **/var/xdl/.ctxlog** fehlt (z. B. versehentlich gelöscht wurde).

/var/log/messages:

```
Apr 1 02:28:21 RH72 citrix-ctxlogd[17881]: Failed to open logging
configuration file.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service: main process exited,
code=exited, status=1/FAILURE



Apr 1 02:28:21 RH72 systemd: Unit ctxlogd.service entered failed state.



Apr 1 02:28:21 RH72 systemd: ctxlogd.service failed.
```

Um dieses Problem zu beheben, führen Sie `setlog` als Root-Benutzer aus, um die Datei **/var/xdl/.ctxlog** neu zu erstellen. Starten Sie dann den `ctxlogd`-Dienst neu, von dem andere Dienste abhängen.

Sitzungsschatten

Das Shadowing von Sitzungen ermöglicht Domänenadministratoren, die ICA®-Sitzungen von Benutzern in einem Intranet anzuzeigen. Die Funktion verwendet noVNC, um eine Verbindung zu den ICA-Sitzungen herzustellen.

> **Hinweis:**

> Um die Funktion zu verwenden, nutzen Sie `Citrix Director` 7.16 oder höher.

Installation und Konfiguration

Abhängigkeiten

Für das Sitzungsschatten sind zwei neue Abhängigkeiten, `python-websockify` und `x11vnc`, erforderlich. Installieren Sie `python-websockify` und `x11vnc` manuell, nachdem Sie den Linux VDA installiert haben.

Für RHEL 7.x und Amazon Linux2:

Führen Sie die folgenden Befehle aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
sudo pip3 install websockify

sudo yum install x11vnc
```

(Für RHEL 7.x) Lösen Sie `python-websockify` und `x11vnc`, indem Sie die Repositorys Extra Packages for Enterprise Linux (EPEL) und optionale RPMs aktivieren:

- EPEL

  Das EPEL-Repository ist für `x11vnc` erforderlich. Führen Sie den folgenden Befehl aus, um das EPEL-Repository zu aktivieren:

  ```
  yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  ```

- Optionale RPMs

  Führen Sie den folgenden Befehl aus, um das optionale `RPMs`-Repository für die Installation einiger Abhängigkeitspakete von `x11vnc` zu aktivieren:

  ```
  subscription-manager repos --enable rhel-7-server-optional-rpms --enable rhel-7-server-extras-rpms
  ```

Für RHEL 9.2/9.0/8.x und Rocky Linux 9.2/9.0/8.x:

Führen Sie die folgenden Befehle aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren.

```
sudo pip3 install websockify

sudo yum install x11vnc
```

Lösen Sie `x11vnc`, indem Sie die Repositorys EPEL und CodeReady Linux Builder aktivieren:

```
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"
```

Für Ubuntu:

Führen Sie die folgenden 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
```

Für SUSE:

Führen Sie die folgenden Befehle aus, um `python-websockify` und `x11vnc` (`x11vnc` Version 0.9.13 oder höher) zu installieren:

```
sudo pip3 install websockify

sudo zypper install x11vnc
```

Für Debian:

Führen Sie die folgenden 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
```

Port

Die Sitzungsschattenfunktion wählt automatisch verfügbare Ports im Bereich von 6001-6099 aus, um Verbindungen vom Linux VDA zu `Citrix Director` aufzubauen. Daher ist die Anzahl der ICA-Sitzungen, die Sie gleichzeitig schatten können, auf 99 begrenzt. Stellen Sie sicher, dass genügend Ports verfügbar sind, um Ihre Anforderungen zu erfüllen, insbesondere für das Schatten von mehreren Sitzungen.

Registrierung

Die folgende Tabelle listet die zugehörigen Registrierungseinträge auf:

REGISTRIERUNG	BESCHREIBUNG	STANDARDWERT
EnableSessionShadowing	Aktiviert oder deaktiviert die Sitzungsschattenfunktion	1 (Aktiviert)
ShadowingUseSSL	Legt fest, ob die Verbindung zwischen dem Linux VDA und Citrix Director verschlüsselt werden soll	0 (Deaktiviert)

Führen Sie den Befehl `ctxreg` auf dem Linux VDA aus, um die Registrierungswerte zu ändern. Um beispielsweise die Sitzungsschattenfunktion zu deaktivieren, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v "EnableSessionShadowing" -d
"0x00000000"
```

SSL

Die noVNC-Verbindung zwischen dem Linux VDA und Citrix Director verwendet das WebSocket-Protokoll. Für das Session Shadowing hängt die Wahl zwischen `ws://` und `wss://` von dem zuvor erwähnten Registrierungsschlüssel „ShadowingUseSSL“ ab. Standardmäßig wird `ws://` gewählt. Aus Sicherheitsgründen empfehlen wir jedoch die Verwendung von `wss://` und die Installation von Zertifikaten auf jedem Citrix Director-Client und auf jedem Linux VDA-Server. Citrix

lehnt jede Sicherheitsverantwortung für das Linux VDA-Session Shadowing unter Verwendung von `ws://` ab.

Um SSL zu aktivieren, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v "ShadowingUseSSL" -d
"0x00000001"
```

SERVER- UND ROOT-SSL-ZERTIFIKATE ABRUFEN

Zertifikate müssen von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert sein.

Für jeden Linux VDA-Server, auf dem Sie SSL konfigurieren möchten, ist ein separates Serverzertifikat (einschließlich des Schlüssels) erforderlich. Ein Serverzertifikat identifiziert einen bestimmten Computer, daher müssen Sie den vollqualifizierten Domänennamen (FQDN) jedes Servers kennen. Erwägen Sie der Einfachheit halber die Verwendung eines Wildcard-Zertifikats für die gesamte Domäne.

Ein Root-Zertifikat ist auch für jeden Citrix Director-Client erforderlich, der mit dem Linux VDA kommuniziert. Root-Zertifikate sind von denselben Zertifizierungsstellen erhältlich, die auch die Serverzertifikate ausstellen.

Sie können Server- und Clientzertifikate von den folgenden Zertifizierungsstellen installieren:

- Eine CA, die mit Ihrem Betriebssystem gebündelt ist
- Eine Unternehmens-CA (eine CA, die Ihre Organisation Ihnen zugänglich macht)
- Eine CA, die nicht mit Ihrem Betriebssystem gebündelt ist

Wenden Sie sich an das Sicherheitsteam Ihrer Organisation, um herauszufinden, welche Methoden sie für den Bezug von Zertifikaten vorschreiben.

Wichtig:

- Der Common Name für ein Serverzertifikat muss der exakte FQDN des Linux VDA oder zumindest der korrekte Wildcard plus Domänenzeichen sein. Zum Beispiel vda1.basedomain.com oder *.basedomain.com.
- Hashing-Algorithmen wie SHA1 und MD5 sind für Signaturen in digitalen Zertifikaten zu schwach, um von einigen Browsern unterstützt zu werden. Daher ist SHA-256 als Mindeststandard festgelegt.

- Chrome akzeptiert keine selbstsignierten SSL-Zertifikate mehr, da diese als unsicher gelten. Der `NET::ERR_CERT_COMMON_NAME_INVALID` Fehler tritt auf, weil dem generierten Zertifikat das SAN-Feld (subjectAltName) fehlt. Um dieses Problem zu beheben, stellen Sie ein Zertifikat mit erweiterten Attributen (X509 v3-Erweiterungen) bereit, das das SAN-Feld enthält.

INSTALLIEREN SIE EIN STAMMZERTIFIKAT AUF JEDEM CITRIX DIRECTOR-CLIENT

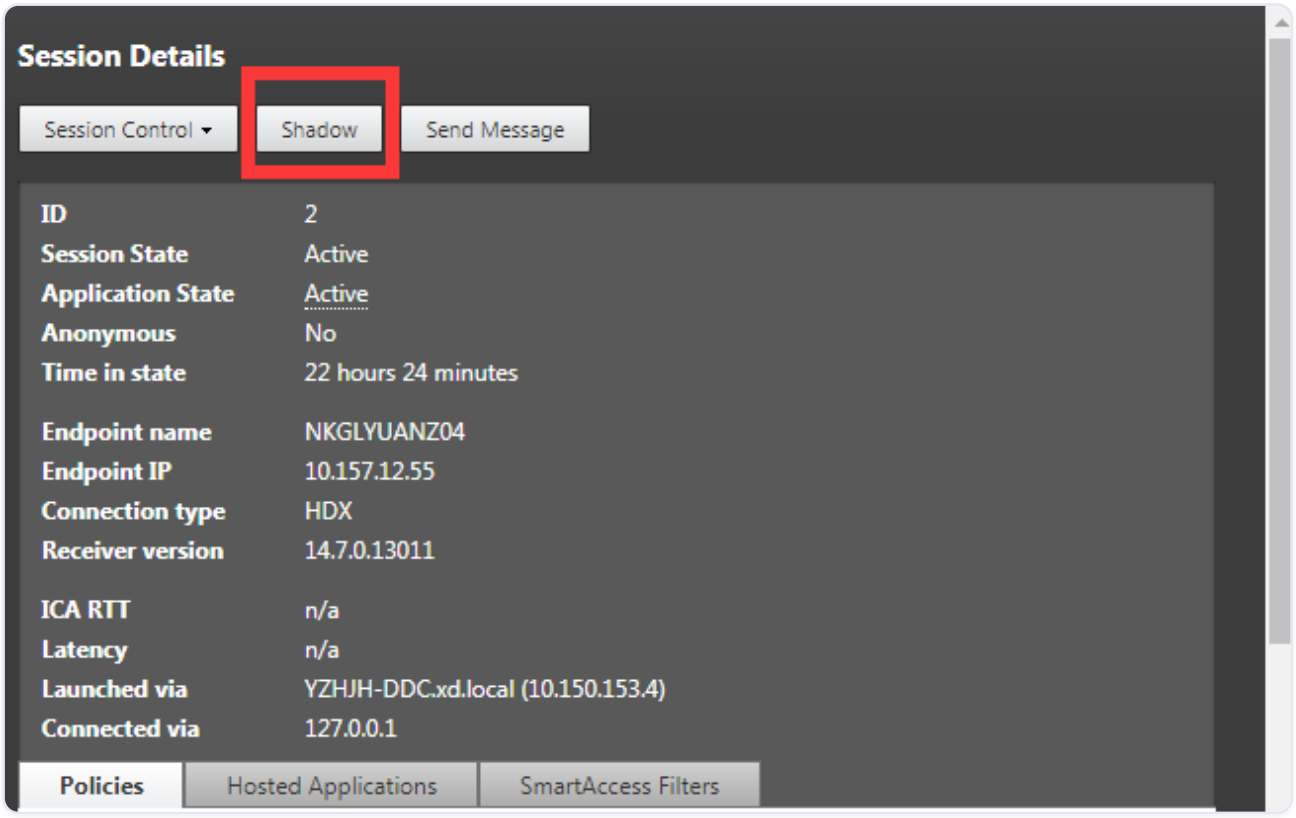
Die Sitzungsschattenfunktion verwendet denselben registrierungsbasierten Zertifikatspeicher wie IIS. Sie können Stammzertifikate daher mit IIS oder dem MMC-Snap-In (Microsoft Management Console) „Zertifikate“ installieren. Wenn Sie ein Zertifikat von einer Zertifizierungsstelle erhalten, können Sie den Webserver-Zertifikat-Assistenten in IIS neu starten, und der Assistent installiert das Zertifikat. Alternativ können Sie Zertifikate auf dem Computer mit der MMC anzeigen und importieren und das Zertifikat als eigenständiges Snap-In hinzufügen. Internet Explorer und Google Chrome importieren die auf Ihrem Betriebssystem installierten Zertifikate standardmäßig. Für Mozilla Firefox müssen Sie Ihre SSL-Stammzertifikate auf der Registerkarte **Zertifizierungsstellen** des Zertifikat-Managers importieren.

INSTALLIEREN SIE EIN SERVERZERTIFIKAT UND DESSEN SCHLÜSSEL AUF JEDEM LINUX VDA-SERVER

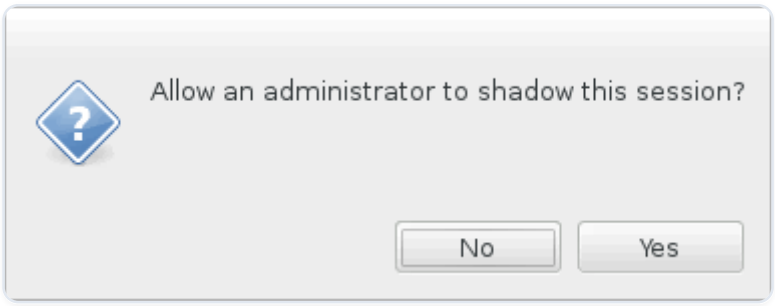
Benennen Sie die Serverzertifikate „shadowingcert.*“ und die Schlüsseldatei „shadowingkey.*“ (* gibt das Format an, z. B. shadowingcert.pem und shadowingkey.key). Legen Sie Serverzertifikate und Schlüsseldateien unter dem Pfad **/etc/xdl/shadowingssl** ab und schützen Sie sie ordnungsgemäß mit eingeschränkten Berechtigungen. Ein falscher Name oder Pfad führt dazu, dass der Linux VDA ein bestimmtes Zertifikat oder eine Schlüsseldatei nicht finden kann und somit eine Verbindungsfehler mit `Citrix Director` verursacht.

Verwendung

Suchen Sie unter `Citrix Director` die Zielsession und klicken Sie in der Ansicht **Sitzungsdetails** auf **Schatten**, um eine Shadowing-Anfrage an den Linux VDA zu senden.



Nachdem die Verbindung initialisiert wurde, erscheint eine Bestätigung auf dem ICA-Sitzungsclient (nicht dem `Citrix Director`-Client), um den Benutzer um Erlaubnis zum Shadowing der Sitzung zu bitten.



Wenn der Benutzer auf **Ja** klickt, erscheint auf der `Citrix Director`-Seite ein Fenster, das anzeigt, dass die ICA-Sitzung geschattet wird.

Weitere Informationen zur Verwendung finden Sie in der Citrix Director-Dokumentation.

Einschränkungen

- Sitzungsschatten ist nur für die Verwendung in einem Intranet konzipiert. Es funktioniert nicht für externe Netzwerke, selbst wenn die Verbindung über Citrix Gateway erfolgt. Citrix lehnt jede Verantwortung für das Linux VDA-Sitzungsschatten in einem externen Netzwerk ab.
- Wenn das Sitzungsschatten aktiviert ist, kann ein Domänenadministrator die ICA-Sitzungen nur anzeigen, hat aber keine Berechtigung, sie zu schreiben oder zu steuern.

- Nachdem ein Administrator unter `Citrix Director` auf **Schatten** geklickt hat, erscheint eine Bestätigung, die den Benutzer um Erlaubnis zum Shadowing der Sitzung bittet. Eine Sitzung kann nur geschattet werden, wenn der Sitzungsbenutzer die Erlaubnis erteilt.
- Die zuvor erwähnte Bestätigung hat eine Zeitüberschreitung von 20 Sekunden. Eine Shadowing-Anfrage schlägt fehl, wenn die Zeit abläuft.
- Eine Sitzung kann nur von einem Administrator überwacht werden. Wenn beispielsweise Administrator B eine Überwachungsanfrage für eine Sitzung sendet, die Administrator A überwacht, wird die Bestätigung zur Einholung der Benutzerberechtigung auf dem Benutzergerät erneut angezeigt. Wenn der Benutzer zustimmt, wird die Überwachungsverbindung für Administrator A beendet und eine neue Überwachungsverbindung für Administrator B aufgebaut. Wenn ein Administrator eine weitere Überwachungsanfrage für dieselbe Sitzung sendet, kann ebenfalls eine neue Überwachungsverbindung aufgebaut werden.
- Um die Sitzungsüberwachung zu verwenden, installieren Sie `Citrix Director` 7.16 oder höher.
- Ein `Citrix Director` Client verwendet einen FQDN anstelle einer IP-Adresse, um eine Verbindung zum Ziel-Linux-VDA-Server herzustellen. Daher muss der `Citrix Director` Client den FQDN des Linux-VDA-Servers auflösen können.

Problembehandlung

Wenn die Sitzungsüberwachung fehlschlägt, führen Sie das Debugging sowohl auf dem `Citrix Director` Client als auch auf dem Linux-VDA durch.

Auf dem Citrix Director Client

Über die Entwicklertools des Browsers überprüfen Sie die Ausgabeprotokolle auf der Registerkarte **Konsole**. Oder überprüfen Sie die Antwort der ShadowLinuxSession API auf der Registerkarte **Netzwerk**. Wenn die Bestätigung zur Einholung der Benutzerberechtigung angezeigt wird, der Verbindungsaufbau jedoch fehlschlägt, pingen Sie den FQDN des VDA manuell an, um zu überprüfen, ob `Citrix Director` den FQDN auflösen kann. Wenn es ein Problem mit der `wss://` Verbindung gibt, überprüfen Sie Ihre Zertifikate.

Auf dem Linux-VDA

1. Überprüfen Sie die Datei `/var/log/xdl/vda.log` auf Hinweise.
2. Bearbeiten Sie die Datei `/var/xdl/sessionshadowing.sh` und ändern Sie die Variable 'logFile', um eine Protokolldatei anzugeben, die während der Sitzungsüberwachung vom Director aus auf Hinweise überwacht werden kann.

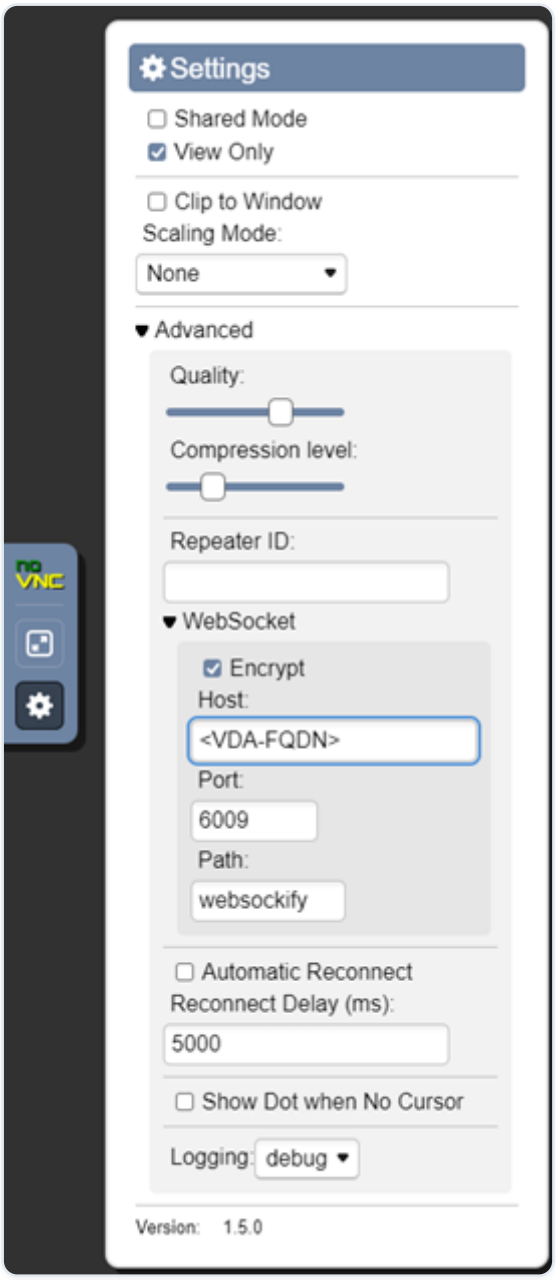
3. Sie können auch manuell überprüfen, ob Ihre Zertifikate mit der noVNC-Verbindung korrekt funktionieren:

   a. Führen Sie **ps aux \| grep xorg** aus, um die Xorg-Anzeigenummer `<display-num>` der aktuellen Sitzung zu finden, zum Beispiel `:3`.

   b. Führen Sie den folgenden Befehl aus, um einen x11vnc-Server zu starten und auf eine eingehende Verbindung zu warten.

   ```
   runuser -l "ctxsrvr" -s /bin/bash -c "websockify <port> -v --cert  /
   etc/xdl/shadowingssl/shadowingcert.pem --key  /etc/xdl/shadowingssl/
   shadowingkey.key -- x11vnc  -viewonly  -shared -passwd <passwd>
   -rfbport <port> -display <display-num> -many -o /var/log/xdl/
   x11vnc.log"
   ```

   c. Versuchen Sie, über noVNC eine Verbindung herzustellen, um den SSL-Modus wie folgt zu überprüfen. Geben Sie den FQDN Ihres VDA und die Portnummer ein. In diesem Beispiel ist die Portnummer 6009.



d. Beheben Sie alle Fehler, die von Websockify auf dem VDA ausgegeben oder vom Browser auf dem Client gemeldet werden.

   Wichtige Prüfpunkte während des Verbindungsaufbaus:

   i. Prüfen Sie auf Firewall-Einschränkungen, die die Sitzungsschattenfunktion daran hindern, den Port zu öffnen.

   ii. Stellen Sie sicher, dass Sie Zertifikate und Schlüsseldateien korrekt benannt und am richtigen Pfad abgelegt haben, falls es sich um ein SSL-Szenario handelt.

   iii. Stellen Sie sicher, dass zwischen 6001 und 6099 genügend Ports für neue Shadowing-Anfragen verfügbar sind.

iv. Stellen Sie sicher, dass 'netstat' installiert ist, da es von `/var/xdl/sessionshadowing.sh` benötigt wird.

v. Führen Sie `openssl x509 -in shadowingcert.pem -text -noout` aus, um zu überprüfen, ob die Zertifikate korrekt konfiguriert sind, und achten Sie dabei besonders auf die Felder CN und SAN.

vi. Unter RHEL 8 kann es vorkommen, dass `rebind.so` nicht gefunden wird. Um dieses Problem zu beheben, führen Sie den folgenden Befehl aus:

```
ln -s /usr/bin/rebind.so /usr/local/bin/rebind.so
```

Der Überwachungsdienst-Daemon

Der Überwachungsdienst-Daemon (**ctxmonitord**) überwacht wichtige Dienste durch regelmäßige Scans. Wenn Ausnahmen erkannt werden, startet oder stoppt der Daemon Dienstprozesse und bereinigt Prozessreste, um Ressourcen freizugeben. Die erkannten Ausnahmen werden in der Datei **/var/log/xdl/ms.log** protokolliert.

Konfiguration

Der Überwachungsdienst-Daemon startet automatisch, wenn Sie den VDA starten.

Sie können die Funktion über die Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** unter **/opt/Citrix/VDA/sbin** mit Administratorrechten konfigurieren.

Damit Ihre Änderungen in den Dateien **scanningpolicy.conf**, **rulesets.conf** und **whitelist.conf** wirksam werden, führen Sie den folgenden Befehl aus, um den Überwachungsdienst-Daemon neu zu starten.

```
systemctl restart ctxmonitord
```

- **scanningpolicy.conf**

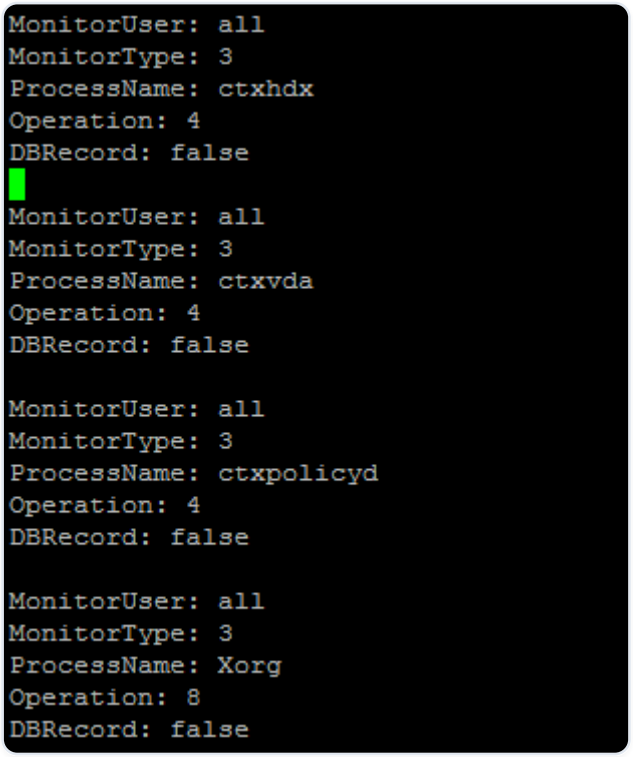
  Diese Konfigurationsdatei aktiviert oder deaktiviert den Überwachungsdienst-Daemon. Sie legt das Dienst-Erkennungsintervall fest und gibt an, ob erkannte Ausnahmen repariert werden sollen.

  - MonitorEnable: true/false (standardmäßig true)
  - DetectTime: 20 (Einheit: Sekunden, Standardwert: 20, Mindestwert: 5)
  - AutoRepair: true/false (standardmäßig true)

- MultBalance: falsch
- ReportAlarm: falsch

- **rulesets.conf**

  Diese Konfigurationsdatei gibt die zu überwachenden Zieldienste an. Standardmäßig gibt es vier überwachte Dienste, wie im folgenden Screenshot gezeigt.



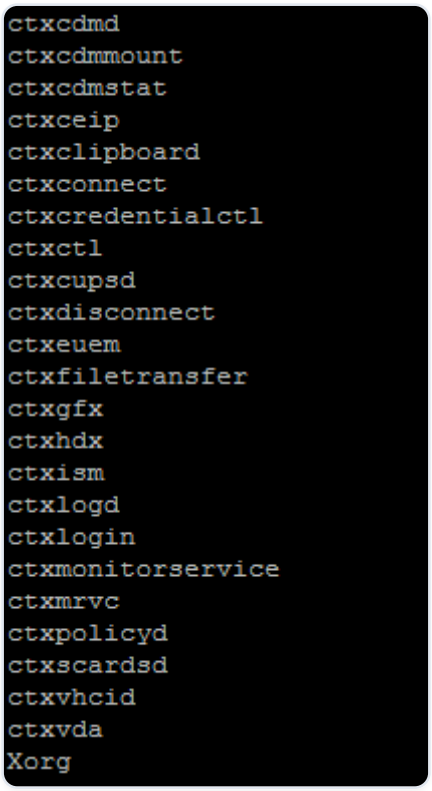
  Um jeden zu überwachenden Dienst zu konfigurieren, legen Sie die folgenden Felder fest.

  - **MonitorUser**: alle
  - **MonitorType**: 3
  - **ProcessName**: <> (Der Prozessname darf nicht leer sein und muss exakt übereinstimmen.)
  - **Operation**: 1/2/4/8 (1 = Dienst beenden, wenn Ausnahmen erkannt werden. 2 = Dienst beenden (kill), wenn Ausnahmen erkannt werden. 4 = Dienst neu starten. 8 = Xorg-Prozessreste löschen.)
  - **DBRecord**: falsch

- **whitelist.conf**

  Die in der Datei **rulesets.conf** angegebenen Zieldienste müssen auch in der Datei **whitelist.conf** konfiguriert werden. Die Whitelist-Konfiguration ist ein sekundärer Filter für die Sicherheit.

Um die Whitelist zu konfigurieren, fügen Sie nur die Prozessnamen (die exakt übereinstimmen müssen) in die Datei **whitelist.conf** ein. Ein Beispiel finden Sie im folgenden Screenshot.



Hinweis:

Bevor Sie die Dienste **ctxvda**, **ctxhdx** und **ctxpolicyd** beenden, führen Sie den Befehl **systemctl stop ctxmonitord** aus, um den Monitor-Dienst-Daemon zu beenden. Andernfalls startet der Monitor-Dienst-Daemon die von Ihnen beendeten Dienste neu.

Tools und Dienstprogramme

Dienstprogramm zur Abfrage von Sitzungsdaten

Wir stellen ein Dienstprogramm (**ctxsdcutil**) bereit, das Sie verwenden können, um Sitzungsdaten auf jedem Linux VDA abzufragen. Um die folgenden Daten aller Sitzungen oder einer bestimmten Sitzung, die auf einem VDA gehostet wird, abzufragen, führen Sie den Befehl `/opt/Citrix/VDA/bin/ctxsdcutil -q <all | SessionID> [-c]` aus. Das Argument `[-c]` bedeutet, Daten jede Sekunde abzufragen.

- **Eingangsbandbreite der Sitzung**
- **Ausgangsbandbreite der Sitzung**

- **Leitungsgeschwindigkeit der Ausgangssitzung**
- **Latenz – zuletzt aufgezeichnet**
- **Roundtripzeit**
- **ThinWire-Ausgangsbandbreite**
- **Audio-Ausgangsbandbreite**
- **Drucker-Ausgangsbandbreite**
- **Laufwerk-Eingangsbandbreite**
- **Laufwerk-Ausgangsbandbreite**

Das xdlcollect Bash-Skript

Das **xdlcollect** Bash-Skript zum Sammeln von Protokollen ist in die Linux VDA-Software integriert und befindet sich unter **/opt/Citrix/VDA/bin**. Nach der Installation des Linux VDA können Sie den Befehl bash **/opt/Citrix/VDA/bin/xdlcollect.sh** ausführen, um Protokolle zu sammeln. Nach Abschluss der Protokollsammlung wird eine komprimierte Protokolldatei im selben Ordner wie das Skript generiert. Das **xdlcollect** Bash-Skript kann Sie 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. Der Upload entfernt die komprimierte Protokolldatei nicht von Ihrem lokalen Computer. Andere Benutzer können die upload_ID verwenden, um auf die Protokolldatei in CIS zuzugreifen.

XDPing

Das Linux-Tool **XDPing** ist eine Befehlszeilenanwendung. Es automatisiert die Überprüfung auf häufige Konfigurationsprobleme in einer Linux-VDA-Umgebung.

Installieren des Linux-Tools XDPing

Das Ausführen von ctxsetup.sh installiert **XDPing** nicht. Um **XDPing** zu installieren, führen Sie `sudo /opt/Citrix/VDA/bin/xdping` aus. Dieser Befehl erstellt auch eine virtuelle **Python3**-Umgebung, die für **XDPing** erforderlich ist. Wenn dieser Befehl keine virtuelle **Python3**-Umgebung erstellen kann, erstellen Sie sie manuell gemäß den Anweisungen unter 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`

Aufgaben, die mit XDPing ausgeführt werden können

XDPing wird mit der einzelnen ausführbaren Datei namens **xdping** geliefert, die über die Befehlsshell ausgeführt wird.

Die folgende Tabelle beschreibt die verschiedenen Aufgaben, die mit den entsprechenden **XDPing**-Befehlen ausgeführt werden können:

AUFGABE	XDPING-BEFEHL	ANMERKUNGEN
Anzeigen der Befehlszeilenoptionen	**sudo /opt/Citrix/VDA/bin/xdping -h (Hilfe)**	N/A
Ausführen der vollständigen Testsuite	**sudo /opt/Citrix/VDA/bin/xdping** (führen Sie **XDPing** ohne Befehlszeilenoption aus)	Das Linux-Tool **XDPing** führt über 150 einzelne Tests auf dem System durch. Weitere Informationen finden Sie unter Einzelne Tests weiter unten in diesem Artikel.
So führen Sie eine Prüfung des VDA-Registrierungsstatus durch	**sudo /opt/Citrix/VDA/bin/xdping -a (alle)**	Weitere Informationen finden Sie unter Umfang der Registrierungsstatusprüfungen weiter unten in diesem Artikel.
So sichern Sie die Schlüsseldaten eines VDA	**sudo /opt/Citrix/VDA/bin/xdping -b**	Weitere Informationen finden Sie unter Sicherung und Vergleich von VDA-Daten weiter unten in diesem Artikel.
So vergleichen Sie die letzten beiden Kopien der VDA-Sicherungsdaten	**sudo /opt/Citrix/VDA/bin/xdping -diff**	Weitere Informationen finden Sie unter Sicherung und Vergleich von VDA-Daten weiter unten in diesem Artikel.
So vergleichen Sie zwei bestimmte Kopien der VDA-Sicherungsdaten	**sudo /opt/Citrix/VDA/bin/xdping -diff=<ein Sicherungsdatenverzeichnis>:<das andere**	Weitere Informationen finden Sie unter Sicherung und Vergleich von VDA-Daten

AUFGABE	XDPING-BEFEHL	ANMERKUNGEN
	Sicherungsdatenverzeichnis>	weiter unten in diesem Artikel.
So überprüfen Sie die Umgebung vor der Installation des Linux-VDA-Pakets	**sudo /opt/Citrix/VDA/bin/xdping --vorabprüfung**	N/A
Um nur bestimmte Testkategorien auszuführen, zum Beispiel die Zeit-, Kerberos- und Datenbanktests	**sudo /opt/Citrix/VDA/bin/xdping -T zeit,kerberos,datenbank**	N/A
Um einen bestimmten Delivery Controller zu prüfen	**sudo /opt/Citrix/VDA/bin/xdping -d <FQDN des Delivery Controllers>**	N/A

EINZELNE TESTS

Das Linux-Tool **XDPing** führt über 150 einzelne Tests auf dem System durch, die grob wie folgt kategorisiert sind:

- Prüfen, ob die Systemanforderungen des Linux VDA erfüllt sind.
- Maschineninformationen, einschließlich der Linux-Distributionen, identifizieren und anzeigen.
- Die Kompatibilität des Linux-Kernels prüfen.
- Auf bekannte Probleme mit Linux-Distributionen prüfen, die den Betrieb des Linux VDA beeinträchtigen können.
- Den Security-Enhanced Linux (SELinux)-Modus und die Kompatibilität prüfen.
- Netzwerkschnittstellen identifizieren und Netzwerkeinstellungen prüfen.
- Speicherpartitionierung und verfügbaren Speicherplatz prüfen.
- Die Konfiguration von Maschinen-Host- und Domänennamen prüfen.
- Die DNS-Konfiguration prüfen und Lookup-Tests durchführen.
- Zugrunde liegende Hypervisoren identifizieren und die Konfiguration der virtuellen Maschine überprüfen. Unterstützung für:
    - Citrix Hypervisor™

  - Microsoft HyperV
  - VMware vSphere

- Zeiteinstellungen überprüfen und prüfen, ob die Netzwerkzeitsynchronisierung betriebsbereit ist.
- 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 geöffnet sind.
- Kerberos-Konfiguration überprüfen und Authentifizierungstests durchführen.
- Die LDAP-Suchumgebung für die Gruppenrichtlinien-Dienst-Engine überprüfen.
- Überprüfen, ob die Active Directory-Integration ordnungsgemäß eingerichtet ist und die aktuelle Maschine der Domäne beigetreten ist. Unterstützung für:
  - Samba Winbind
  - Dell Quest Authentication Services
  - Centrify DirectControl
  - SSSD
- Die Integrität des Linux-Computerobjekts im Active Directory überprüfen.
- Die Konfiguration des Pluggable Authentication Module (PAM) überprüfen.
- Überprüfen Sie das Core-Dump-Muster.
- Überprüfen Sie, ob die vom Linux VDA benötigten Pakete installiert sind.
- Identifizieren Sie das Linux VDA-Paket und überprüfen Sie die Integrität der Installation.
- Überprüfen Sie die Integrität der PostgreSQL-Registrierungsdatenbank.
- Überprüfen Sie, ob die Linux VDA-Dienste ordnungsgemäß konfiguriert und betriebsbereit sind.
- Überprüfen Sie die Integrität der VDA- und HDX™-Konfiguration.
- Testen Sie jeden konfigurierten Delivery Controller™, um zu überprüfen, ob der Broker Service erreichbar, betriebsbereit und reaktionsfähig ist.
- Überprüfen Sie, ob der Computer bei der Delivery Controller-Farm registriert ist.
- Überprüfen Sie den Status jeder aktiven oder getrennten HDX-Sitzung.
- Durchsuchen Sie Protokolldateien nach Linux VDA-bezogenen Fehlern und Warnungen.
- Überprüfen Sie, ob die Xorg-Version geeignet ist.
- Überprüfen Sie, ob die erforderlichen Abhängigkeiten installiert sind.

BEISPIELAUSGABE

Im Folgenden sehen Sie eine Beispielausgabe des Kerberos-Tests:

```
sudo xdping -T kerberos

Root User ------------------------------------------------------------------
    User:         root
    EUID:         0
      Verify user is root                                              [Pass]

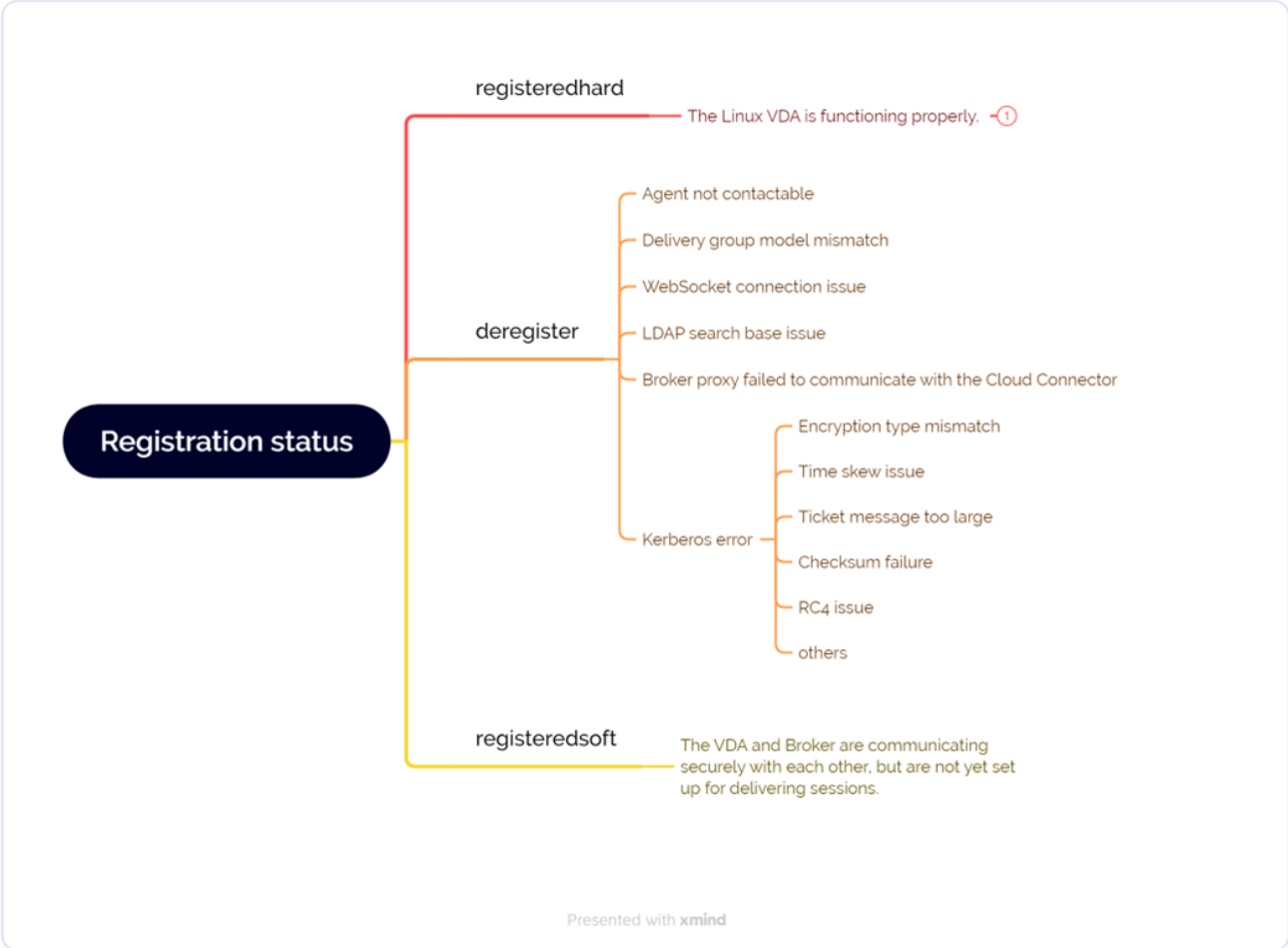
Kerberos -------------------------------------------------------------------
    Kerberos version: 5
      Verify Kerberos available                                        [Pass]
      Verify Kerberos version 5                                        [Pass]
    KRB5CCNAME:   [Not set]
                  Distro default FILE:/tmp/krb5cc_%{uid}
    KRB5CCNAME type: [Supported]
    KRB5CCNAME format: [Default]
      Verify KRB5CCNAME cache type                                     [Pass]
      Verify KRB5CCNAME format                                         [Pass]
    Configuration file: /etc/krb5.conf [Exists]
      Verify Kerberos configuration file found                         [Pass]
  Keytab file:  /etc/krb5.keytab [Exists]
  Default realm: XD2.LOCAL
  Default realm KDCs: [NONE SPECIFIED]
  Default realm domains: [NONE SPECIFIED]
  DNS lookup realm: [Enabled]
  DNS lookup KDC: [Enabled]
  Weak crypto:  [Disabled]
  Clock skew limit:  300 s
    Verify system keytab file exists                                   [Pass]
    Verify default realm set                                           [Pass]
    Verify default realm in upper-case                                 [Pass]
    Verify default realm not EXAMPLE.COM                               [Pass]
    Verify default realm domain mappings                               [Pass]
    Verify default realm master KDC configured                         [Pass]
    Verify Kerberos weak crypto disabled                               [Pass]
    Verify Kerberos clock skew setting                                 [Pass]
  Default ccache: [Not set]
                  Distro default FILE:/tmp/krb5cc_%{uid}
  Default ccache type: [Supported]
  Default ccache format: [Default]
    Verify default credential cache cache type                         [Pass]
    Verify default credential cache format                             [Pass]
  UPN system key [MYVDA1$@[redacted]]: [MISSING]
  SPN system key [host/[redacted]]: [Exists]
    Verify Kerberos system keys for UPN exist                          [ERROR]
    No system keys were found for the user principal name (UPN) of
    the machine account. For the Linux VDA to mutually authenticate
    with the Delivery Controller, the system keytab file must
    contain keys for both the UPN and host-based SPN of the machine
    account.
```

```
      Verify Kerberos system keys for SPN exist                    [Pass]
    Kerberos login: [FAILED AUTHENTICATION]
                    Keytab contains no suitable keys for MYVDA1$@[redacted]
                    while getting initial credentials
      Verify KDC authentication                                    [ERROR]
      Failed to authenticate and obtain a Ticket Granting Ticket (TGT)
      from the KDC authentication service for the machine account UPN
      MYVDA1$@[redacted]. Check that the Kerberos configuration is
      valid and the keys in the system keytab are current.


Summary ------------------------------------------------------------------------
  The following tests did not pass:
      Verify Kerberos system keys for UPN exist                    [ERROR]
      Verify KDC authentication                                    [ERROR]
```

UMFANG DER VDA-REGISTRIERUNGSSTATUSPRÜFUNGEN

Das Linux-Tool **XDPing** bietet auch ein Analysemodul, mit dem Sie den Registrierungsstatus Ihres VDA überprüfen und analysieren können. Den Umfang der Registrierungsstatusprüfungen finden Sie im folgenden Screenshot:



SICHERUNG UND VERGLEICH VON VDA-DATEN

Ab Linux VDA 2305 führt das **XDPing**-Tool ein VDA-Sicherungsmodul ein. Mit diesem Modul können Sie die wichtigsten Daten eines VDA jederzeit sichern, z. B. die Konfigurations-, Datenbank- und Binärberechtigungsdaten. Sie können die wichtigsten Daten eines VDA sichern, wenn dieser ordnungsgemäß funktioniert. Falls der VDA später ausfällt, sichern Sie eine weitere Kopie der Daten und vergleichen Sie die beiden Datenkopien, um die Fehlerbehebung zu erleichtern. Die folgende Tabelle beschreibt die Sicherung und den Vergleich von VDA-Daten mit den entsprechenden **XDPing**-Befehlen:

AUFGABE	XDPING-BEFEHL	ANMERKUNGEN
So sichern Sie die wichtigsten Daten eines VDA	**sudo /opt/Citrix/VDA/bin/xdping -b**	Jedes Mal, wenn Sie den Sicherungsbefehl ausführen, wird eine Kopie der Sicherungsdaten generiert und in einem Verzeichnis unter **/var/ctxbackup** gespeichert. Die Verzeichnisse der Sicherungsdaten werden nach dem aktuellen Datum und der Uhrzeit im Format **JJJJ-MM-TT-HH_MM_SS** benannt, z. B. **2023-02-27-16_31_27**. Standardmäßig beträgt die maximale Anzahl der Sicherungsdatenverzeichnisse 30, und das **XDPing**-Tool rotiert oder löscht alte Sicherungsdatenverzeichnisse, wenn die Anzahl überschritten wird. Um die Anzahl für die Verzeichnisrotation anzupassen, führen Sie den folgenden Befehl aus: `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent\Backup" -t "REG_DWORD" -v`

AUFGABE	XDPING-BEFEHL	ANMERKUNGEN
		`"MaxDirRotationCount" -d "0x0000005" --force`
So vergleichen Sie die letzten beiden Kopien der VDA-Sicherungsdaten	**sudo /opt/Citrix/VDA/bin/xdping -diff**	N/A
So vergleichen Sie zwei bestimmte Kopien der VDA-Sicherungsdaten	**sudo /opt/Citrix/VDA/bin/xdping -diff=<ein Sicherungsdatenverzeichnis>:<das andere Sicherungsdatenverzeichnis>**	N/A

Andere

Dieser Abschnitt enthält die folgenden Themen:

- Unterstützung der Citrix Workspace-App für HTML5
- Erstellen einer virtuellen **Python3**-Umgebung
- NIS in Active Directory integrieren
- **IPv6**
- LDAPS
- **Xauthority**

Unterstützung für Citrix Workspace™-App für HTML5

Sie können die Citrix Workspace-App für HTML5 verwenden, um direkt auf virtuelle Linux-Apps und -Desktops zuzugreifen, ohne Ihren Client mit Citrix Gateway zu verbinden. Informationen zur Citrix Workspace-App für HTML5 finden Sie in der Citrix-Dokumentation.

Dieses Feature aktivieren

Dieses Feature ist standardmäßig deaktiviert. Gehen Sie zum Aktivieren wie folgt vor:

1. Aktivieren Sie in Citrix StoreFront™ die Citrix Workspace-App für HTML5.

   Die detaillierte Vorgehensweise finden Sie in Schritt 1 des Knowledge Center-Artikels CTX208163.

2. WebSocket-Verbindungen aktivieren.

a. Legen Sie in Citrix Studio die Richtlinie **WebSockets connections** auf **Allowed** fest.

   Sie können auch die anderen WebSocket-Richtlinien festlegen. Eine vollständige Liste der WebSocket-Richtlinien finden Sie unter WebSockets-Richtlinieneinstellungen.

b. Starten Sie auf dem VDA den Dienst `ctxvda` und den Dienst `ctxhdx` in dieser Reihenfolge neu, damit Ihre Einstellung wirksam wird.

c. Führen Sie auf dem VDA den folgenden Befehl aus, um zu überprüfen, ob der WebSocket-Listener ausgeführt wird.

   ```
   netstat -an | grep 8008
   ```

   Wenn der WebSocket-Listener ausgeführt wird, ähnelt die Befehlsausgabe dem Folgenden:

   ```
   tcp 0 0 :::8008 :::* LISTEN
   ```

Hinweis: Sie können auch die TLS-Verschlüsselung aktivieren, um WebSocket-Verbindungen zu sichern. Informationen zum Aktivieren der TLS-Verschlüsselung finden Sie unter Benutzersitzungen mit TLS sichern.

Erstellen einer Python3-virtuellen Umgebung

Wenn Sie mit dem Netzwerk verbunden sind, kann die Ausführung des Befehls `sudo /opt/Citrix/VDA/bin/xdping` oder `/opt/Citrix/VDA/sbin/enable_ldaps.sh` eine **Python3**-virtuelle Umgebung erstellen. Wenn die Befehle jedoch keine **Python3**-virtuelle Umgebung erstellen können, können Sie diese manuell auch ohne Netzwerkverbindung erstellen. Dieser Artikel beschreibt die Voraussetzungen und Schritte zum Erstellen einer **Python3**-virtuellen Umgebung ohne Netzwerkverbindung.

Voraussetzungen

- Sie müssen über Administratorrechte verfügen, um auf das Verzeichnis `/opt/Citrix/VDA/sbin/ctxpython3` zugreifen zu können.
- Die Wheel-Dateien der `Python3`-Pakete sind vorhanden. Sie können die Wheel-Dateien von `<https://pypi.org/>` herunterladen.

Erstellen einer Python3-virtuellen Umgebung

Führen Sie die folgenden Schritte aus, um eine **Python3**-virtuelle Umgebung zu erstellen:

1. Installieren Sie **Python3**-Abhängigkeiten.

   Für Amazon Linux 2:

```
yum -y install python3 python3-devel krb5-devel gcc
```

Für RHEL und Rocky Linux:

```
yum -y install python3-devel krb5-devel gcc
```

Hinweis:

Möglicherweise müssen Sie ein bestimmtes Repository aktivieren, um einige Abhängigkeiten zu installieren. Führen Sie für RHEL 7 den Befehl `subscription-manager repos --enable rhel-7-server-optional-rpms` aus. Führen Sie für RHEL 8 den Befehl `subscription-manager repos --enable=rhel-8-for-x86_64-appstream-rpms` aus.

Für Debian, Ubuntu:

```
apt-get -y install python3-dev python3-pip python3-venv libkrb5-dev
```

Für SUSE:

```
zypper -n install lsb-release python3-devel python3-setuptools krb5-devel gcc libffi-devel libopenssl-devel
```

2. Erstellen Sie eine **Python3**-virtuelle Umgebung.

Hinweis:

Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des Pip-Tools auftreten können, sollten Sie die folgenden vertrauenswürdigen Hosts zur Datei /etc/pip.conf hinzufügen:

\> `[global]`

`trusted-host =`

\> `pypi.org`

`files.pythonhosted.org`

Für Amazon Linux 2, Debian, RHEL, Rocky Linux, Ubuntu:

```
sudo python3 -m venv /opt/Citrix/VDA/sbin/ctxpython3
```

Für 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
```

3. LDAPS-Abhängigkeiten installieren.

```
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
```

4. **XDPing**-Abhängigkeiten installieren.

```
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
```

NIS in Active Directory integrieren

Dieser Artikel beschreibt, wie NIS mit Windows Active Directory (AD) auf dem Linux VDA mithilfe von SSSD integriert wird. Der Linux VDA wird als Komponente von Citrix Virtual Apps and Desktops betrachtet. Daher fügt er sich nahtlos in die Windows AD-Umgebung ein.

Die Verwendung von NIS anstelle von AD als UID- und GID-Anbieter erfordert, dass die Kontoinformationen (Benutzername- und Kennwortkombinationen) in AD und NIS identisch sind.

Hinweis:

Die Authentifizierung wird weiterhin vom AD-Server durchgeführt. NIS+ wird nicht unterstützt. Wenn Sie NIS als UID- und GID-Anbieter verwenden, werden die POSIX-Attribute vom Windows-Server nicht mehr verwendet.

Tipp:

> Diese Methode stellt eine veraltete Art der Bereitstellung des Linux VDA dar, die nur für spezielle Anwendungsfälle verwendet wird. Für eine RHEL/CentOS-Distribution befolgen Sie die Anweisungen unter Installieren des Linux VDA unter Amazon Linux 2, CentOS, RHEL und Rocky Linux manuell. Für eine Ubuntu-Distribution befolgen Sie die Anweisungen unter Installieren des Linux VDA unter Ubuntu manuell.

> Was ist SSSD?

SSSD ist ein System-Daemon. Seine Hauptfunktion besteht darin, den Zugriff auf die Identifizierung und Authentifizierung entfernter Ressourcen über ein gemeinsames Framework zu ermöglichen, das Caching und Offline-Unterstützung für das System bieten kann. Es stellt sowohl PAM- als auch NSS-Module bereit und kann zukünftig D-BUS-basierte Schnittstellen für erweiterte Benutzerinformationen unterstützen. Es bietet auch eine bessere Datenbank zum Speichern lokaler Benutzerkonten und erweiterter Benutzerdaten.

NIS in AD integrieren

Um NIS in AD zu integrieren, führen Sie die folgenden Schritte aus:

SCHRITT 1: LINUX VDA ALS NIS-CLIENT HINZUFÜGEN

Konfigurieren Sie den NIS-Client:

```
yum –y install ypbind rpcbind oddjob-mkhomedir
```

Legen Sie die NIS-Domäne fest:

```
ypdomainname nis.domain

echo "NISDOMAIN=nis.domain" >> /etc/sysconfig/network
```

Fügen Sie die IP-Adresse für den NIS-Server und -Client in **/etc/hosts** hinzu:

`{NIS server IP address}  server.nis.domain nis.domain`

Konfigurieren Sie NIS durch `authconfig`:

```
sudo authconfig --enablenis --nisdomain=nis.domain --
nisserver=server.nis.domain --enablemkhomedir --update
```

Die **nis.domain** stellt den Domänennamen des NIS-Servers dar. Die **server.nis.domain** ist der Hostname des NIS-Servers, der auch die IP-Adresse des NIS-Servers sein kann.

Konfigurieren Sie die NIS-Dienste:

```
sudo systemctl start rpcbind ypbind



sudo systemctl enable rpcbind ypbind
```

Stellen Sie sicher, dass die NIS-Konfiguration korrekt ist:

```
ypwhich
```

Überprüfen Sie, ob die Kontoinformationen vom NIS-Server verfügbar sind:

```
getent passwd nisaccount
```

Hinweis:

Das **nisaccount** stellt das echte NIS-Konto auf dem NIS-Server dar. Stellen Sie sicher, dass UID, GID, Home-Verzeichnis und Anmelde-Shell korrekt konfiguriert sind.

SCHRITT 2: DOMÄNE BEITRETEN UND HOST-KEYTAB MIT SAMBA ERSTELLEN

SSSD bietet keine AD-Client-Funktionen zum Beitreten der Domäne und zur Verwaltung der System-Keytab-Datei. Es gibt verschiedene Methoden, um diese Funktionen zu erreichen, darunter:

- `adcli`
- `realmd`
- `Winbind`
- `Samba`

Die Informationen in diesem Abschnitt beschreiben nur den Samba-Ansatz. Für `realmd` siehe die Dokumentation des RHEL- oder CentOS-Anbieters. Diese Schritte müssen vor der Konfiguration von SSSD befolgt werden.

Domäne beitreten und Host-Keytab mit Samba erstellen:

Auf dem Linux-Client mit ordnungsgemäß konfigurierten Dateien:

- /etc/krb5.conf
- /etc/samba/smb.conf:

Konfigurieren Sie den Computer für Samba- und Kerberos-Authentifizierung:

```
sudo authconfig --smbsecurity=ads --smbworkgroup=domain --smbrealm=REALM
--krb5realm=REALM --krb5kdc=fqdn-of-domain-controller --update
```

Wobei **REALM** der Kerberos-Realm-Name in Großbuchstaben und **domain** der NetBIOS-Name der Domäne ist.

Wenn eine DNS-basierte Suche nach dem KDC-Server und dem Realm-Namen erforderlich ist, fügen Sie die folgenden beiden Optionen zum vorhergehenden Befehl hinzu:

`--enablekrb5kdcdns --enablekrb5realmdns`

Öffnen Sie **/etc/samba/smb.conf** und fügen Sie die folgenden Einträge unter dem Abschnitt **\[Global\]** hinzu, jedoch nach dem Abschnitt, der vom **authconfig**-Tool generiert wurde:

`kerberos method = secrets and keytab`

`winbind offline logon = no`

Das Beitreten zur Windows-Domäne erfordert, dass Ihr Domänencontroller erreichbar ist und Sie über ein AD-Benutzerkonto mit Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen:

```
sudo net ads join REALM -U user
```

REALM ist der Kerberos-Realm-Name in Großbuchstaben und **user** ist ein Domänenbenutzer, der Berechtigungen zum Hinzufügen von Computern zur Domäne besitzt.

SCHRITT 3: SSSD EINRICHTEN

Die Einrichtung von SSSD umfasst die folgenden Schritte:

- Installieren Sie die Pakete **sssd-ad** und **sssd-proxy** auf dem Linux-Client.

- Nehmen Sie Konfigurationsänderungen an verschiedenen Dateien vor (zum Beispiel **sssd.conf**).
- Starten Sie den **sssd-Dienst**.

/etc/sssd/sssd.conf
Eine Beispielkonfiguration für **sssd.conf** (weitere Optionen können bei Bedarf hinzugefügt werden):

```
[sssd]

config_file_version = 2

domains = EXAMPLE

services = nss, pam



[domain/EXAMPLE]

# Uncomment if you need offline logins

# cache_credentials = true

re_expression = (((?P<domain>[^\\]+)\\(?P<name>.+$))|((?P<name>[^@]+)@(?
P<domain>.+$))|(^(?P<name>[^@\\]+)$))

id_provider = proxy

proxy_lib_name = nis

auth_provider = ad

access_provider = ad



# Should be specified as the long version of the Active Directory domain.

ad_domain = EXAMPLE.COM
```

```
# Kerberos settings

krb5_ccachedir = /tmp

krb5_ccname_template = FILE:%d/krb5cc_%U



# Uncomment if service discovery is not working

# ad_server = server.ad.example.com



# Comment out if the users have the shell and home dir set on the AD side

default_shell = /bin/bash

fallback_homedir = /home/%d/%u



# Uncomment and adjust if the default principal SHORTNAME$@REALM is not
available

# ldap_sasl_authid = host/client.ad.example.com@AD.EXAMPLE.COM
```

Ersetzen Sie **ad.domain.com**, **server.ad.example.com** durch den entsprechenden Wert. Weitere Informationen finden Sie auf der **sssd-ad**(5) - Linux-Manpage.

Legen Sie den Dateibesitz und die Berechtigungen für **sssd.conf** fest:

`chown root:root /etc/sssd/sssd.conf`

`chmod 0600 /etc/sssd/sssd.conf` `restorecon /etc/sssd/sssd.conf`

SCHRITT 4: NSS/PAM KONFIGURIEREN

RHEL/CentOS:

Verwenden Sie **authconfig**, um SSSD zu aktivieren. Installieren Sie **oddjob-mkhomedir**, um sicherzustellen, dass die Erstellung des Home-Verzeichnisses mit SELinux kompatibel ist:

```
authconfig --enablesssd --enablesssdauth --enablemkhomedir --update


sudo systemctl start sssd


sudo systemctl enable sssd
```

Tipp:

Beachten Sie bei der Konfiguration der Linux VDA-Einstellungen, dass es für SSSD keine speziellen Einstellungen für den Linux VDA-Client gibt. Verwenden Sie für zusätzliche Lösungen im Skript **ctxsetup.sh** den Standardwert.

SCHRITT 5: KERBEROS-KONFIGURATION ÜBERPRÜFEN

Um sicherzustellen, dass Kerberos für die Verwendung mit dem Linux VDA korrekt konfiguriert ist, überprüfen Sie, ob die Systemdatei **keytab** erstellt wurde und gültige Schlüssel enthält:

```
sudo klist -ke
```

Dieser Befehl zeigt die Liste der Schlüssel an, die für die verschiedenen Kombinationen von Prinzipalnamen und Chiffriersuiten verfügbar sind. Führen Sie den Kerberos-Befehl **kinit** aus, um den Computer mit dem Domänencontroller unter Verwendung dieser Schlüssel zu authentifizieren:

```
sudo kinit –k MACHINE\$@REALM
```

Die Computer- und Realm-Namen müssen in Großbuchstaben angegeben werden. Das Dollarzeichen ($) muss mit einem Backslash (\\) maskiert werden, um eine Shell-Substitution zu verhindern. In einigen Umgebungen unterscheidet sich der DNS-Domänenname vom Kerberos-Realm-Namen. Stellen Sie sicher, dass der Realm-Name verwendet wird. Wenn dieser Befehl erfolgreich ist, wird keine Ausgabe angezeigt.

Überprüfen Sie, ob das TGT-Ticket für das Computerkonto mit folgendem Befehl zwischengespeichert wurde:

```
sudo klist -ke
```

SCHRITT 6: BENUTZERAUTHENTIFIZIERUNG ÜBERPRÜFEN

Verwenden Sie den Befehl **getent**, um zu überprüfen, ob das Anmeldeformat unterstützt wird und ob der NSS funktioniert:

```
sudo getent passwd DOMAIN\\username
```

Der Parameter **DOMAIN** gibt den Kurznamen der Domäne an. Wenn ein anderes Anmeldeformat erforderlich ist, überprüfen Sie dies zuerst mit dem Befehl **getent**.

Die unterstützten Anmeldeformate sind:

- Down-Level-Anmeldename: `DOMAIN\username`
- UPN: `username@domain.com`
- NetBIOS-Suffix-Format: `username@DOMAIN`

Um zu überprüfen, ob das SSSD PAM-Modul korrekt konfiguriert ist, melden Sie sich mit einem Domänenbenutzerkonto am Linux VDA an. Das Domänenbenutzerkonto wurde zuvor noch nicht verwendet.

```
sudo ssh localhost –l DOMAIN\\username



id -u
```

Überprüfen Sie, ob eine entsprechende Kerberos-Anmeldeinformations-Cache-Datei für die vom Befehl zurückgegebene **uid** erstellt wurde:

```
ls /tmp/krb5cc_{uid}
```

Überprüfen Sie, ob die Tickets im Kerberos-Anmeldeinformations-Cache des Benutzers gültig und nicht abgelaufen sind:

```
klist
```

IPv6

Der Linux VDA unterstützt **IPv6**, um mit Citrix Virtual Apps and Desktops übereinzustimmen. Beachten Sie bei der Verwendung dieser Funktion Folgendes:

- In Dual-Stack-Umgebungen wird **IPv4** verwendet, es sei denn, **IPv6** ist explizit aktiviert.
- Wenn **IPv6** in einer **IPv4**-Umgebung aktiviert ist, funktioniert der Linux VDA nicht.

> **Wichtig:**
>
> - Die gesamte Netzwerkumgebung muss **IPv6** sein, nicht nur für den Linux VDA.
> - **Centrify** unterstützt kein reines **IPv6**.

> Bei der Installation des Linux VDA sind keine speziellen Einrichtungsschritte für **IPv6** erforderlich.

IPv6 für den Linux VDA konfigurieren

Bevor Sie die Konfiguration für den Linux VDA ändern, stellen Sie sicher, dass Ihre Linux-VM zuvor in einem **IPv6**-Netzwerk funktioniert hat. Es gibt zwei Registrierungsschlüssel, die sich auf die **IPv6**-Konfiguration beziehen:

```
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"OnlyUseIPv6ControllerRegistration"

"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"ControllerRegistrationIPv6Netmask"
```

OnlyUseIPv6ControllerRegistration muss auf 1 gesetzt werden, um **IPv6** auf dem Linux VDA zu aktivieren:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_DWORD" -v
"OnlyUseIPv6ControllerRegistration" -d "0x00000001" --force
```

Wenn der Linux VDA mehr als eine Netzwerkschnittstelle hat, kann **ControllerRegistrationIPv6Netmask** verwendet werden, um anzugeben, welche für die Linux VDA-Registrierung verwendet wird:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Policies\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ControllerRegistrationIPv6Netmask " -d "{IPv6 netmask}" --force
```

Ersetzen Sie **{IPv6 netmask}** durch die tatsächliche Netzmaske (z. B. 2000::/64).

Weitere Informationen zur **IPv6**-Bereitstellung in Citrix Virtual Apps and Desktops finden Sie unter **IPv4/IPv6-Unterstützung**.

Problembehandlung

Überprüfen Sie die grundlegende **IPv6**-Netzwerkumgebung und verwenden Sie ping6, um zu prüfen, ob AD und Delivery Controller™ erreichbar sind.

LDAPS

LDAPS ist die sichere Version des Lightweight Directory Access Protocol (LDAP), bei der LDAP-Kommunikationen mit TLS/SSL verschlüsselt werden.

Standardmäßig sind LDAP-Kommunikationen zwischen Client- und Serveranwendungen nicht verschlüsselt. LDAPS ermöglicht es Ihnen, den Inhalt von LDAP-Abfragen zwischen dem Linux VDA und den LDAP-Servern zu schützen.

Die folgenden Linux VDA-Komponenten sind von LDAPS abhängig:

- Broker-Agent: Linux VDA-Registrierung bei einem Delivery Controller™
- Richtliniendienst: Richtlinienauswertung

Die Konfiguration von LDAPS umfasst:

- LDAPS auf dem Active Directory (AD)/LDAP-Server aktivieren
- Stammzertifizierungsstelle für die Clientnutzung exportieren
- LDAPS auf dem Linux VDA aktivieren/deaktivieren
- LDAPS für Drittanbieterplattformen konfigurieren
- SSSD konfigurieren
- Winbind konfigurieren
- Centrify konfigurieren
- Quest konfigurieren

Hinweis:

Sie können den folgenden Befehl ausführen, um einen Überwachungszyklus für Ihre LDAP-Server festzulegen. Der Standardwert ist 15 Minuten. Stellen Sie ihn auf mindestens 10 Minuten ein.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -v
"ListOfLDAPServersMonitorPeroid" -t "REG_DWORD" -d "0x0000000f" --
force
```

LDAPS auf dem AD/LDAP-Server aktivieren

Sie können LDAP über SSL (LDAPS) aktivieren, indem Sie ein ordnungsgemäß formatiertes Zertifikat von einer Microsoft-Zertifizierungsstelle (CA) oder einer Nicht-Microsoft-CA installieren.

Tipp:

LDAPS wird automatisch aktiviert, wenn Sie eine Enterprise-Stamm-CA auf einem Domänencontroller installieren.

Weitere Informationen zum Installieren des Zertifikats und zum Überprüfen der LDAPS-Verbindung finden Sie unter How to enable LDAP over SSL with a third-party certification authority.

Wenn Sie eine mehrstufige Zertifizierungsstellenhierarchie haben, verfügen Sie nicht automatisch über das entsprechende Zertifikat für die LDAPS-Authentifizierung auf dem Domänencontroller.

Informationen zum Aktivieren von LDAPS für Domänencontroller, die eine mehrstufige Zertifizierungsstellenhierarchie verwenden, finden Sie im Artikel LDAP over SSL (LDAPS) Certificate.

Stammzertifizierungsstelle für die Clientnutzung aktivieren

Der Client muss ein Zertifikat von einer CA verwenden, der der LDAP-Server vertraut. Um die LDAPS-Authentifizierung für den Client zu aktivieren, importieren Sie das Stamm-CA-Zertifikat in einen vertrauenswürdigen Keystore.

Weitere Informationen zum Exportieren der Stamm-CA finden Sie unter How to export Root Certification Authority Certificate auf der Microsoft Support-Website.

LDAPS auf dem Linux VDA aktivieren oder deaktivieren

Um LDAPS auf dem Linux VDA zu aktivieren oder zu deaktivieren, führen Sie das folgende Skript aus (als Administrator angemeldet):

Die Syntax für diesen Befehl umfasst Folgendes:

- LDAP über SSL/TLS mit dem bereitgestellten Stamm-CA-Zertifikat aktivieren:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enable pathToRootCA
```

- LDAP über SSL/TLS mit Kanalbindung aktivieren:

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Enablecb pathToRootCA
```

Hinweis:

Das Stamm-CA-Zertifikat für die Kanalbindung muss im PEM-Format vorliegen. Wenn die Aktivierung von LDAPS keine **Python3**-virtuelle Umgebung erfolgreich erstellt, erstellen Sie diese manuell gemäß den Anweisungen unter Eine **Python3**-virtuelle Umgebung erstellen.

Um SSL-Verbindungsfehler zu beheben, die bei der Verwendung des pip-Tools auftreten können, sollten Sie die folgenden vertrauenswürdigen Hosts zur Datei /etc/pip.conf hinzufügen:

\> `[global]`

`trusted-host =`

\> `pypi.org`

`files.pythonhosted.org`

- Rückgriff auf LDAP ohne SSL/TLS

```
/opt/Citrix/VDA/sbin/enable_ldaps.sh -Disable
```

Der für LDAPS dedizierte Java-Keystore befindet sich in **/etc/xdl/.keystore**. Betroffene Registrierungsschlüssel sind:

```
HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServers

HKLM\Software\Citrix\VirtualDesktopAgent\ListOfLDAPServersForPolicy

HKLM\Software\Citrix\VirtualDesktopAgent\UseLDAPS

HKLM\Software\Policies\Citrix\VirtualDesktopAgent\Keystore

HKLM\Software\Citrix\VirtualDesktopAgent\EnableChannelBinding
```

LDAPS für Drittanbieterplattform konfigurieren

Neben den Linux-VDA-Komponenten benötigen möglicherweise auch mehrere Drittanbieter-Softwarekomponenten, die dem VDA entsprechen, sicheres LDAP, wie SSSD, Winbind, Centrify und Quest. Die folgenden Abschnitte beschreiben, wie sicheres LDAP mit LDAPS, STARTTLS oder SASL Sign and Seal konfiguriert wird.

Tipp:

Nicht alle dieser Softwarekomponenten bevorzugen die Verwendung von SSL-Port 636, um sicheres LDAP zu gewährleisten. Und meistens kann LDAPS (LDAP über SSL auf Port 636) nicht mit STARTTLS auf Port 389 koexistieren.

SSSD

Konfigurieren Sie den sicheren LDAP-Verkehr von SSSD auf Port 636 oder Port 389 gemäß den Optionen. Weitere Informationen finden Sie auf der SSSD LDAP Linux Manpage.

Winbind

Die Winbind-LDAP-Abfrage verwendet die ADS-Methode. Winbind unterstützt nur die StartTLS-Methode auf Port 389. Betroffene Konfigurationsdateien sind **/etc/samba/smb.conf** und **/etc/openldap/ldap.conf** (für Amazon Linux 2, RHEL, Rocky Linux, CentOS und SUSE) oder **/etc/ldap/ldap.conf** (für Debian und Ubuntu). Ändern Sie die Dateien wie folgt:

- smb.conf

  `ldap ssl = start tls`

  `ldap ssl ads = yes` `client ldap sasl wrapping = plain`

- ldap.conf

  `TLS_REQCERT never`

Alternativ können Sie sicheres LDAP über SASL GSSAPI Sign and Seal konfigurieren, dies kann jedoch nicht mit TLS/SSL koexistieren. Um die SASL-Verschlüsselung zu verwenden, ändern Sie die **smb.conf**-Konfiguration:

`ldap ssl = off`

`ldap ssl ads = no` `client ldap sasl wrapping = seal`

Centrify

Centrify unterstützt LDAPS auf Port 636 nicht. Es bietet jedoch eine sichere Verschlüsselung auf Port 389. Weitere Informationen finden Sie auf der Centrify-Website.

Quest

Quest Authentication Service unterstützt LDAPS auf Port 636 nicht, bietet aber eine sichere Verschlüsselung auf Port 389 mit einer anderen Methode.

Problembehandlung

Die folgenden Probleme können bei der Verwendung dieser Funktion auftreten:

- **Verfügbarkeit des LDAPS-Dienstes**

  Stellen Sie sicher, dass die LDAPS-Verbindung auf dem AD/LDAP-Server verfügbar ist. Der Port ist standardmäßig auf 636 eingestellt.

- **Linux VDA-Registrierung fehlgeschlagen, wenn LDAPS aktiviert ist**

Stellen Sie sicher, dass der LDAP-Server und die Ports korrekt konfiguriert sind. Überprüfen Sie zuerst das Root-CA-Zertifikat und stellen Sie sicher, dass es mit dem AD/LDAP-Server übereinstimmt.

- **Versehentliche falsche Registrierungsänderung**

  Wenn Sie die LDAPS-bezogenen Schlüssel versehentlich aktualisiert haben, ohne **enable_ldaps.sh** zu verwenden, kann dies die Abhängigkeit der LDAPS-Komponenten beeinträchtigen.

- **LDAP-Datenverkehr wird nicht über SSL/TLS von Wireshark oder anderen Netzwerküberwachungstools verschlüsselt**

  Standardmäßig ist LDAPS deaktiviert. Führen Sie **/opt/Citrix/VDA/sbin/enable_ldaps.sh** aus, um es zu erzwingen.

- **Kein LDAPS-Datenverkehr von Wireshark oder anderen Netzwerküberwachungstools**

  LDAP-/LDAPS-Datenverkehr tritt auf, wenn die Linux VDA-Registrierung und die Gruppenrichtlinienauswertung erfolgen.

- **Fehler beim Überprüfen der LDAPS-Verfügbarkeit durch Ausführen von ldp connect auf dem AD-Server**

  Verwenden Sie den AD-FQDN anstelle der IP-Adresse.

- **Fehler beim Importieren des Stammzertifizierungsstellenzertifikats durch Ausführen des Skripts /opt/Citrix/VDA/sbin/enable_ldaps.sh**

  Geben Sie den vollständigen Pfad des CA-Zertifikats an und überprüfen Sie, ob das Stammzertifizierungsstellenzertifikat den richtigen Typ hat. Es sollte mit den meisten unterstützten Java Keytool-Typen kompatibel sein. Wenn es nicht in der Supportliste aufgeführt ist, können Sie den Typ zuerst konvertieren. Wir empfehlen das base64-kodierte PEM-Format, wenn Sie ein Problem mit dem Zertifikatsformat haben.

- **Fehler beim Anzeigen des Stammzertifizierungsstellenzertifikats mit Keytool -list**

  Wenn Sie LDAPS durch Ausführen von `/opt/Citrix/VDA/sbin/enable_ldaps.sh` aktivieren, wird das Zertifikat nach /etc/xdl/.keystore importiert, und das Kennwort wird zum Schutz des Keystores festgelegt. Wenn Sie das Kennwort vergessen, können Sie das Skript erneut ausführen, um einen Keystore zu erstellen.

Xauthority

Der Linux VDA unterstützt Umgebungen, die X11-Anzeigefunktionen (einschließlich `xterm` und `gvim`) für interaktives Remoting verwenden. Diese Funktion bietet einen Sicherheitsmechanismus, der für eine sichere Kommunikation zwischen XClient und XServer erforderlich ist.

Es gibt zwei Methoden, um die Berechtigung für diese sichere Kommunikation zu gewährleisten:

- **Xhost**. Standardmäßig erlaubt Xhost nur dem localhost XClient, mit dem XServer zu kommunizieren. Wenn Sie einem Remote-XClient den Zugriff auf den XServer erlauben möchten, muss der Xhost-Befehl ausgeführt werden, um die Berechtigung auf der spezifischen Maschine zu erteilen. Alternativ können Sie auch **xhost +** verwenden, um jedem XClient die Verbindung zum XServer zu ermöglichen.
- **Xauthority**. Die `.Xauthority`-Datei befindet sich im Home-Verzeichnis jedes Benutzers. Sie wird verwendet, um Anmeldeinformationen in Cookies zu speichern, die von xauth zur Authentifizierung des XServers verwendet werden. Wenn eine XServer-Instanz (Xorg) gestartet wird, wird das Cookie verwendet, um Verbindungen zu dieser spezifischen Anzeige zu authentifizieren.

Funktionsweise

Wenn Xorg startet, wird eine `.Xauthority`-Datei an Xorg übergeben. Diese `.Xauthority`-Datei enthält die folgenden Elemente:

- Anzeigennummer
- Remote-Anforderungsprotokoll
- Cookie-Nummer

Sie können diese Datei mit dem Befehl `xauth` durchsuchen. Zum Beispiel:

```
# xauth -f ~/.Xauthority



# > list



# > us01msip06:107  MIT-MAGIC-COOKIE-1  fb228d1b695729242616c5908f11624b
```

Wenn sich ein **XClient** remote mit Xorg verbindet, müssen zwei Voraussetzungen erfüllt sein:

- Setzen Sie die Umgebungsvariable **DISPLAY** auf den Remote-XServer.
- Rufen Sie die `.Xauthority`-Datei ab, die eine der Cookie-Nummern in Xorg enthält.

Xauthority konfigurieren

Um **Xauthority** auf dem Linux VDA für die Remote-X11-Anzeige zu aktivieren, müssen Sie die folgenden zwei Registrierungsschlüssel erstellen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"XauthEnabled" -d "0x00000001" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Xorg" -t "REG_DWORD" -v
"ListenTCP" -d "0x00000001" --force
```

Nach dem Aktivieren von **Xauthority** übergeben Sie die Datei `.Xauthority` manuell oder durch das Einbinden eines freigegebenen Home-Verzeichnisses an den **XClient**:

- Übergeben Sie die Datei `.Xauthority` manuell an den XClient

  Nach dem Starten einer ICA®-Sitzung generiert der Linux VDA die Datei `.Xauthority` für den XClient und speichert die Datei im Home-Verzeichnis des angemeldeten Benutzers. Sie können diese Datei `.Xauthority` auf den Remote-XClient-Computer kopieren und die Umgebungsvariablen **DISPLAY** und **XAUTHORITY** festlegen. `DISPLAY` ist die in der Datei `.Xauthority` gespeicherte Anzeigenummer und `XAUTHORITY` ist der Dateipfad von **Xauthority**. Ein Beispiel finden Sie im folgenden Befehl:

  ```
  export DISPLAY={Display number stored in the Xauthority file}



  export XAUTHORITY={the file path of .Xauthority}
  ```

  Hinweis:

> Wenn die Umgebungsvariable **XAUTHORITY** nicht festgelegt ist, wird standardmäßig die Datei `~/.Xauthority` verwendet.

- Übergeben Sie die Datei `.Xauthority` an den XClient, indem Sie ein freigegebenes Home-Verzeichnis einbinden

  Der bequemste Weg ist, ein freigegebenes Home-Verzeichnis für den angemeldeten Benutzer einzubinden. Wenn der Linux VDA eine ICA-Sitzung startet, wird die Datei `.Xauthority` im Home-Verzeichnis des angemeldeten Benutzers erstellt. Wenn dieses Home-Verzeichnis mit dem XClient geteilt wird, muss der Benutzer diese Datei `.Xauthority` nicht manuell an den XClient übertragen. Nachdem die Umgebungsvariablen **DISPLAY** und **XAUTHORITY** korrekt festgelegt wurden, wird die GUI automatisch auf dem XServer-Desktop angezeigt.

Problembehandlung

Wenn **Xauthority** nicht funktioniert, führen Sie die folgenden Schritte zur Fehlerbehebung aus:

1. Als Administrator mit Root-Berechtigung rufen Sie alle Xorg-Cookies ab:

   ```
   ps aux | grep -i xorg
   ```

   Dieser Befehl zeigt den Xorg-Prozess und die Parameter an, die beim Starten an Xorg übergeben wurden. Ein weiterer Parameter zeigt an, welche Datei `.Xauthority` verwendet wird. Zum Beispiel:

   ```
   /var/xdl/xauth/.Xauthority110
   ```

   Zeigen Sie die Cookies mit dem Befehl **Xauth** an:

   ```
   Xauth -f /var/xdl/xauth/.Xauthority110
   ```

2. Verwenden Sie den Befehl `Xauth`, um die in `~/.Xauthority` enthaltenen Cookies anzuzeigen. Bei gleicher Anzeigenummer müssen die angezeigten Cookies in den `.Xauthority`-Dateien von Xorg und XClient identisch sein.
3. Wenn die Cookies identisch sind, überprüfen Sie die Erreichbarkeit des Remote-Anzeigeports mithilfe der IP-Adresse des Linux VDA und der Anzeigenummer des veröffentlichten Desktops.

   Führen Sie beispielsweise den folgenden Befehl auf dem XClient-Computer aus:

```
telnet 10.158.11.11 6160
```

Die Portnummer ist die Summe aus 6000 + \<Anzeigenummer\>.

Wenn dieser Telnet-Vorgang fehlschlägt, blockiert möglicherweise die Firewall die Anforderung.

Authentifizierung

Dieser Abschnitt enthält die folgenden Themen:

- Authentifizierung mit Azure Active Directory
- Double-Hop-Single-Sign-On-Authentifizierung
- Federated Authentication Service
- Nicht-SSO-Authentifizierung
- Smartcards
- Zugriff durch nicht authentifizierte (anonyme) Benutzer

Authentifizierung mit Azure Active Directory

> **Hinweis:**

> Diese Funktion ist nur für in Azure gehostete VDAs verfügbar.

> Je nach Bedarf können Sie zwei Arten von Linux-VDAs in Azure bereitstellen:

- In Azure AD DS eingebundene VMs. Die VMs sind in eine von Azure Active Directory (AAD) Domain Services (DS) verwaltete Domäne eingebunden. Benutzer melden sich mit ihren Domänenanmeldeinformationen an den VMs an.
- Nicht in eine Domäne eingebundene VMs. Die VMs sind in den AAD-Identitätsdienst integriert, um die Benutzerauthentifizierung bereitzustellen. Benutzer melden sich mit ihren AAD-Anmeldeinformationen an den VMs an.

Weitere Informationen zu AAD DS und AAD finden Sie in diesem Microsoft-Artikel.

Dieser Artikel zeigt Ihnen, wie Sie den AAD-Identitätsdienst auf nicht in eine Domäne eingebundenen VDAs aktivieren und konfigurieren.

Unterstützte Distributionen

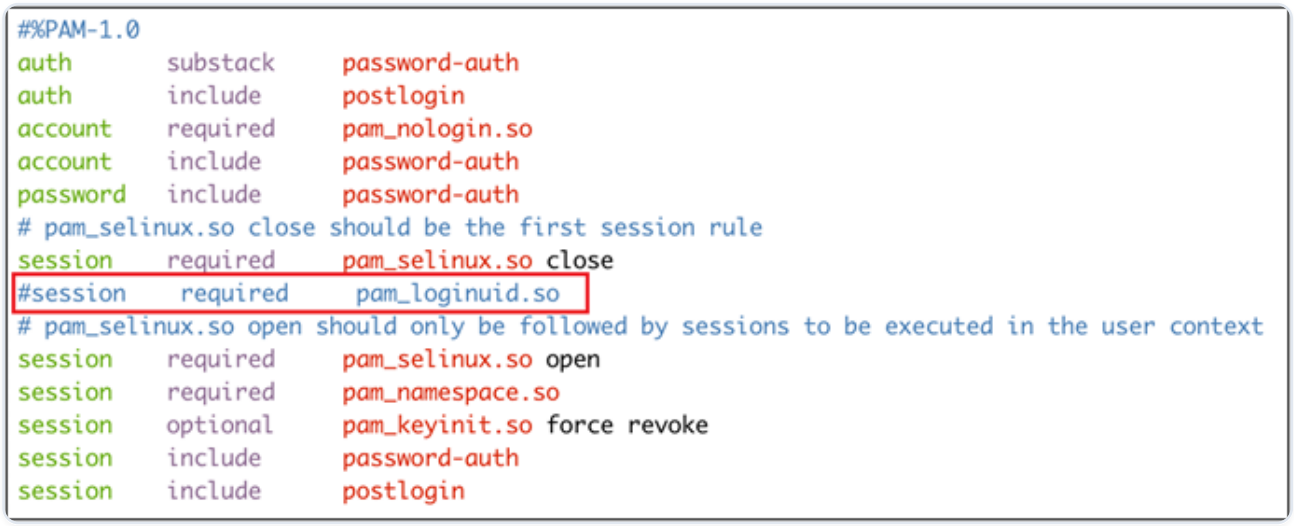
- Ubuntu 22.04, 20.04
- RHEL 8.8, 8.6, 7.9
- SUSE 15.4

Weitere Informationen finden Sie in diesem Microsoft-Artikel.

Bekannte Probleme und Problemumgehungen

Unter RHEL 7.9 kann PAM (Pluggable Authentication Module) `pam_loginuid.so` nach der AAD-Benutzerauthentifizierung `loginuid` nicht festlegen. Dieses Problem verhindert, dass AAD-Benutzer auf VDA-Sitzungen zugreifen können.

Um dieses Problem zu umgehen, kommentieren Sie in `/etc/pam.d/remote` die Zeile `Session required pam_loginuid.so` aus. Ein Beispiel finden Sie im folgenden Screenshot.



Schritt 1: Erstellen einer Vorlagen-VM im Azure-Portal

Erstellen Sie eine Vorlagen-VM und installieren Sie die Azure CLI auf der VM.

1. Erstellen Sie im Azure-Portal eine Vorlagen-VM. Stellen Sie sicher, dass Sie auf der Registerkarte **Verwaltung** die Option **Anmeldung mit Azure AD** auswählen, bevor Sie auf **Überprüfen + erstellen** klicken.

   Einstellung zum Aktivieren der Anmeldung mit AAD(/en-us/linux-virtual-delivery-agent/2308/media/aad-auth-create-vm.png)

2. Installieren Sie die Azure CLI auf der Vorlagen-VM. Weitere Informationen finden Sie in diesem Microsoft-Artikel.

Schritt 2: Masterimage auf der Vorlagen-VM vorbereiten

Um ein Masterimage vorzubereiten, folgen Sie **Schritt 3: Masterimage vorbereiten** in Linux-VDAs mit Machine Creation Services (MCS) erstellen.

Schritt 3: Vorlagen-VM in den nicht-domänengebundenen Modus versetzen

Nachdem Sie ein Masterimage erstellt haben, führen Sie die folgenden Schritte aus, um die VM in den nicht-domänengebundenen Modus zu versetzen:

1. Führen Sie das folgende Skript über die Eingabeaufforderung aus.

   ```
   Modify /var/xdl/mcs/mcs_util.sh
   ```

2. Suchen Sie `function read_non_domain_joined_info()`, und ändern Sie dann den Wert von `NonDomainJoined` in `2`. Ein Beispiel finden Sie im folgenden Codeblock.

   ```
   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

   ...

   }
   ```

3. Speichern Sie die Änderung.
4. Fahren Sie die Vorlagen-VM herunter.

Schritt 4: Linux-VMs aus der Vorlagen-VM erstellen

Nachdem die nicht-domänengebundene Vorlagen-VM bereit ist, führen Sie die folgenden Schritte aus, um VMs zu erstellen:

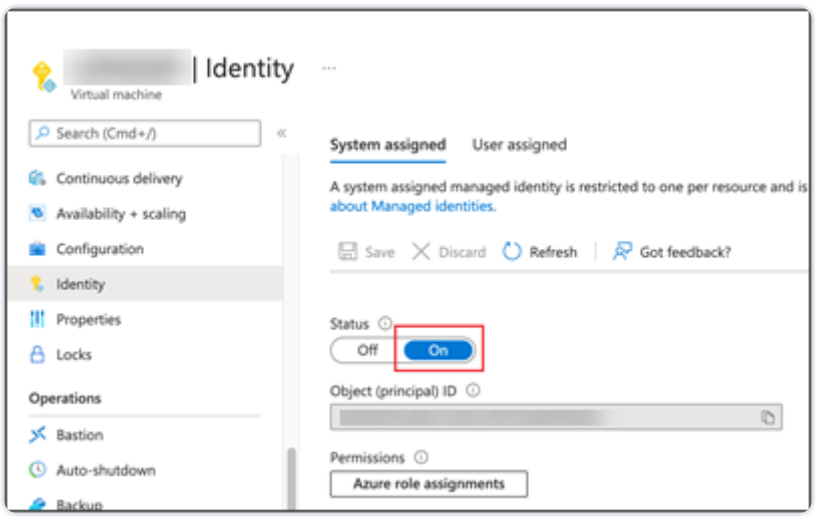
1. Melden Sie sich bei Citrix Cloud an.
2. Doppelklicken Sie auf Citrix DaaS™ und greifen Sie dann auf die Verwaltungskonsole für die vollständige Konfiguration zu.
3. Wählen Sie unter **Maschinenkataloge** die Verwendung von Machine Creation Services, um die Linux-VMs aus der Vorlagen-VM zu erstellen. Weitere Informationen finden Sie im Citrix DaaS-Artikel Nicht in Domäne eingebunden.

Schritt 5: AAD-Benutzerkonten den Linux-VMs zuweisen

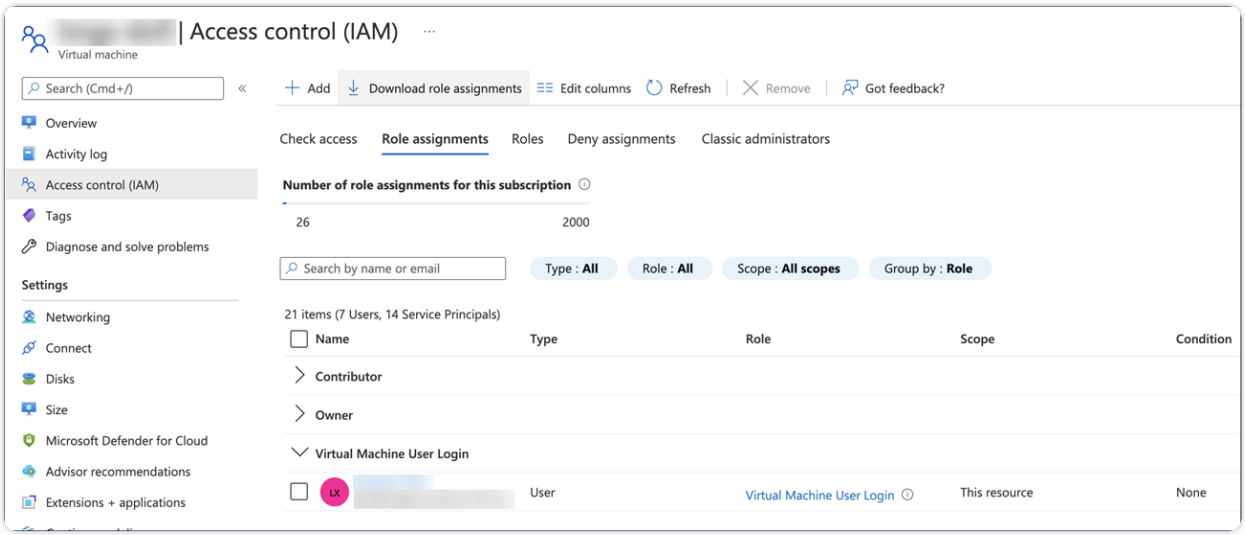
Nachdem Sie die nicht in Domäne eingebundenen VMs erstellt haben, weisen Sie ihnen AAD-Benutzerkonten zu.

Um einer VM AAD-Benutzerkonten zuzuweisen, führen Sie die folgenden Schritte aus:

1. Greifen Sie mit einem Administratorkonto auf die VM zu.
2. Aktivieren Sie auf der Registerkarte **Identität > System zugewiesen** die Option **Systemidentität**.



3. Suchen Sie auf der Registerkarte **Zugriffssteuerung (IAM) > Rollenzuweisungen** den Bereich **Anmeldung von VM-Benutzern**, und fügen Sie dann die AAD-Benutzerkonten nach Bedarf hinzu.



Anmeldung bei nicht in Domäne eingebundenen VDAs

Endbenutzer in Ihrer Organisation können sich auf zwei Arten bei einem nicht in Domäne eingebundenen VDA anmelden. Die detaillierten Schritte sind wie folgt:

1. Starten Sie die Workspace-App, und melden Sie sich dann beim Workspace an, indem Sie den AAD-Benutzernamen und das Kennwort eingeben. Die Workspace-Seite wird angezeigt.
2. Doppelklicken Sie auf einen nicht in Domäne eingebundenen Desktop. Die AAD-ANMELDESEITE wird angezeigt.

   Die Seite variiert je nach dem auf dem VDA eingestellten Anmeldemodus: Gerätecode oder AAD-Konto/Kennwort. Standardmäßig authentifizieren Linux-VDAs AAD-Benutzer im Gerätecode-Anmeldemodus wie folgt. Als Administrator können Sie den Anmeldemodus bei Bedarf auf AAD-Konto/Kennwort ändern. Detaillierte Schritte finden Sie im folgenden Abschnitt.



3. Melden Sie sich gemäß den Anweisungen auf dem Bildschirm auf eine der folgenden Arten bei der Desktopsitzung an:

   - Scannen Sie den QR-Code und geben Sie den Code ein.
   - Geben Sie den AAD-Benutzernamen und das Kennwort ein.

Wechseln Sie in den Anmeldemodus für AAD-Konto/Kennwort

Standardmäßig authentifizieren Linux-VDAs AAD-Benutzer mit Gerätecodes. Weitere Informationen finden Sie in diesem Microsoft-Artikel. Um den Anmeldemodus in *AAD-Konto/Kennwort* zu ändern, führen Sie die folgenden Schritte aus:

Führen Sie den folgenden Befehl auf dem VDA aus, suchen Sie den Schlüssel `AADAcctPwdAuthEnable` und ändern Sie seinen Wert in `0x00000001`.

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Services\CitrixBrokerAgent\WebSocket" -t
"REG_DWORD" -v "AADAcctPwdAuthEnable" -d "0x00000001" --force
```

Hinweis:

Diese Methode funktioniert nicht mit Microsoft-Konten oder Konten, bei denen die Zwei-Faktor-Authentifizierung aktiviert ist.

Double-Hop-Single-Sign-On-Authentifizierung

Benutzeranmeldeinformationen für den Zugriff auf einen StoreFront-Store können in das AuthManager-Modul der Citrix Workspace-App für Linux und des Citrix Receiver für Linux 13.10 injiziert werden. Nach der Injektion können Sie den Client verwenden, um aus einer Linux-Virtual-Desktop-Sitzung heraus auf virtuelle Desktops und Anwendungen zuzugreifen, ohne die Benutzeranmeldeinformationen ein zweites Mal einzugeben.

Hinweis:

Diese Funktion wird von der Citrix Workspace-App für Linux und dem Citrix Receiver für Linux 13.10 unterstützt.

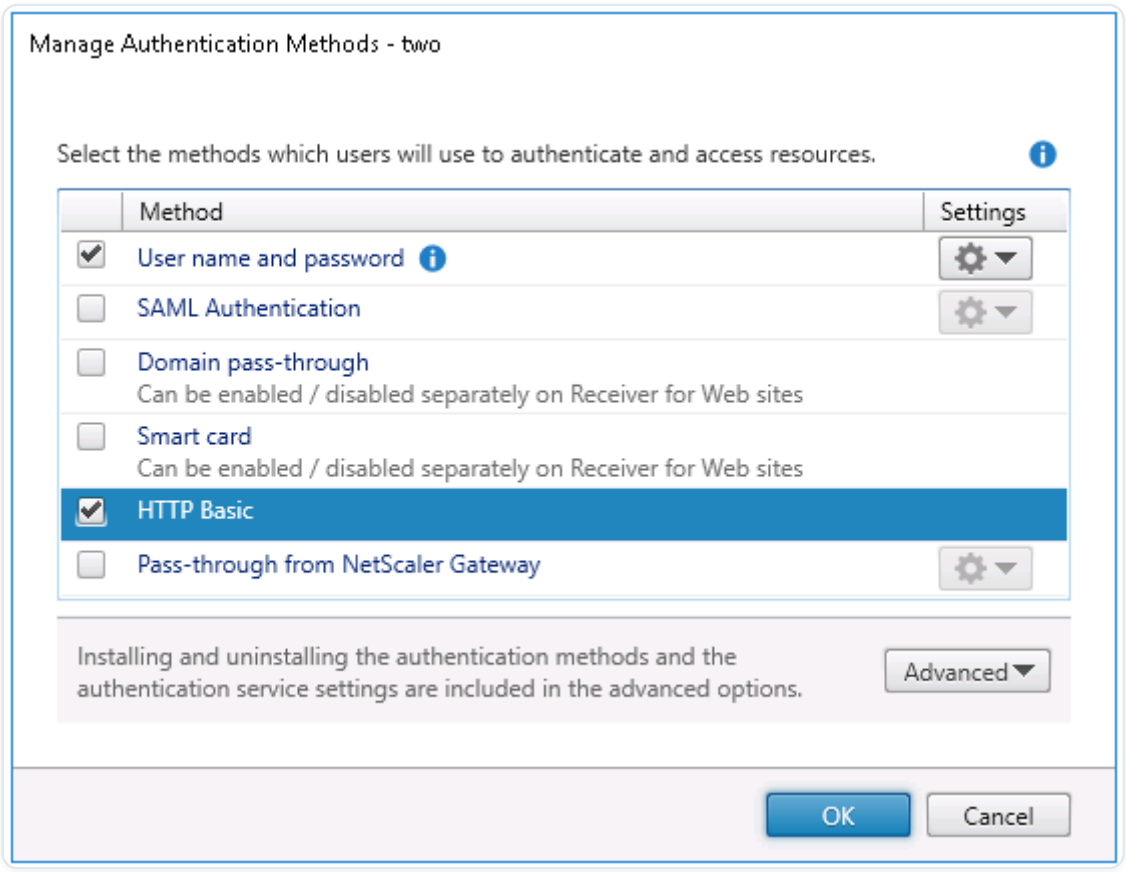
So aktivieren Sie die Funktion:

1. Installieren Sie auf dem Linux-VDA die Citrix Workspace-App für Linux oder den Citrix Receiver für Linux 13.10.

Laden Sie die App von der Citrix Downloadseite für die Citrix Workspace-App oder für Citrix Receiver herunter.

Der Standardinstallationspfad ist /opt/Citrix/ICAClient/. Wenn Sie die App in einem anderen Pfad installieren, legen Sie die Umgebungsvariable ICAROOT fest, um auf den tatsächlichen Installationspfad zu verweisen.

2. Fügen Sie in der Citrix StoreFront™-Verwaltungskonsole die **HTTP Basic**-Authentifizierungsmethode für den Ziel-Store hinzu.



3. Fügen Sie den folgenden Schlüssel zur AuthManager-Konfigurationsdatei ($ICAROOT/config/AuthManConfig.xml) hinzu, um die HTTP Basic-Authentifizierung zu ermöglichen:

```
<Protocols>

     <HTTPBasic>

         <Enabled>True</Enabled>

    </HTTPBasic>

</Protocols>
```

4. Führen Sie die folgenden Befehle aus, um das Stammzertifikat im angegebenen Verzeichnis zu installieren.

```
cp rootcert.pem $ICAROOT/keystore/cacerts/

$ICAROOT/util/ctx_rehash  $ICAROOT/keystore/cacerts/
```

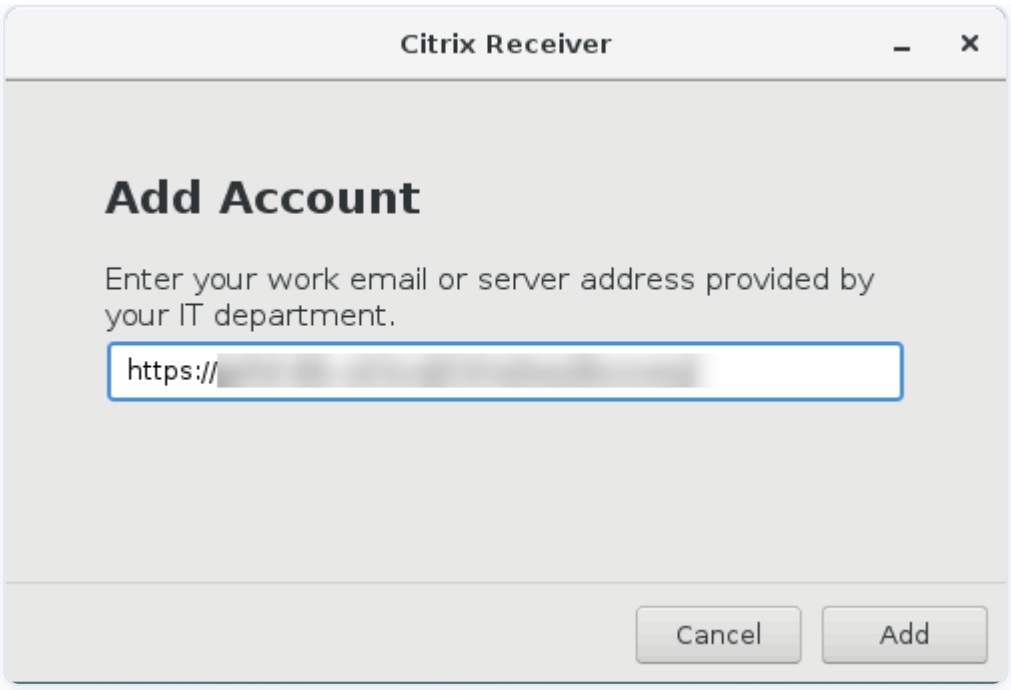
5. Führen Sie den folgenden Befehl aus, um die Funktion zu aktivieren:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix" -v "LurSsonEnabled" -d
"0x00000001"
```

6. Starten Sie eine Linux-Virtual-Desktop-Sitzung und starten Sie die Citrix Workspace-App für Linux oder den Citrix Receiver für Linux 13.10 innerhalb dieser Sitzung.

   Sie werden nach einem Store-Konto gefragt, wenn Sie die Citrix Workspace™-App zum ersten Mal starten. Später werden Sie automatisch bei dem zuvor angegebenen Store angemeldet.

> **Hinweis:**
>
> Geben Sie eine HTTPS-URL als Ihr Store-Konto ein.



Föderierter Authentifizierungsdienst

Sie können den Federated Authentication Service (FAS) verwenden, um Benutzer zu authentifizieren, die sich bei einem Linux VDA anmelden. Der Linux VDA verwendet dieselbe Windows-Umgebung wie der Windows VDA für die FAS-Anmeldefunktion. Informationen zum Konfigurieren der Windows-Umgebung für FAS finden Sie unter Federated Authentication Service. Dieser Artikel enthält zusätzliche Informationen speziell für den Linux VDA.

Hinweis:

- Der Linux VDA unterstützt die Richtlinie **In-session Behavior** nicht.
- Der Linux VDA verwendet kurze Verbindungen, um Daten mit FAS-Servern zu übertragen.
- Ab Release 2206 können Sie den FAS-Port auf der Linux VDA-Seite über CTX_XDL_FAS_LIST in der ctxsetup.sh anpassen. Weitere Informationen finden Sie im Linux VDA-Installationsartikel, basierend auf Ihrer Distribution.

Unterstützte Distributionen

FAS unterstützt nur eine begrenzte Anzahl von Linux-Distributionen und Domänenbeitrittsmethoden. Siehe folgende Matrix:

	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

	WINBIND	SSSD	CENTRIFY	PBIS
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

FAS auf dem Linux VDA konfigurieren

FAS-Unterstützung auf RHEL 8.x/9.x und Rocky Linux 8.x/9.x

FAS hängt vom pam_krb5-Modul ab, 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 Mehrfachsitzungs-Betriebssystemmodus bereitgestellt werden. Für FAS auf RHEL 8.x- und Rocky Linux 8.x-Maschinen, die im Einzelsitzungs-Betriebssystemmodus (VDI) bereitgestellt werden, können Sie die folgenden Schritte überspringen.

1. Laden Sie den pam_krb5-2.4.8-6-Quellcode von der folgenden Website herunter:

   `<https://centos.pkgs.org/7/centos-x86_64/pam_krb5-2.4.8-6.el7.x86_64.rpm.html>`.

2. Erstellen und installieren Sie das pam_krb5-Modul auf 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
```

3. Überprüfen Sie, ob pam_krb5.so unter /usr/lib64/security/ vorhanden ist.

```
ls -l /usr/lib64/security | grep pam_krb5
```

FAS-Server festlegen

Um FAS in einer neuen Linux VDA-Installation 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 FAS-Richtlinieneinstellung auf dem Domänen-GPO finden Sie unter Gruppenrichtlinie konfigurieren.

Da der Linux VDA die AD-Gruppenrichtlinie nicht unterstützt, können Sie stattdessen eine durch Semikolons getrennte Liste von FAS-Servern angeben. Beachten Sie Folgendes:

- Die Reihenfolge der Liste muss mit der in der AD-Gruppenrichtlinie konfigurierten Reihenfolge übereinstimmen.
- Wenn eine Serveradresse entfernt wird, füllen Sie das leere Feld mit der Textzeichenfolge **\<none\>** und behalten Sie den Index der Serveradressen unverändert bei.

Um eine vorhandene Linux VDA-Installation zu aktualisieren, können Sie `ctxsetup.sh` erneut ausführen, um die FAS-Server festzulegen. Alternativ können Sie die folgenden

Befehle ausführen, um die FAS-Server festzulegen und den `ctxvda`-Dienst neu zu starten, damit Ihre Einstellung wirksam wird.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "<Your-FAS-Server-List>" --force



service ctxjproxy restart



service ctxvda restart
```

Um die FAS-Server über `ctxreg` zu aktualisieren, führen Sie die folgenden Befehle aus:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -v "Addresses" -d "<Your-FAS-Server-List>"



service ctxjproxy restart



service ctxvda restart
```

Zertifikate installieren

Zur Überprüfung der Benutzerzertifikate installieren Sie das Stammzertifikat der Zertifizierungsstelle und alle Zwischenzertifikate auf dem VDA. Um beispielsweise das Stammzertifikat der Zertifizierungsstelle zu installieren, rufen Sie das AD-Stammzertifikat aus dem vorhergehenden Schritt **Abrufen des CA-Zertifikats von der Microsoft CA (auf AD)** ab oder laden Sie dessen DER-Format vom Stammzertifizierungsstellenserver `http://CA-SERVER/certsrv` herunter.

Hinweis:

> Die folgenden Befehle gelten auch für die Konfiguration eines Zwischenzertifikats.

> Konvertieren Sie eine DER-Datei (.crt, .cer, .der) in PEM, indem Sie einen Befehl ähnlich dem folgenden ausführen:

```
sudo openssl x509 -inform der -in root.cer -out root.pem
```

Installieren Sie dann das Stammzertifikat der Zertifizierungsstelle im Verzeichnis `openssl`, indem Sie einen Befehl ähnlich dem folgenden ausführen:

```
sudo cp root.pem /etc/pki/CA/certs/
```

> **Hinweis:**
>
> Legen Sie das Stammzertifikat der Zertifizierungsstelle nicht unter dem Pfad **/root** ab. Andernfalls hat FAS keine Leseberechtigung für das Stammzertifikat der Zertifizierungsstelle.

ctxfascfg.sh ausführen

Führen Sie das Skript ctxfascfg.sh aus, um FAS zu konfigurieren:

```
sudo /opt/Citrix/VDA/sbin/ctxfascfg.sh
```

Umgebungsvariablen werden hinzugefügt, damit `ctxfascfg.sh` im unbeaufsichtigten Modus ausgeführt werden kann:

- **CTX_FAS_ADINTEGRATIONWAY=winbind \| sssd \| centrify \| pbis**: Bezeichnet die Active Directory-Integrationsmethode, die `CTX_EASYINSTALL_ADINTEGRATIONWAY` entspricht, wenn `CTX_EASYINSTALL_ADINTEGRATIONWAY` angegeben ist. Wenn `CTX_EASYINSTALL_ADINTEGRATIONWAY` nicht angegeben ist, verwendet `CTX_FAS_ADINTEGRATIONWAY` seine eigene Werteinstellung.
- **CTX_FAS_CERT_PATH \=\<certificate path\>**: Gibt den vollständigen Pfad an, der das Stammzertifikat und alle Zwischenzertifikate speichert.
- **CTX_FAS_KDC_HOSTNAME**: Gibt den Hostnamen des Key Distribution Center (KDC) an, wenn Sie PBIS auswählen.

- **CTX_FAS_PKINIT_KDC_HOSTNAME**: Gibt den PKINIT KDC-Hostnamen an, der, sofern nicht anders angegeben, CTX_FAS_KDC_HOSTNAME entspricht. 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 richtige Active Directory-Integrationsmethode und geben Sie dann den korrekten Pfad der Zertifikate ein (z. B. `/etc/pki/CA/certs/`).

Das Skript installiert dann die Pakete krb5-pkinit und pam_krb5 und richtet die relevanten Konfigurationsdateien ein.

FAS deaktivieren

Um FAS auf dem Linux VDA zu deaktivieren, entfernen Sie alle FAS-Server aus der ConfDB mit den folgenden Befehlen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\Authentication\UserCredentialSer
vice" -t "REG_SZ" -v "Addresses" -d "" --force



service ctxjproxy restart



service ctxvda restart
```

Einschränkung

- FAS unterstützt die Bildschirmsperre noch nicht. Wenn Sie in einer Sitzung auf die Sperrtaste klicken, können Sie sich nicht erneut mit FAS bei der Sitzung anmelden.
- Diese Version unterstützt nur die gängigen FAS-Bereitstellungen, die im Artikel Architekturübersicht des Federated Authentication Service zusammengefasst sind, und beinhaltet nicht **Windows 10 Azure AD Join**.

Problembehandlung

Bevor Sie FAS beheben, stellen Sie sicher, dass der Linux VDA korrekt installiert und konfiguriert ist und eine Nicht-FAS-Sitzung erfolgreich im gemeinsamen Store mit Kennwortauthentifizierung gestartet werden kann.

Wenn Nicht-FAS-Sitzungen ordnungsgemäß funktionieren, setzen Sie die HDX-Protokollstufe der Klasse **Login** auf VERBOSE und die VDA-Protokollstufe auf TRACE. Informationen zum Aktivieren der Ablaufverfolgungsprotokollierung für den Linux VDA finden Sie im Knowledge Center-Artikel CTX220130.

Sie können auch das Linux-Tool **XDPing** verwenden, um häufige Konfigurationsprobleme in Ihrer Linux VDA-Umgebung zu überprüfen. Weitere Informationen finden Sie unter **XDPing**.

FAS-Server-Konfigurationsfehler

Das Starten einer Sitzung aus dem FAS-Store schlägt fehl.

Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie nach einer Fehlermeldung, die der folgenden ähnelt:

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: [Logon
Type] Federated Authentication Logon.



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: entry



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas: start
connect to server 0



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: connect_fas0: failed
to connect: Connection refused.



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: failed
to connect to server [0], please confirm if fas service list is well
configurated in condb



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_fas: exit,
43
```

```
2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: validate_user: failed
to validate fas credential



2021-01-28 01:42:16.164 <P26422:S4> citrix-ctxlogin: LoginBoxValidate:
failed validation of user 'user1@CTXDEV.LOCAL', INVALID_PARAMETER
```

LÖSUNG

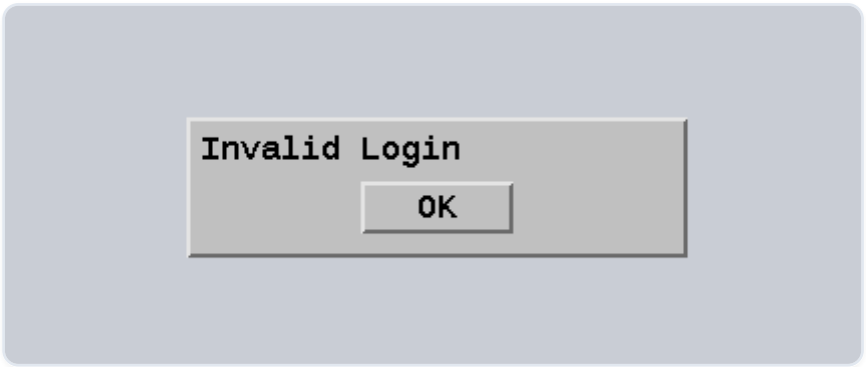
Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Citrix-Registrierungswert „HKEY_LOCAL_MACHINE\\SOFTWARE\\Citrix\\VirtualDesktopAgent\\Authentication\ \\UserCredentialService“ auf \<Your-FAS-Server-List\> gesetzt ist.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep "UserCredentialService"
```

Wenn die vorhandene Einstellung falsch ist, befolgen Sie den vorhergehenden Schritt FAS-Server einrichten, um sie erneut festzulegen.

Falsche CA-Zertifikatkonfiguration

Das Starten einer Sitzung aus dem FAS-Speicher schlägt fehl. Ein graues Fenster erscheint und verschwindet einige Sekunden später.



Überprüfen Sie **/var/log/xdl/hdx.log** und suchen Sie nach dem Fehlerprotokoll, das dem folgenden ähnelt:

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: entry
```

```
2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin: check_caller: current
process: pid [30656], name [/opt/Citrix/VDA/bin/ctxlogin]



2021-01-28 01:47:46.210 <P30656:S5> citrix-ctxlogin:
get_public_certificate: entry



2021-01-28 01:47:46.211 <P30656:S5> citrix-ctxlogin: query_fas: waiting
for response...



2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: query_fas: query to
server success



2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin:
get_public_certificate: exit



2021-01-28 01:47:46.270 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
input size 1888



2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: fas_base64_decode:
output size 1415



2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: get logon certificate success



2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin: cache_certificate:
cache certificate success
```

```
2021-01-28 01:47:46.271 <P30656:S5> citrix-ctxlogin:
get_logon_certificate: exit, 0



2021-01-28 01:47:48.060 <P30656:S5> citrix-ctxlogin: validate_user:
pam_authenticate err,can retry for user user1@CTXDEV.LOCAL
```

LÖSUNG

Stellen Sie sicher, dass Sie den vollständigen Pfad, der das Root-CA-Zertifikat und alle Zwischenzertifikate speichert, in `/etc/krb5.conf` korrekt festgelegt haben. Der vollständige Pfad ähnelt dem folgenden:

```
 [realms]


EXAMPLE.COM = {


    ......


    pkinit_anchors = DIR:/etc/pki/CA/certs/


    ......

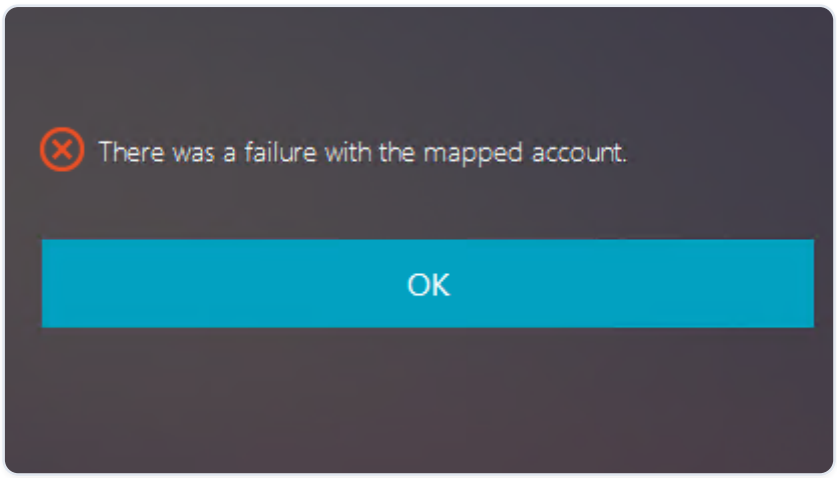

}
```

Wenn die vorhandene Einstellung falsch ist, befolgen Sie den vorhergehenden Schritt Zertifikate installieren, um sie erneut festzulegen.

Alternativ prüfen Sie, ob das Root-CA-Zertifikat gültig ist.

Fehler bei der Zuordnung von Schattenkonten

FAS ist über SAML-Authentifizierung konfiguriert. Der folgende Fehler kann auftreten, nachdem ein ADFS-Benutzer den Benutzernamen und das Kennwort auf der ADFS-Anmeldeseite eingegeben hat.



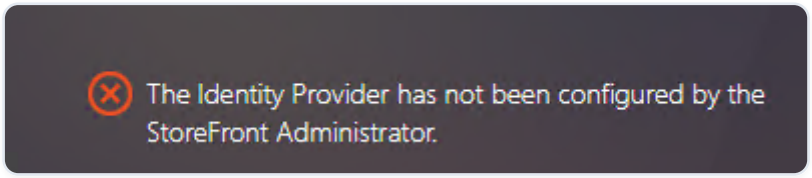
Dieser Fehler weist darauf hin, dass der ADFS-Benutzer erfolgreich überprüft wurde, aber kein Schattenbenutzer in AD konfiguriert ist.

LÖSUNG

Legen Sie das Schattenkonto in AD fest.

ADFS nicht konfiguriert

Der folgende Fehler tritt bei einem Anmeldeversuch im FAS-Speicher auf:



Das Problem tritt auf, wenn Sie den FAS-Speicher für die SAML-Authentifizierung konfigurieren, aber die ADFS-Bereitstellung fehlt.

LÖSUNG

Stellen Sie den ADFS IdP für den Federated Authentication Service bereit. Weitere Informationen finden Sie unter Bereitstellung von ADFS für den Federated Authentication Service.

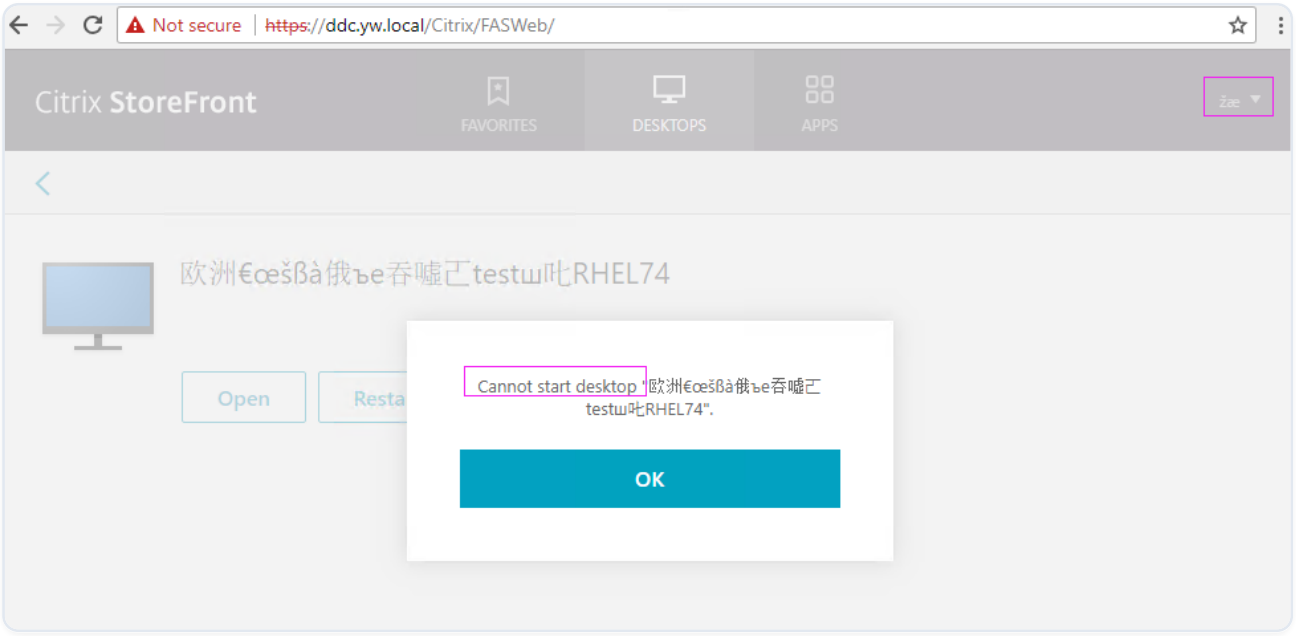
Verwandte Informationen

- Die gängigen FAS-Bereitstellungen sind im Artikel Architekturübersicht des Federated Authentication Service zusammengefasst.

- „How-to“-Artikel werden im Kapitel Erweiterte Konfiguration des Federated Authentication Service vorgestellt.

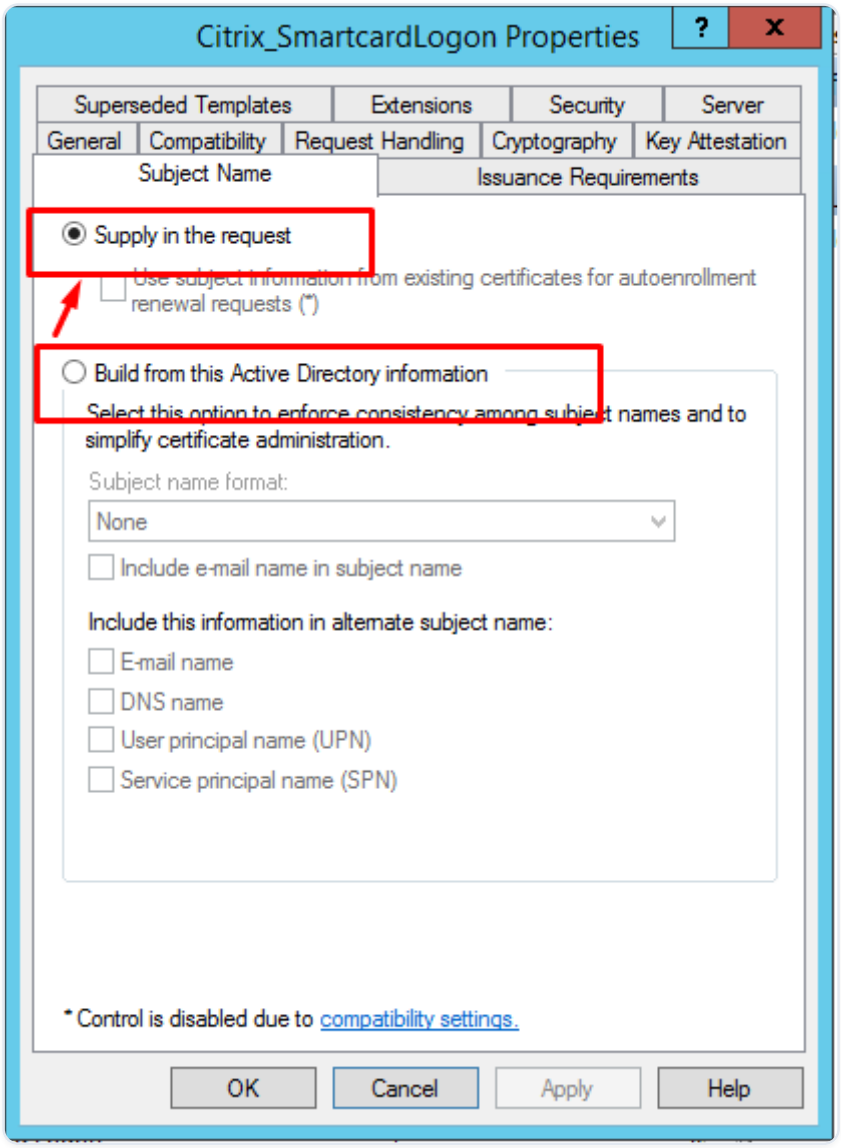
Bekannte Probleme

Wenn FAS verwendet wird, kann es zu Fehlern kommen, wenn Sie versuchen, eine veröffentlichte Desktop- oder App-Sitzung mit nicht-englischen Zeichen zu starten.



Problemumgehung

Klicken Sie im CA-Tool mit der rechten Maustaste auf **Vorlagen verwalten**, um die Vorlage **Citrix_SmartcardLogon** von **Aus diesen Active Directory-Informationen erstellen** in **In der Anforderung bereitstellen** zu ändern:



FIDO2 (Vorschau)

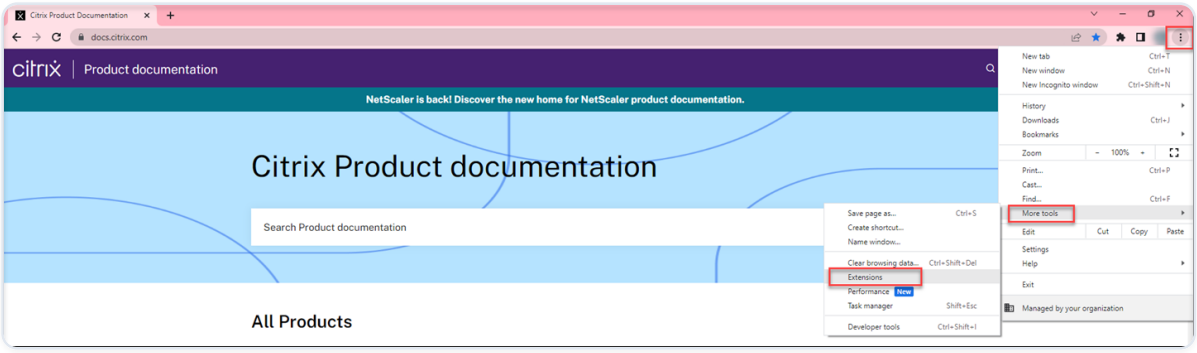
Sie können die FIDO2-Authentifizierung einrichten, um auf Websites zuzugreifen, die Google Chrome auf dem Linux VDA verwenden.

> **Hinweis:**
>
> Diese Funktion befindet sich in der Vorschau. Vorschaufunktionen sind möglicherweise nicht vollständig lokalisiert und werden für den Einsatz in Nicht-Produktionsumgebungen empfohlen. Der technische Support von Citrix unterstützt keine Probleme, die bei Vorschaufunktionen auftreten.

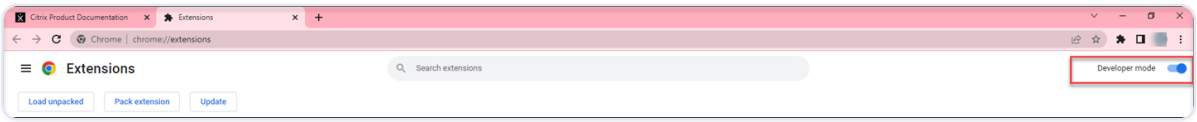
> Der Linux VDA unterstützt nur die Kombination von FIDO2 und Google Chrome.

Führen Sie die folgenden Schritte aus, um die FIDO2-Authentifizierung einzurichten:

1. Laden Sie das Citrix FIDO2-Erweiterungspaket herunter.
   a. Gehen Sie zur Downloadseite für Citrix Virtual Apps and Desktops.
   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 dessen Downloadseite zu öffnen.
   e. Laden Sie das Quellenpaket herunter.
   f. Entpacken Sie das Quellenpaket, um **FIDO2-JavaScript-Extensions.zip** zu finden.
   g. Entpacken Sie das FIDO2-Erweiterungspaket. Das FIDO2-Erweiterungsverzeichnis finden Sie unter **extensions > chrome > fido2**.
2. Fügen Sie die Citrix FIDO2-Erweiterung in Google Chrome hinzu:
   a. Öffnen Sie Google Chrome, das auf dem Linux VDA gehostet wird.
   b. Klicken Sie auf das Drei-Punkte-Menü rechts neben der Adressleiste und wählen Sie dann **Weitere Tools > Erweiterungen**.



   c. Aktivieren Sie den **Entwicklermodus**.



   d. Klicken Sie auf **Entpackte laden** und wählen Sie das Erweiterungsverzeichnis unter **extensions > chrome > fido2**.
3. Registrieren Sie auf der Website, für die Sie die FIDO2-Authentifizierung verwenden möchten, einen FIDO2-Sicherheitsschlüssel, um die FIDO2-Authentifizierung zu nutzen.
   a. Stecken Sie einen FIDO2-Sicherheitsschlüssel in den Client, auf dem die Citrix Workspace™-App installiert ist.

b. Aktivieren Sie die Multifaktor-Authentifizierung und fügen Sie FIDO2 als Authentifizierungsmethode hinzu.

Nachdem die FIDO2-Authentifizierung eingerichtet wurde, werden Sie aufgefordert, den Sicherheitsschlüssel zu berühren, um erfolgreich auf die Website zuzugreifen.

Nicht-SSO-Authentifizierung

Dieser Artikel enthält Anleitungen zum Aktivieren der Nicht-SSO-Authentifizierung auf dem Linux VDA.

Übersicht

Standardmäßig ist auf dem Linux VDA Single Sign-On (SSO) aktiviert. Benutzer melden sich mit einem Satz Anmeldeinformationen bei der Citrix Workspace™-App und bei VDA-Sitzungen an.

Damit sich Benutzer mit einem anderen Satz Anmeldeinformationen bei VDA-Sitzungen anmelden können, deaktivieren Sie SSO auf dem Linux VDA. Die folgende Tabelle listet Kombinationen von Benutzerauthentifizierungsmethoden auf, die in Nicht-SSO-Szenarien unterstützt werden.

CITRIX WORKSPACE-APP	VDA-SITZUNG
Benutzername	Benutzername
Smartcard	Benutzername
Benutzername	Smartcard
FAS	Benutzername
FAS	Smartcard

SSO deaktivieren

Führen Sie den folgenden Befehl auf Ihrem Linux VDA aus:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\WinStations\tcp" -t
"REG_DWORD" -v "fPromptForDifferentUser" -d "0x00000001" --force
```

Smartcards

Sie können eine Smartcard, die mit dem Clientgerät verbunden ist, zur Authentifizierung verwenden, wenn Sie sich bei einer virtuellen Linux-Desktopsitzung anmelden. Diese Funktion wird durch Smartcard-Umleitung über den virtuellen ICA® Smartcard-Kanal implementiert. Sie können die Smartcard auch innerhalb der Sitzung verwenden. Anwendungsfälle sind:

- Hinzufügen einer digitalen Signatur zu einem Dokument
- Verschlüsseln oder Entschlüsseln einer E-Mail
- Authentifizierung bei einer Website

Der Linux VDA verwendet für diese Funktion dieselbe Konfiguration wie der Windows VDA. Weitere Informationen finden Sie im Abschnitt Smartcard-Umgebung konfigurieren in diesem Artikel.

> **Hinweis:**
>
> Die Verwendung einer zugeordneten Smartcard innerhalb einer Linux VDA-Sitzung zur Anmeldung bei Citrix Gateway wird nicht unterstützt.

Voraussetzungen

Die Verfügbarkeit der Smartcard-Pass-Through-Authentifizierung hängt von den folgenden Bedingungen ab:

- Ihr Linux VDA ist auf 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

Nachdem Sie die Installation des VDA abgeschlossen haben, vergewissern Sie sich, dass Ihr VDA sich beim Delivery Controller™ registrieren kann und dass Sie die veröffentlichten Linux-Desktopsitzungen mit Windows-Anmeldeinformationen öffnen können.

- Es werden von OpenSC unterstützte Smartcards verwendet. Weitere Informationen finden Sie unter Stellen Sie sicher, dass OpenSC Ihre Smartcard unterstützt.
- Die Citrix Workspace™-App für Windows wird verwendet.

Stellen Sie sicher, dass OpenSC Ihre Smartcard unterstützt

OpenSC ist ein weit verbreiteter Smartcard-Treiber unter RHEL 7.4+. Als vollständig kompatibler Ersatz für CoolKey unterstützt OpenSC viele Arten von Smartcards (siehe Smartcard-Unterstützung in Red Hat Enterprise Linux).

In diesem Artikel wird die YubiKey-Smartcard als Beispiel zur Veranschaulichung der Konfiguration verwendet. YubiKey ist ein All-in-One-USB-CCID-PIV-Gerät, das einfach bei Amazon oder anderen Einzelhändlern erworben werden kann. Der OpenSC-Treiber unterstützt YubiKey.

Wenn Ihre Organisation eine andere, fortschrittlichere Smartcard benötigt, bereiten Sie eine physische Maschine mit einer unterstützten Linux-Distribution und installiertem OpenSC-Paket vor. Informationen zur OpenSC-Installation finden Sie unter Installieren des Smartcard-Treibers. Legen Sie Ihre Smartcard ein und führen Sie den folgenden Befehl aus, um zu überprüfen, ob OpenSC Ihre Smartcard unterstützt:

```
pkcs11-tool --module opensc-pkcs11.so --list-slots
```

Konfiguration

Stammzertifikat vorbereiten

Ein Stammzertifikat wird verwendet, um das Zertifikat auf der Smartcard zu überprüfen. Führen Sie die folgenden Schritte aus, um ein Stammzertifikat herunterzuladen und zu installieren.

1. Besorgen Sie sich ein Stammzertifikat im PEM-Format, typischerweise von Ihrem CA-Server.

   Sie können einen ähnlichen Befehl wie den folgenden ausführen, um eine DER-Datei (*.crt, *.cer, *.der) in PEM zu konvertieren. Im folgenden Befehlsbeispiel ist **certnew.cer** eine DER-Datei.

   ```
   openssl x509 -inform der -in certnew.cer -out certnew.pem
   ```

2. Installieren Sie das Stammzertifikat im Verzeichnis `openssl`. Die Datei **certnew.pem** wird als Beispiel verwendet.

   ```
   cp certnew.pem <path where you install the root certificate>
   ```

   Um einen Pfad für die Installation des Stammzertifikats zu erstellen, führen Sie `sudo mdkir -p <path where you install the root certificate>` aus.

Erstellen Sie das pam_krb5-Modul unter RHEL 8.x/9.x und Rocky Linux 8.x/9.x

Die Smartcard-Authentifizierung hängt vom pam_krb5-Modul ab, das unter RHEL 8.x und Rocky Linux 8.x als veraltet gilt. Die folgenden Schritte sind erforderlich, wenn Sie die Smartcard-Authentifizierung auf RHEL 8.x- und Rocky Linux 8.x-Maschinen verwenden möchten, die im Mehrfachsitzungs-OS-Modus bereitgestellt werden. Für die Smartcard-Authentifizierung auf RHEL 8.x- und Rocky Linux 8.x-Maschinen, die im Einzelsitzungs-OS-Modus (VDI) 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 pam_krb5-Modul 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
   ```

3. Stellen Sie sicher, dass pam_krb5.so unter /usr/lib64/security/ vorhanden ist.

   ```
   ls -l /usr/lib64/security | grep pam_krb5
   ```

Smartcard-Umgebung konfigurieren

Sie können das Skript ctxsmartlogon.sh verwenden, um die Smartcard-Umgebung zu konfigurieren, oder die Konfiguration manuell abschließen.

(OPTION 1) VERWENDEN SIE DAS SKRIPT CTXSMARTLOGON.SH, UM DIE SMARTCARD-UMGEBUNG ZU KONFIGURIEREN

> **Hinweis:**

> Das Skript ctxsmartlogon.sh fügt PKINIT-Informationen zum Standard-Realm hinzu. Sie können diese Einstellung über die Konfigurationsdatei **/etc/krb5.conf** ändern.

> Bevor Sie Smartcards zum ersten Mal verwenden, führen Sie das Skript ctxsmartlogon.sh aus, um die Smartcard-Umgebung zu konfigurieren.

> **Tipp:**

> Wenn Sie SSSD für den Domänenbeitritt verwendet haben, starten Sie den SSSD-Dienst neu, nachdem Sie ctxsmartlogon.sh ausgeführt haben.

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
```

Die Ergebnisse sehen wie folgt aus:

```
#************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] y
Step 2:Select the Active Directory integration method.
  Please select which Active Directory integration method to use:
     1: Winbind
     2: SSSD
     3: Centrify
  Select one of the above options (1-3)[1] 1
Step 3:Install dependent packages.
  Installing, please wait...
    [krb5-pkinit][pam_krb5] already installed.
    [pcsc-lite][pcsc-lite-ccid][pcsc-lite-libs][coolkey] already installed.
  Packages installed. [Success]
Step 4:Configure krb5.conf.
  Specify the path to the root CA (e.g., /etc/pki/CA/certs/root.pem):/etc/pki/CA/certs/root.pem
  /etc/krb5.conf configure successfully.
Step 5:Configure PAM files.
  Specify the path to the smart card PKCS11 driver (e.g., /usr/lib64/pkcs11/libcoolkeypk11.so):/usr/lib64/pkcs11/libcoolkeypk11.so
  /etc/pam.d/ctxfsc configure successfully.
  /etc/pam.d/smartcard-auth configure successfully.
ctxsmartlogon.sh executed successfully. SmartCard is ready.
```

Sie können Smartcards auch deaktivieren, indem Sie das Skript ctxsmartlogon.sh ausführen:

```
sudo /opt/Citrix/VDA/sbin/ctxsmartlogon.sh
```

Die Ergebnisse sehen wie folgt aus:

```
#************************************************************************
# ctxsmartlogon.sh sets up smart card logon for the Linux VDA, which
# includes automatic installation of the necessary packages and changes to
# the configuration files.
#
# Note:
# The ctxsmartlogon.sh adds pkinit information to the default realm. You can
# change this setting through the /etc/krb5.conf configuration file.
#************************************************************************
Step 1:Enable smart card logon.
  Do you want enable smart card logon? (y/n)[y] n
ctxsmartlogon.sh exit.
```

(OPTION 2) SMARTCARD-UMGEBUNG MANUELL KONFIGURIEREN

Der Linux VDA verwendet dieselbe Smartcard-Umgebung wie der Windows VDA. In dieser Umgebung müssen mehrere Komponenten konfiguriert werden, darunter der Domänencontroller, die Microsoft-Zertifizierungsstelle (CA), Internet Information Services, Citrix StoreFront und die Citrix Workspace-App. Informationen zur Konfiguration basierend auf der YubiKey-Smartcard finden Sie im Knowledge Center-Artikel CTX206156.

Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie sicher, dass:

- Sie alle Komponenten korrekt konfiguriert haben.

- Sie den privaten Schlüssel und das Benutzerzertifikat auf die Smartcard heruntergeladen haben.
- Sie sich erfolgreich mit der Smartcard am VDA anmelden können.

PC/SC Lite-Pakete installieren
PCSC Lite ist eine Implementierung der Personal Computer/Smart Card (PC/SC)-Spezifikation unter Linux. Es bietet eine Windows-Smartcard-Schnittstelle für die Kommunikation mit Smartcards und Lesegeräten. Die Smartcard-Umleitung im Linux VDA wird auf PC/SC-Ebene implementiert.

Führen Sie den folgenden Befehl aus, um die PC/SC Lite-Pakete zu installieren:

RHEL 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
```

Ubuntu 22.04, Ubuntu 20.04, Debian 11.3:

```
apt-get install -y libpcsclite1 libccid
```

Smartcard-Treiber installieren
OpenSC ist ein weit verbreiteter Smartcard-Treiber. Wenn OpenSC nicht installiert ist, führen Sie den folgenden Befehl aus, um es zu installieren:

RHEL 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x, RHEL 7/CentOS 7:

```
yum install opensc
```

Ubuntu 22.04, Ubuntu 20.04, Debian 11.3:

```
apt-get install -y opensc
```

Installieren Sie die PAM-Module für die Smartcard-Authentifizierung
Führen Sie den folgenden Befehl aus, um die Module pam_krb5 und krb5-pkinit zu installieren.

RHEL 7/CentOS 7:

```
yum install pam_krb5 krb5-pkinit
```

RHEL 9.2/9.0/8.x, Rocky Linux 9.2/9.0/8.x:

```
yum install krb5-pkinit
```

Ubuntu 22.04, Ubuntu 20.04:

```
apt-get install libpam-krb5 krb5-pkinit
```

Debian 11.3:

```
apt-get install -y libpam-krb5 krb5-pkinit
```

Das pam_krb5-Modul ist ein steckbares Authentifizierungsmodul. PAM-fähige Anwendungen können pam_krb5 verwenden, um Passwörter zu überprüfen und Ticket-Granting-Tickets vom Key Distribution Center (KDC) zu erhalten. Das krb5-pkinit-Modul enthält das PKINIT-Plug-in, das Clients ermöglicht, anfängliche Anmeldeinformationen vom KDC mithilfe eines privaten Schlüssels und eines Zertifikats zu erhalten.
Konfigurieren Sie das pam_krb5-Modul
Das pam_krb5-Modul interagiert mit dem KDC, um Kerberos-Tickets mithilfe von Zertifikaten auf der Smartcard zu erhalten. Um die pam_krb5-Authentifizierung in PAM zu aktivieren, führen Sie den folgenden Befehl aus:

```
authconfig --enablekrb5 --update
```

Fügen Sie in der Konfigurationsdatei **/etc/krb5.conf** PKINIT-Informationen entsprechend dem tatsächlichen Realm hinzu.

> **Hinweis:**

> Die Option **pkinit_cert_match** gibt Abgleichsregeln an, denen das Client-Zertifikat entsprechen muss, bevor es für den Versuch der PKINIT-Authentifizierung verwendet wird. Die Syntax der Abgleichsregeln lautet:

> **component-rule …**

wobei **relation-operator** entweder **&&** sein kann, was bedeutet, dass alle Komponentenregeln übereinstimmen müssen, oder **\|\|**, was bedeutet, dass nur eine Komponentenregel übereinstimmen muss.

Hier ist ein Beispiel für eine generische krb5.conf-Datei:

```
EXAMPLE.COM = {


    kdc = KDC.EXAMPLE.COM


    auth_to_local = RULE:[1:$1@$0]


    pkinit_anchors = FILE:<path where you install the root certificate>/
certnew.pem


    pkinit_kdc_hostname = KDC.EXAMPLE.COM


    pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature


    pkinit_eku_checking = kpServerAuth


 }
```

Die Konfigurationsdatei sieht nach dem Hinzufügen der PKINIT-Informationen wie folgt aus.

```
CTXDEV.LOCAL = {
     kdc = [redacted]
     auth_to_local = RULE:[1:$1@$0]
     pkinit_kdc_hostname = ctx-ad.ctxdev.local
     pkinit_anchors = FILE:/etc/pki/CA/certs/certnew.pem
     pkinit_eku_checking = kpServerAuth
     pkinit_cert_match = ||<EKU>msScLogin,<KU>digitalSignature
}
```

PAM-Authentifizierung konfigurieren

PAM-Konfigurationsdateien geben an, welche Module für die PAM-Authentifizierung verwendet werden. Um pam_krb5 als Authentifizierungsmodul hinzuzufügen, fügen Sie die folgende Zeile zur Datei **/etc/pam.d/smartcard-auth** hinzu:

`auth [success=done ignore=ignore default=die] pam_krb5.so preauth_options=X509_user_identity=PKCS11:<path to the pkcs11 driver>/opensc-pkcs11.so`

Die Konfigurationsdatei sieht nach der Änderung wie folgt aus, wenn SSSD verwendet wird.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=done ignore=ignore default=die]  pam_krb5.so preauth_opt=X509_user_identity=PKCS11:/usr/lib/x86_64-linux-gnu/pkcs11/opensc-pkcs11.so
auth        sufficient    pam_permit.so
auth        required      pam_deny.so

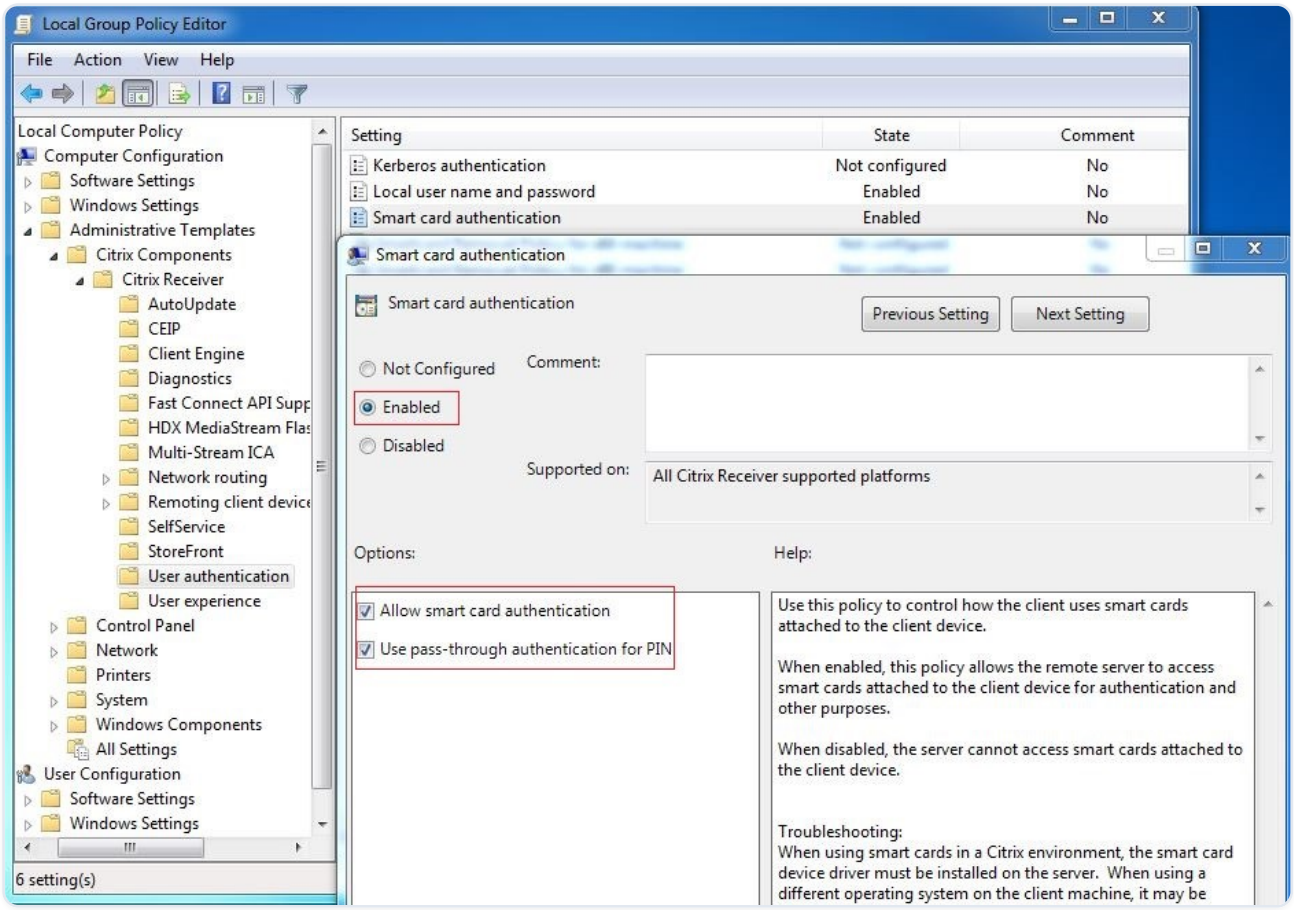
account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok auth_err=ignore user_unknown=ignore ignore=ignore]  pam_krb5.so
account     required      pam_permit.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
#session     optional      pam_oddjob_mkhomedir.so umask=0077
session     optional      pam_mkhomedir.so umask=0077
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
session     optional      pam_krb5.so
```

(Optional) Einmaliges Anmelden mit Smartcards

Einmaliges Anmelden (SSO) ist eine Citrix-Funktion, die die Pass-Through-Authentifizierung bei der Bereitstellung virtueller Desktops und Anwendungen implementiert. Diese Funktion reduziert die Häufigkeit, mit der Benutzer ihre PIN eingeben müssen. Um SSO mit dem Linux VDA zu verwenden, konfigurieren Sie die Citrix Workspace-App. Die Konfiguration ist dieselbe wie beim Windows VDA. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX133982.

Aktivieren Sie die Smartcard-Authentifizierung wie folgt, wenn Sie die Gruppenrichtlinie in der Citrix Workspace-App konfigurieren.



Schnelle Smartcard-Anmeldung

Die schnelle Smartcard ist eine Verbesserung gegenüber der bestehenden HDX PC/SC-basierten Smartcard-Umleitung. Sie verbessert die Leistung, wenn Smartcards in WAN-Umgebungen mit hoher Latenz verwendet werden. Weitere Informationen finden Sie unter Smartcards.

Der Linux VDA unterstützt schnelle Smartcards in den folgenden Versionen der Citrix Workspace-App:

- Citrix Receiver für Windows 4.12
- Citrix Workspace app 1808 für Windows und höher

SCHNELLE SMARTCARD-ANMELDUNG AUF DEM CLIENT AKTIVIEREN

Die schnelle Smartcard-Anmeldung ist standardmäßig auf dem VDA aktiviert und auf dem Client standardmäßig deaktiviert. Um die schnelle Smartcard-Anmeldung auf dem Client zu aktivieren, fügen Sie den folgenden Parameter in die Datei default.ica der zugehörigen StoreFront-Site ein:

```
[WFClient]

SmartCardCryptographicRedirection=On
```

SCHNELLE SMARTCARD-ANMELDUNG AUF DEM CLIENT DEAKTIVIEREN

Um die schnelle Smartcard-Anmeldung auf dem Client zu deaktivieren, entfernen Sie den Parameter **SmartCardCryptographicRedirection** aus der Datei default.ica der zugehörigen StoreFront-Site.

XDPing ausführen

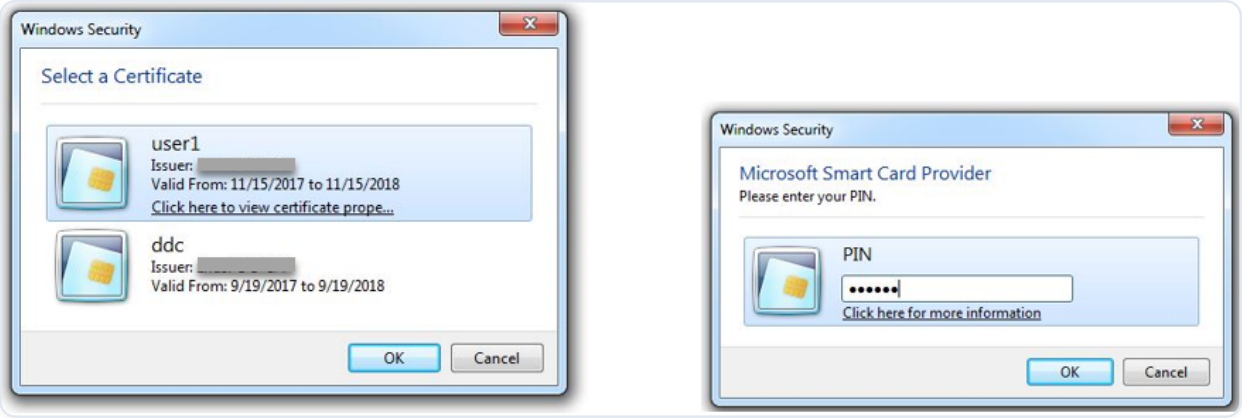
Nachdem Sie die vorhergehenden Schritte abgeschlossen haben, können Sie das Linux-Tool **XDPing** verwenden, um nach häufigen Konfigurationsproblemen zu suchen, die in Ihrer Linux-VDA-Umgebung auftreten können. Weitere Informationen finden Sie unter XDPing.

Verwendung

Anmeldung am Linux VDA mit einer Smartcard

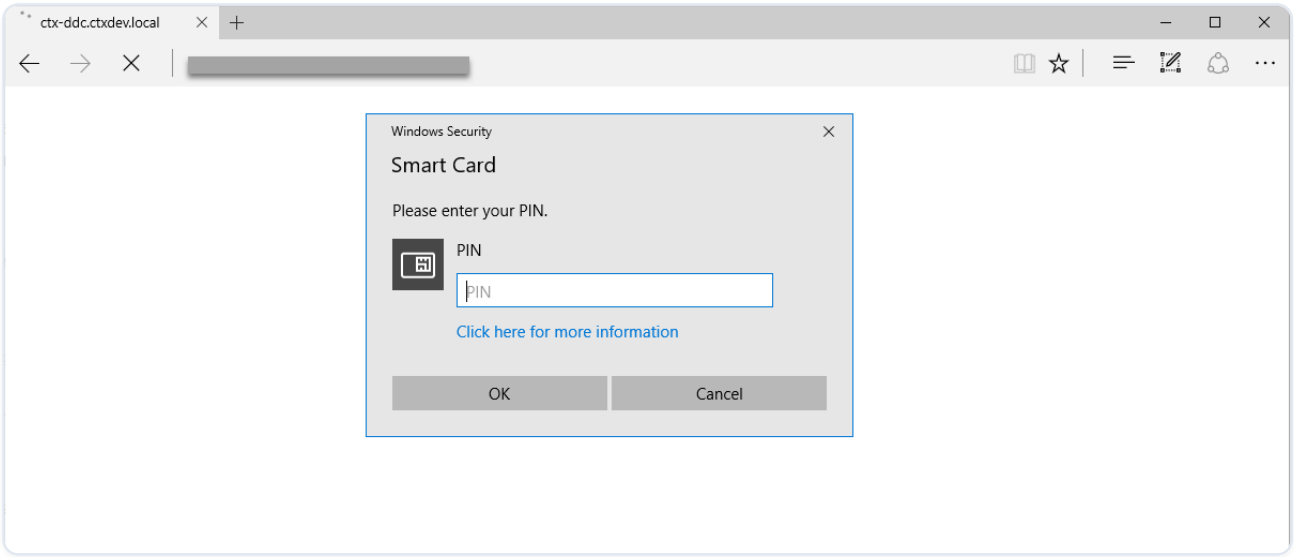
Sie können eine Smartcard verwenden, um sich sowohl in SSO- als auch in Nicht-SSO-Szenarien am Linux VDA anzumelden.

- Im SSO-Szenario werden Sie automatisch bei StoreFront™ angemeldet, indem das zwischengespeicherte Smartcard-Zertifikat und die PIN verwendet werden. Wenn Sie eine virtuelle Linux-Desktopsitzung in StoreFront starten, wird die PIN zur Smartcard-Authentifizierung an den Linux VDA übergeben.
- Im Nicht-SSO-Szenario werden Sie aufgefordert, ein Zertifikat auszuwählen und eine PIN einzugeben, um sich bei StoreFront anzumelden.



Wenn Sie eine virtuelle Linux-Desktopsitzung in StoreFront starten, wird ein Dialogfeld für die Anmeldung am Linux VDA wie folgt angezeigt. Der Benutzername wird aus dem Zertifikat auf der Smartcard extrahiert, und Sie müssen die PIN erneut für die Anmeldeauthentifizierung eingeben.

Dieses Verhalten ist dasselbe wie beim Windows VDA.



Wiederverbindung mit einer Sitzung mithilfe einer Smartcard

Um die Verbindung zu einer Sitzung wiederherzustellen, stellen Sie sicher, dass die Smartcard mit dem Clientgerät verbunden ist. Andernfalls wird auf der Linux-VDA-Seite ein graues Caching-Fenster angezeigt und schnell wieder geschlossen, da die erneute Authentifizierung ohne angeschlossene Smartcard fehlschlägt. In diesem Fall wird keine weitere Aufforderung angezeigt, die Sie daran erinnert, die Smartcard anzuschließen.

Auf der StoreFront-Seite hingegen kann die StoreFront-Weboberfläche eine Warnung wie folgt anzeigen, wenn keine Smartcard angeschlossen ist, wenn Sie die Verbindung zu einer Sitzung wiederherstellen:



Einschränkung

Unterstützung für eingeschränkte Linux-Distributionen und AD-Integrationsmethoden

- Die Smartcard-Pass-Through-Authentifizierung unterstützt eingeschränkte Linux-Distributionen und AD-Integrationsmethoden. Siehe folgende Matrix:

	WINBIND	SSSD	CENTRIFY
Debian 11.3	Ja	Ja	Ja

	WINBIND	SSSD	CENTRIFY
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

Smartcard-Entfernungsrichtlinie

Der Linux VDA verwendet nur das Standardverhalten für die Smartcard-Entfernung. Wenn Sie die Smartcard nach erfolgreicher Anmeldung am Linux VDA entfernen, bleibt die Sitzung verbunden und der Sitzungsbildschirm wird nicht gesperrt.

Unterstützung für andere Smartcards und die PKCS#11-Bibliothek

Citrix bietet eine generische Smartcard-Umleitungslösung. Obwohl nur die OpenSC-Smartcard auf unserer Supportliste aufgeführt ist, können Sie versuchen, andere Smartcards und die PKCS#11-Bibliothek zu verwenden. Um zu Ihrer spezifischen Smartcard oder der PKCS#11-Bibliothek zu wechseln:

1. Ersetzen Sie alle `opensc-pkcs11.so`-Instanzen durch Ihre PKCS#11-Bibliothek.
2. Um den Pfad Ihrer PKCS#11-Bibliothek in der Registrierung festzulegen, führen Sie den folgenden Befehl aus:

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\Scard" -v
   "PKCS11LibPath" -d "PATH"
   ```

   wobei **PATH** auf Ihre PKCS#11-Bibliothek verweist, z. B. /usr/lib64/pkcs11/opensc-pkcs11.so
3. Deaktivieren Sie die schnelle Smartcard-Anmeldung auf dem Client.

Zugriff durch nicht authentifizierte (anonyme) Benutzer

Sie können Benutzern den Zugriff auf Anwendungen und Desktops ermöglichen, ohne Anmeldeinformationen bei StoreFront™ oder der Citrix Workspace™-App vorlegen zu müssen. Um nicht authentifizierten Benutzern Zugriff zu gewähren, müssen Sie einen nicht authentifizierten StoreFront-Store haben und den Zugriff für nicht authentifizierte Benutzer in einer Bereitstellungsgruppe aktivieren.

> **Hinweis:**
>
> Der Zugriff durch nicht authentifizierte Benutzer wird nur für in die Domäne eingebundene VDAs unterstützt.
>
> Das Sitzungs-Prelaunch wird für nicht authentifizierte Benutzer nicht unterstützt. Das Sitzungs-Prelaunch wird auch in der Citrix Workspace-App für Android nicht unterstützt.

Nicht authentifizierten StoreFront-Store erstellen

1. Wählen Sie den Knoten **Stores** im linken Bereich der Citrix StoreFront-Verwaltungskonsole aus und klicken Sie im Bereich **Aktionen** auf **Store erstellen**.
2. Geben Sie auf der Seite **Store-Name** einen Namen für Ihren Store an, wählen Sie **Nur nicht authentifizierten (anonymen) Benutzern den Zugriff auf diesen Store erlauben** und klicken Sie auf **Weiter**.

Weitere Informationen finden Sie unter Nicht authentifizierten Store erstellen.

Zugriff für nicht authentifizierte Benutzer in einer Bereitstellungsgruppe aktivieren

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen, die aus einem oder mehreren Maschinenkatalogen ausgewählt wurden. Wenn Sie festlegen, wer die Anwendungen und Desktops in einer Bereitstellungsgruppe verwenden darf, können Sie nicht authentifizierten Benutzern Zugriff gewähren. Weitere Informationen finden Sie unter Bereitstellungsgruppen erstellen.

Leerlauf-Timeout für nicht authentifizierte Benutzersitzungen festlegen

Nicht authentifizierte Benutzersitzungen haben ein Standard-Leerlauf-Timeout von 10 Minuten und werden automatisch abgemeldet, wenn der Client die Verbindung trennt. Sie können ein benutzerdefiniertes Leerlauf-Timeout über die Registrierungseinstellung

AnonymousUserIdleTime konfigurieren. Um beispielsweise ein benutzerdefiniertes Leerlauf-Timeout von fünf Minuten festzulegen, führen Sie den folgenden Befehl aus:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v AnonymousUserIdleTime
 -d 0x00000005
```

Maximale Anzahl nicht authentifizierter Benutzer festlegen

Um die maximale Anzahl nicht authentifizierter Benutzer festzulegen, verwenden Sie den Registrierungsschlüssel **MaxAnonymousUserNumber**. Diese Einstellung begrenzt die Anzahl der nicht authentifizierten Benutzersitzungen, die gleichzeitig auf einem einzelnen Linux-VDA ausgeführt werden. Verwenden Sie das Tool **ctxreg**, um diese Registrierungseinstellung zu konfigurieren. Um den Wert beispielsweise auf 32 festzulegen, führen Sie den folgenden Befehl aus:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
 "HKLM\System\CurrentControlSet\Control\Citrix"  -v MaxAnonymousUserNumber
 -d  0x00000020
```

Wichtig:

Begrenzen Sie die Anzahl der nicht authentifizierten Benutzersitzungen. Zu viele gleichzeitig gestartete Sitzungen können Probleme auf dem VDA verursachen, einschließlich eines Mangels an verfügbarem Speicher.

Problembehandlung

Beachten Sie Folgendes bei der Konfiguration von nicht authentifizierten Benutzersitzungen:

- **Fehler beim Anmelden an einer nicht authentifizierten Benutzersitzung**.

Stellen Sie sicher, dass die Registrierung aktualisiert wurde und Folgendes enthält (auf 0 gesetzt):

```
sudo /opt/Citrix/VDA/bin/ctxreg read –k
"HKLM\System\CurrentControlSet\Control\Citrix" –v MaxAnonymousUserNumber
```

Stellen Sie sicher, dass der Dienst **ncsd** ausgeführt wird und für die Aktivierung des **passwd**-Caches konfiguriert ist:

```
ps  uax | grep nscd

cat /etc/nscd.conf | grep 'passwd' | grep 'enable-cache'
```

Setzen Sie die **passwd**-Cache-Variable auf **no**, falls sie aktiviert ist, und starten Sie dann den Dienst **ncsd** neu. Möglicherweise müssen Sie den Linux VDA nach dieser Konfigurationsänderung neu installieren.

- **Die Schaltfläche zum Sperren des Bildschirms wird in einer nicht authentifizierten Benutzersitzung mit KDE angezeigt**.

Die Schaltfläche und das Menü zum Sperren des Bildschirms sind in einer nicht authentifizierten Benutzersitzung standardmäßig deaktiviert. Sie können jedoch weiterhin in KDE angezeigt werden. Um in KDE die Schaltfläche und das Menü zum Sperren des Bildschirms für einen bestimmten Benutzer zu deaktivieren, fügen Sie die folgenden Zeilen zur Konfigurationsdatei **$Home/.kde/share/config/kdeglobals** hinzu. Beispiel:

```
[KDE Action Restrictions]

action/lock_screen=false
```

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.

Um dieses Problem zu beheben, ändern Sie die systemweite `kdeglobals`-Datei, um das Tag `[$i]` im Abschnitt `[KDE Action Restrictions]` zu entfernen, oder verwenden Sie direkt die systemweite Konfiguration, um die Schaltfläche und das Menü zum Sperren des Bildschirms zu deaktivieren. Details zur KDE-Konfiguration finden Sie auf der KDE System Administration/Kiosk/Keys-Seite.

Datei

Dieser Abschnitt enthält die folgenden Themen:

- Dateikopieren und -einfügen

- Dateiübertragung

Dateien kopieren und einfügen

Benutzer können Dateien zwischen einer Sitzung und einem lokalen Client mithilfe des Rechtsklickmenüs oder Tastenkombinationen kopieren und einfügen. Diese Funktion erfordert Citrix Virtual Apps and Desktops™ 2006 oder höher und Citrix Workspace™ App 1903 oder höher für Windows.

Um Dateien erfolgreich zu kopieren und einzufügen, stellen Sie sicher, dass:

- Die maximale Anzahl von Dateien 20 nicht überschreitet.
- Die maximale Dateigröße 200 MB nicht überschreitet.
- Der Nautilus-Dateimanager auf dem Computer verfügbar ist, auf dem Sie den Linux VDA installiert haben.

Unterstützte Linux-Distributionen

Die **Funktion zum Kopieren und Einfügen von Dateien** ist für alle Linux-Distributionen verfügbar, die der Linux VDA unterstützt.

Relevante Richtlinien

Die folgenden Zwischenablage-Richtlinien sind für die Konfiguration der Funktion relevant. Weitere Informationen zu den Zwischenablage-Richtlinien finden Sie in der Richtlinien-Supportliste.

- Client-Zwischenablagenumleitung
- Zwischenablage-Auswahlaktualisierungsmodus
- Primärer Auswahlaktualisierungsmodus

> **Hinweis:**
>
> Um die Funktion zum Kopieren und Einfügen von Dateien zu deaktivieren, setzen Sie die Richtlinie **Client-Zwischenablageumleitung** in Citrix Studio auf **Verboten**.

Einschränkungen

- Ausschneiden wird nicht unterstützt. Anfragen zum Ausschneiden einer Datei werden als Kopiervorgänge behandelt.
- Drag & Drop wird nicht unterstützt.

- Das Kopieren von Verzeichnissen wird nicht unterstützt.
- Das Kopieren und Einfügen von Dateien muss sequenziell erfolgen. Erst nachdem die vorherige Datei erfolgreich kopiert und eingefügt wurde, kann die nächste Datei kopiert werden.

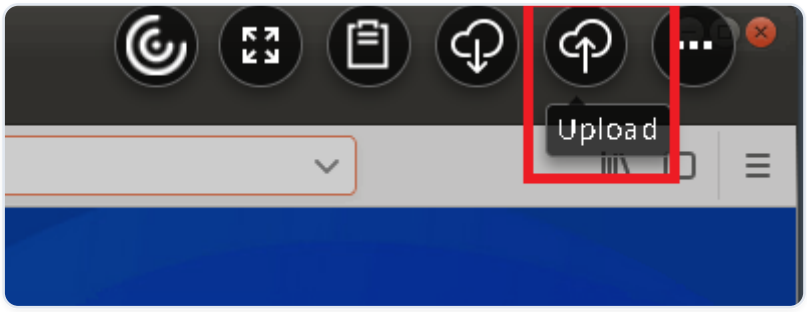
Dateiübertragung

Die Dateiübertragung wird zwischen dem Linux VDA und dem Clientgerät unterstützt. Diese Funktion ist verfügbar, wenn das Clientgerät einen Webbrowser ausführt, 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:**

> Die Dateiübertragung ist für die Citrix Workspace-App für HTML5 und für Chrome verfügbar.

> Innerhalb veröffentlichter App- und Desktopsitzungen ermöglicht die Dateiübertragung das Hoch- und Herunterladen von Dateien zwischen dem Linux VDA und dem Clientgerät. Um Dateien vom Clientgerät auf den Linux VDA hochzuladen, klicken Sie auf das Symbol **Hochladen** in der Symbolleiste der Citrix Workspace-App und wählen Sie die gewünschte Datei in den Dateidialogen aus. Um Dateien vom Linux VDA auf das Clientgerät herunterzuladen, klicken Sie auf das Symbol **Herunterladen**. Sie können Dateien während des Hoch- oder Herunterladens hinzufügen. Sie können bis zu 100 Dateien gleichzeitig übertragen.



> **Hinweis:**

> Um Dateien zwischen dem Linux VDA und dem Clientgerät hoch- und herunterzuladen, aktivieren Sie die Symbolleiste der Citrix Workspace-App.

> Sie können eine Version der Citrix Workspace-App verwenden, mit der Sie Dateien per Drag & Drop verschieben können.

> Der Autodownload ist eine Erweiterung für die Dateiübertragung. Dateien, die Sie in das Verzeichnis **Auf meinem Gerät speichern** auf dem VDA herunterladen oder verschieben, werden automatisch auf das Clientgerät übertragen.

> **Hinweis:**

> Für den Autodownload müssen die Richtlinien **Dateiübertragung zwischen Desktop und Client zulassen** und **Datei vom Desktop herunterladen** auf **Zugelassen** festgelegt sein.

> Hier sind einige Anwendungsfälle für den Autodownload:

- Dateien in **Auf meinem Gerät speichern** herunterladen

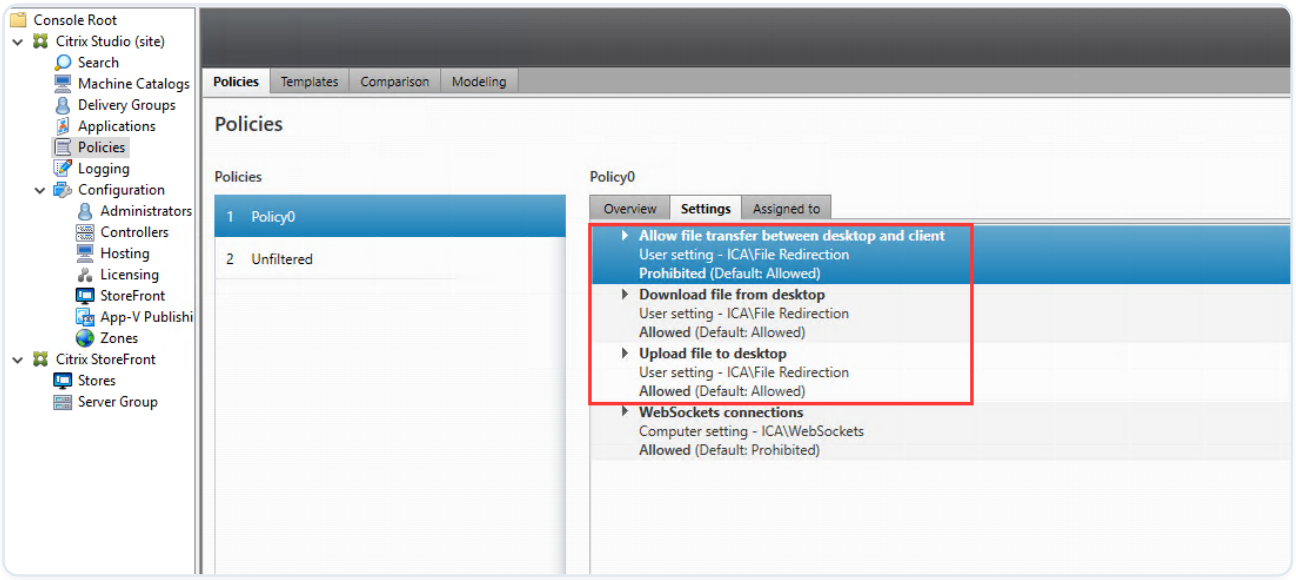
  Innerhalb veröffentlichter Desktop- und Webbrowser-App-Sitzungen können Dateien, die Sie von Websites herunterladen, im Verzeichnis **Auf meinem Gerät speichern** auf dem VDA zur automatischen Übertragung auf das Clientgerät gespeichert werden. Um den Autodownload zu erreichen, legen Sie das Standard-Downloadverzeichnis des In-Session-Webbrowsers auf **Auf meinem Gerät speichern** fest und ein lokales Downloadverzeichnis im Webbrowser, der Ihre Citrix Workspace-App für HTML5 oder für Chrome ausführt.

- Dateien in **Auf meinem Gerät speichern** verschieben oder kopieren

  Innerhalb veröffentlichter Desktopsitzungen wählen Sie die Zieldateien aus und verschieben oder kopieren sie in das Verzeichnis **Auf meinem Gerät speichern**, damit sie auf dem Clientgerät verfügbar sind.

Richtlinien für die Dateiübertragung

Sie können Citrix Studio verwenden, um die Richtlinien für die Dateiübertragung festzulegen. Standardmäßig ist die Dateiübertragung aktiviert.



Richtlinienbeschreibungen:

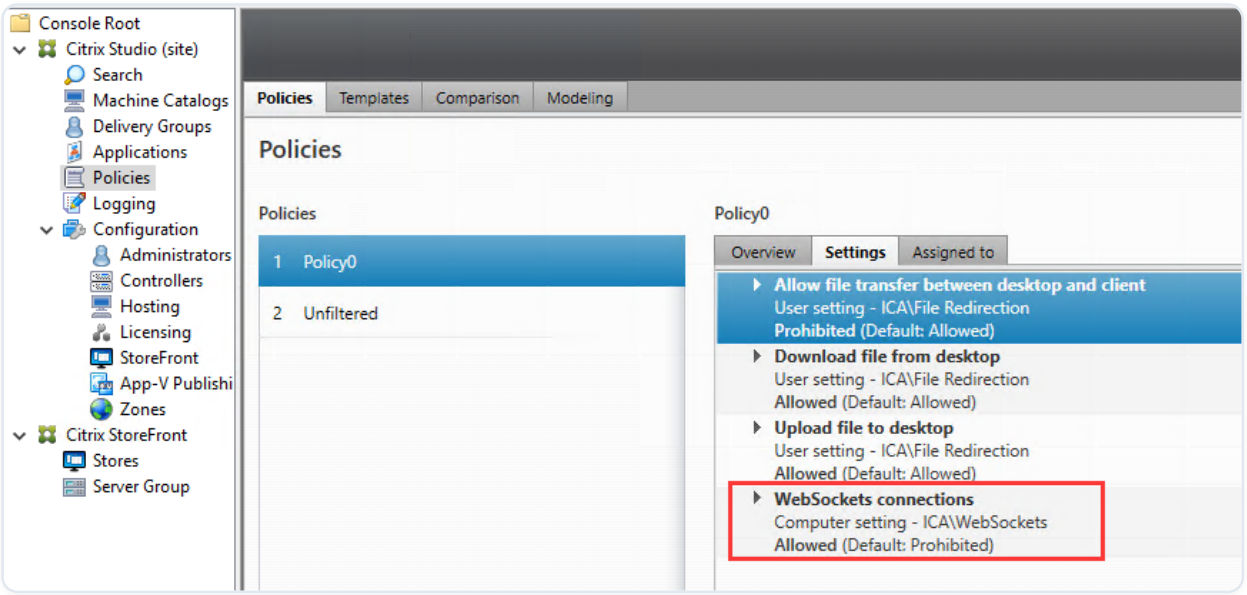
- **Dateiübertragung zwischen Desktop und Client zulassen.** Ermöglicht oder verhindert Dateiübertragungen zwischen den Citrix Virtual Apps and Desktops™-Sitzungen und den Clientgeräten.
- **Datei vom Desktop herunterladen.** Ermöglicht oder verhindert Dateidownloads von den Citrix Virtual Apps™ and Desktops-Sitzungen auf die Clientgeräte.
- **Datei auf den Desktop hochladen.** Ermöglicht oder verhindert Dateidownloads von den Clientgeräten auf die Citrix Virtual Apps and Desktops-Sitzungen.

> **Hinweis:**
>
> Um sicherzustellen, dass die Richtlinien **Datei vom Desktop herunterladen** und **Datei auf den Desktop hochladen** wirksam werden, setzen Sie die Richtlinie **Dateiübertragung zwischen Desktop und Client zulassen** auf **Zugelassen**.

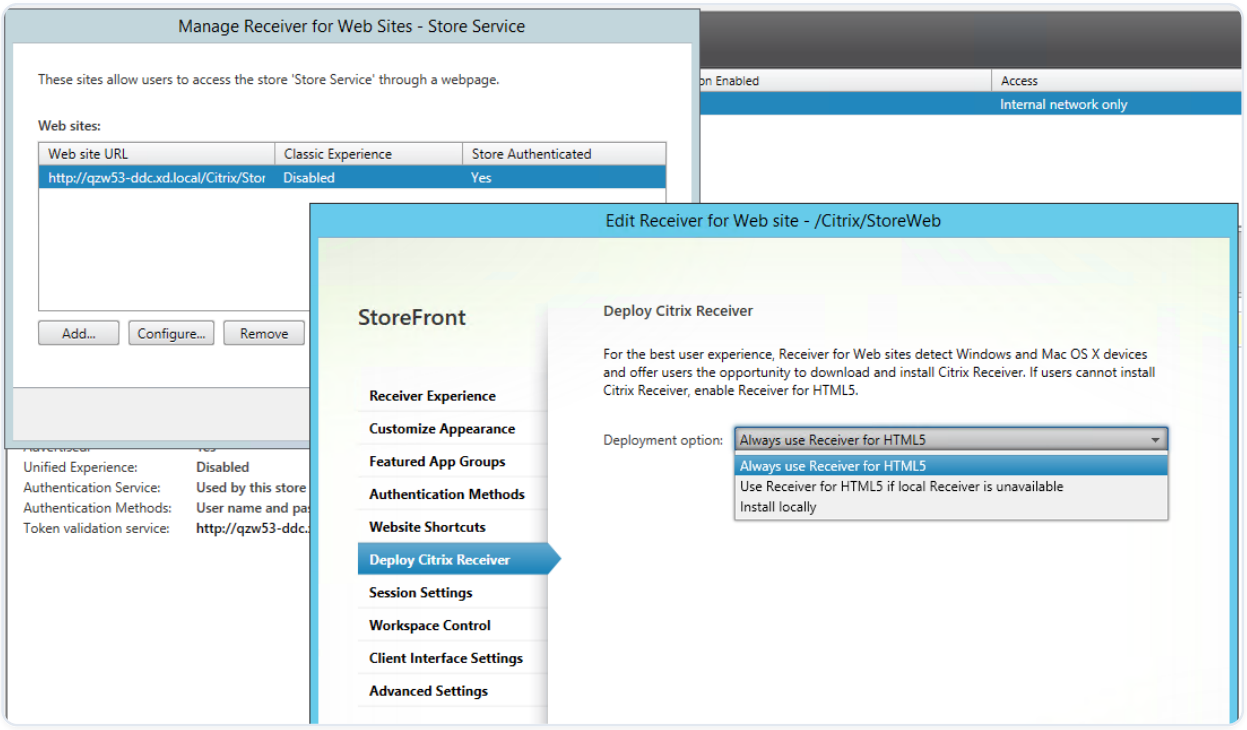
Verwendung

So verwenden Sie die Dateiübertragungsfunktion über die Citrix Workspace-App für HTML5:

1. Legen Sie in Citrix Studio die Richtlinie **WebSockets connections** auf **Zugelassen** fest.



2. Aktivieren Sie in Citrix Studio die Dateiübertragung über die zuvor beschriebenen Dateiübertragungsrichtlinien.
3. Klicken Sie in der Citrix StoreFront-Verwaltungskonsole auf **Stores**, wählen Sie den Knoten **Manage Receiver for Web Sites** aus und aktivieren Sie Citrix Receiver™ für HTML5, indem Sie die Option **Always use Receiver for HTML5** auswählen.



4. Starten Sie eine virtuelle Desktop- oder Webbrowser-App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux VDA und Ihrem Clientgerät durch.

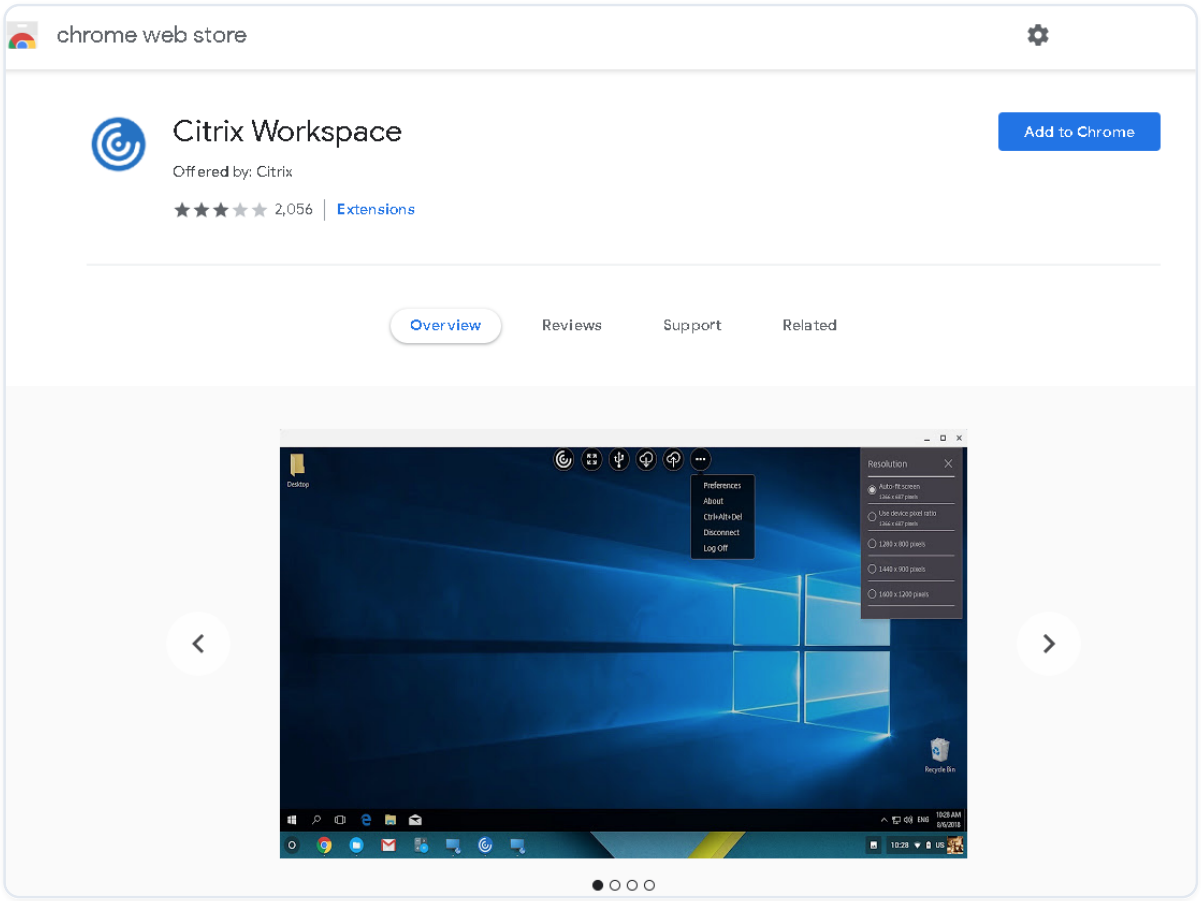
So verwenden Sie die Dateiübertragungsfunktion über die Citrix Workspace-App für Chrome:

1. Aktivieren Sie die Dateiübertragung über die zuvor beschriebenen Dateiübertragungsrichtlinien.
2. Beziehen Sie die Citrix Workspace-App aus dem Chrome Web Store.

   Überspringen Sie diesen Schritt, wenn Sie die Citrix Workspace-App für Chrome bereits zur Chrome Apps-Seite hinzugefügt haben.

   a. Geben Sie **Citrix Workspace for Chrome** in das Suchfeld von Google Chrome ein. Klicken Sie auf das Suchsymbol.

   b. Klicken Sie in den Suchergebnissen auf die URL zum Chrome Web Store, wo die Citrix Workspace-App verfügbar ist.



   c. Klicken Sie auf **Zu Chrome hinzufügen**, um die Citrix Workspace-App zu Google Chrome hinzuzufügen.

3. Klicken Sie auf der Seite „Chrome-Apps“ auf die Citrix Workspace-App für Chrome.
4. Geben Sie die URL Ihres StoreFront™-Stores ein, um eine Verbindung herzustellen.

   Überspringen Sie diesen Schritt, wenn Sie die URL bereits eingegeben haben.

5. Starten Sie eine virtuelle Desktop- oder App-Sitzung. Führen Sie eine oder mehrere Dateiübertragungen zwischen dem Linux VDA und Ihrem Clientgerät durch.

Grafik

Dieser Abschnitt enthält die folgenden Themen:

- Automatische DPI-Skalierung
- Anzeige des Client-Akkustatus
- Grafikkonfiguration und Feinabstimmung
- HDX-Bildschirmfreigabe
- Nicht virtualisierte GPUs
- Sitzungswasserzeichen
- Thinwire Progressive Display

Automatische DPI-Skalierung

Der Linux VDA unterstützt die automatische DPI-Skalierung. Wenn ein Benutzer eine virtuelle Desktop- oder Anwendungssitzung öffnet, ändert sich der DPI-Wert in der Sitzung automatisch, um der DPI-Einstellung auf der Clientseite zu entsprechen.

Im Folgenden sind Überlegungen zu dieser Funktion aufgeführt:

- Die Funktion erfordert, dass Sie die DPI-Anpassung für Citrix Workspace aktivieren. Stellen Sie bei der Citrix Workspace-App für Windows sicher, dass die Option **Nein, native Auflösung verwenden** ausgewählt ist. Weitere Informationen zum Konfigurieren der DPI-Skalierung für die Citrix Workspace-App für Windows finden Sie unter DPI-Skalierung.
- Damit die Funktion in Multi-Monitor-Szenarien funktioniert, muss jeder Monitor mit derselben DPI-Einstellung konfiguriert sein. Gemischte DPI-Szenarien werden nicht unterstützt. Wenn Monitore mit unterschiedlichen DPI-Einstellungen konfiguriert sind, wendet der Linux VDA den kleinsten DPI-Wert für alle Bildschirme an.
- Die Funktion ist für MATE, GNOME, GNOME Classic und KDE aktiviert. Bei Verwendung von KDE oder MATE ist Folgendes zu beachten:
    - Für virtuelle Linux-Desktops, die in einer KDE-Desktopumgebung ausgeführt werden:
        - Wir empfehlen die Verwendung von KDE Plasma 5 oder höher.
        - Das Ändern der DPI-Einstellungen auf der Clientseite während laufender Sitzungen erfordert, dass sich Benutzer abmelden und erneut anmelden.
    - Für virtuelle Linux-Desktops, die in einer MATE-Desktopumgebung ausgeführt werden:

    - Es werden nur Skalierungsfaktoren von 1 und 2 unterstützt.
    - Das Ändern der DPI-Einstellungen auf der Clientseite während laufender Sitzungen erfordert, dass sich Benutzer abmelden und erneut anmelden.

- Der DPI-Wert in der virtuellen Sitzung ändert sich automatisch entsprechend der DPI-Einstellung auf der Clientseite. Derzeit unterstützt die Funktion nur Skalierungsfaktoren vom Typ Ganzzahl, z. B. 100 % und 200 %. Wenn der auf der Clientseite konfigurierte Skalierungsfaktor vom Typ Bruch ist, ändert sich der DPI-Wert der virtuellen Sitzung gemäß der folgenden Tabelle in einen ganzzahligen Skalierungsfaktor. Beispiel: Wenn der Skalierungsfaktor 125 % beträgt, ändert sich der DPI-Wert auf 100 %.

CLIENTSEITIGER SKALIERUNGSFAKTOR	DPI DER REMOTESITZUNG
Kleiner oder gleich 174 %	96 (1 x 96)
175 %–274 %	192 (2 x 96)
275 %–399 %	288 (3 x 96)
Größer oder gleich 400 %	384 (4 x 96)

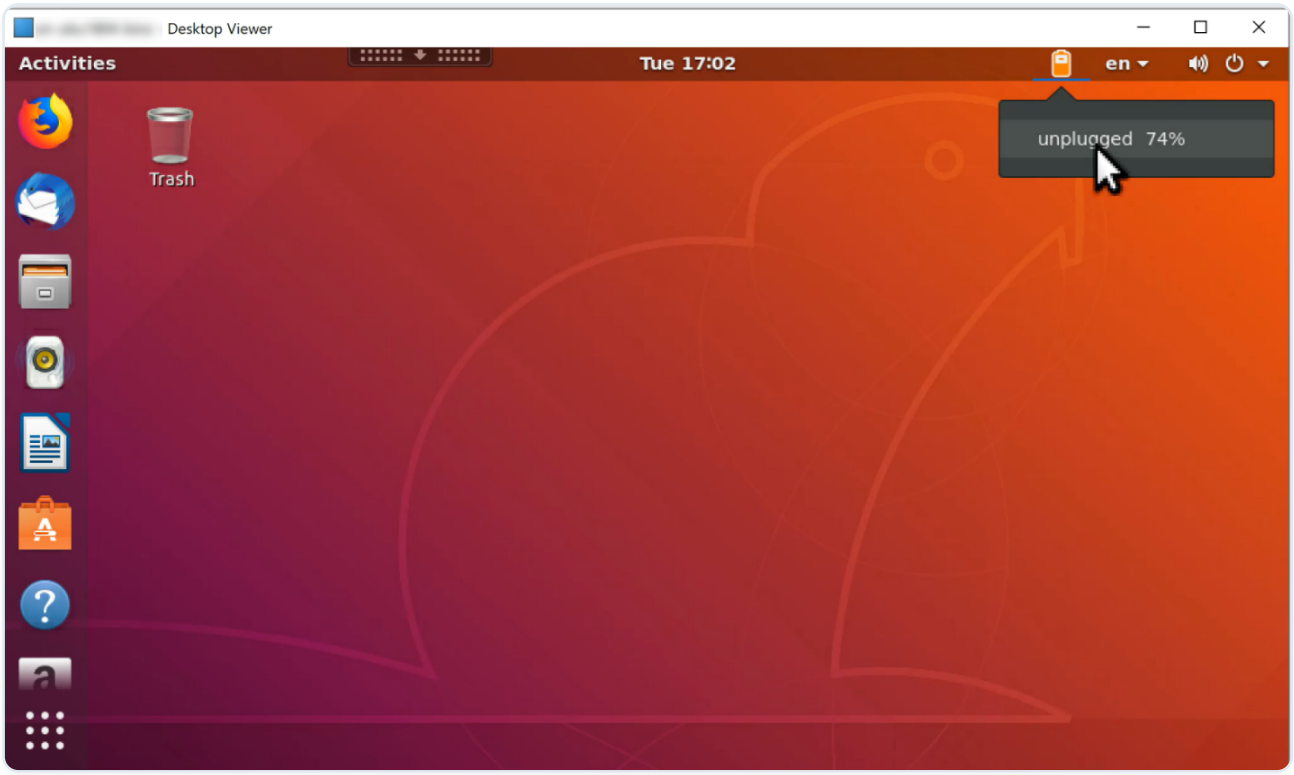
Anzeige des Client-Akkustatus

Der Linux-VDA kann den Akkustatus von Clientgeräten in virtuellen Desktops umleiten und anzeigen. Diese Funktion ist standardmäßig aktiviert und für die folgenden 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, sehen sie ein Akkusymbol in der Linux-Systemleiste. Das Akkusymbol zeigt den Akkustatus ihrer Clientgeräte an. Um den Prozentsatz der verbleibenden Akkulaufzeit zu überprüfen, klicken Sie auf das Akkusymbol. Beispiel siehe folgenden Screenshot:



Verschiedene Akkusymbole zeigen unterschiedliche Akkustatus an. Eine Übersicht finden Sie in der folgenden Tabelle:

AKKUSYMBOL	LADESTATUS	VERBLEIBENDE AKKULAUFZEIT	PROZENTSATZ DER VERBLEIBENDEN AKKULAUFZEIT
	Wird geladen, angezeigt durch ein „+“-Symbol	Hoch, angezeigt durch grüne Farbe	>=80%
Akku, der geladen wird und eine mittlere Restladung hat(/en-us/linux-virtual-delivery-agent/2308/media/battery-charging-medium.png)	Wird geladen, angezeigt durch ein „+“-Symbol	Mittel, bernsteinfarben angezeigt	>=20% und <80%
Akku, der geladen wird und eine niedrige Restladung hat(/en-us/linux-virtual-delivery-agent/2308/media/	Wird geladen, angezeigt durch ein „+“-Symbol	Niedrig, rot angezeigt	< 20%

AKKUSYMBOL	LADESTATUS	VERBLEIBENDE AKKULAUFZEIT	PROZENTSATZ DER VERBLEIBENDEN AKKULAUFZEIT
battery-charging-low.png)			
Akku, der nicht geladen wird und eine hohe Restladung hat(/en-us/linux-virtual-delivery-agent/2308/media/battery-not-charging-high.png)	Wird nicht geladen, angezeigt durch ein „-“-Symbol	Hoch, grün angezeigt	>=80%
Akku, der nicht geladen wird und eine mittlere Restladung hat(/en-us/linux-virtual-delivery-agent/2308/media/battery-not-charging-medium.png)	Wird nicht geladen, angezeigt durch ein „-“-Symbol	Mittel, bernsteinfarben angezeigt	>=20 % und <80 %
	Wird nicht geladen, angezeigt durch ein „-“-Symbol	Niedrig, angezeigt durch rote Farbe	< 20 %
	Unbekannt	Unbekannt	Unbekannt

Konfiguration

Die Anzeige des Client-Akkustatus ist standardmäßig aktiviert.

Um die Funktion zu deaktivieren, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000000"
```

Um die Funktion zu aktivieren, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000001"
```

Hinweis:

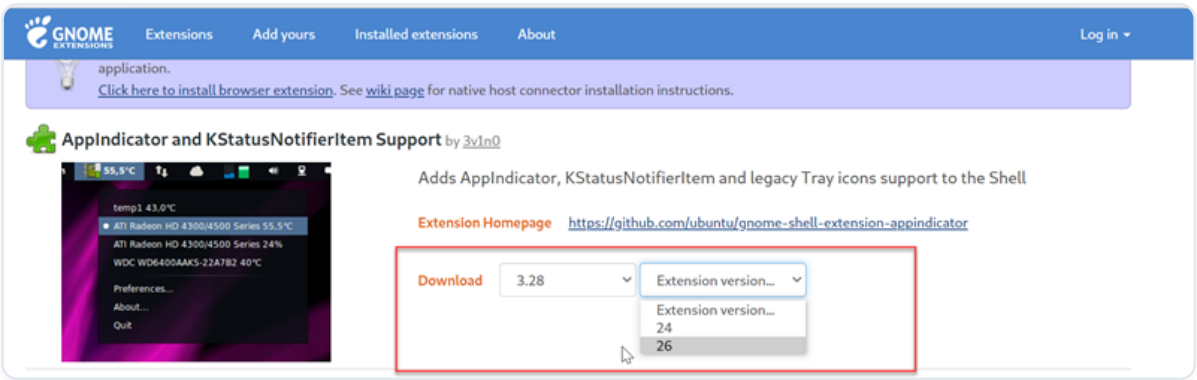
Die vorhergehenden Befehle wirken sich auf die Funktion Soft-Tastatur aus, die den Mobile Receiver Virtual Channel (MRVC) mit der Client-Akkustatusanzeige teilt.

Führen Sie je nach Distribution die folgenden zusätzlichen Schritte aus:

1. Wenn Sie RHEL 8.x oder SUSE 15.x mit GNOME verwenden, installieren Sie eine kompatible Erweiterung für Ihre GNOME-Shell, um die AppIndicator-Unterstützung zu aktivieren:

   a. Führen Sie den Befehl `gnome-shell --version` aus, um Ihre GNOME-Shell-Version zu überprüfen.

   b. Laden Sie eine kompatible Erweiterung für Ihre GNOME-Shell von `<https://extensions.gnome.org/extension/615/appindicator-support>` herunter. Wenn Ihre Shell-Version beispielsweise 3.28 ist, können Sie 24 oder 26 für die Erweiterungsversion auswählen.



   c. Entpacken Sie das heruntergeladene Paket. Stellen Sie sicher, dass der Wert **„uuid“** in der Datei **metadata.json** im Paket auf appindicatorsupport@rgcjonas.gmail.com eingestellt ist.

   d. Führen Sie den Befehl `mv` aus, um das Verzeichnis appindicatorsupport@rgcjonas.gmail.com an den Speicherort unter `/usr/share/gnome-shell/extensions/` zu verschieben.

e. Führen Sie den Befehl `chmod a+r metadata.json` aus, um die Datei **metadata.json** für andere Benutzer lesbar zu machen.

> **Tipp:**
>
> Standardmäßig ist die Datei **metadata.json** im Verzeichnis appindicatorsupport@rgcjonas.gmail.com nur für den Root-Benutzer lesbar. Um die Bildschirmfreigabe zu unterstützen, machen Sie die Datei **metadata.json** auch für andere Benutzer lesbar.

f. Installieren Sie GNOME Tweaks.

g. In der Desktop-Umgebung laden Sie Ihre GNOME-Shell neu, indem Sie nacheinander die Tasten `Alt+F2`, `r` und `Enter` drücken oder indem Sie den Befehl `killall -SIGQUIT gnome-shell` ausführen.

h. In der Desktop-Umgebung führen Sie GNOME Tweaks aus und aktivieren Sie dann **KStatusNotifierItem/AppIndicator Support** im Tweaks-Tool.

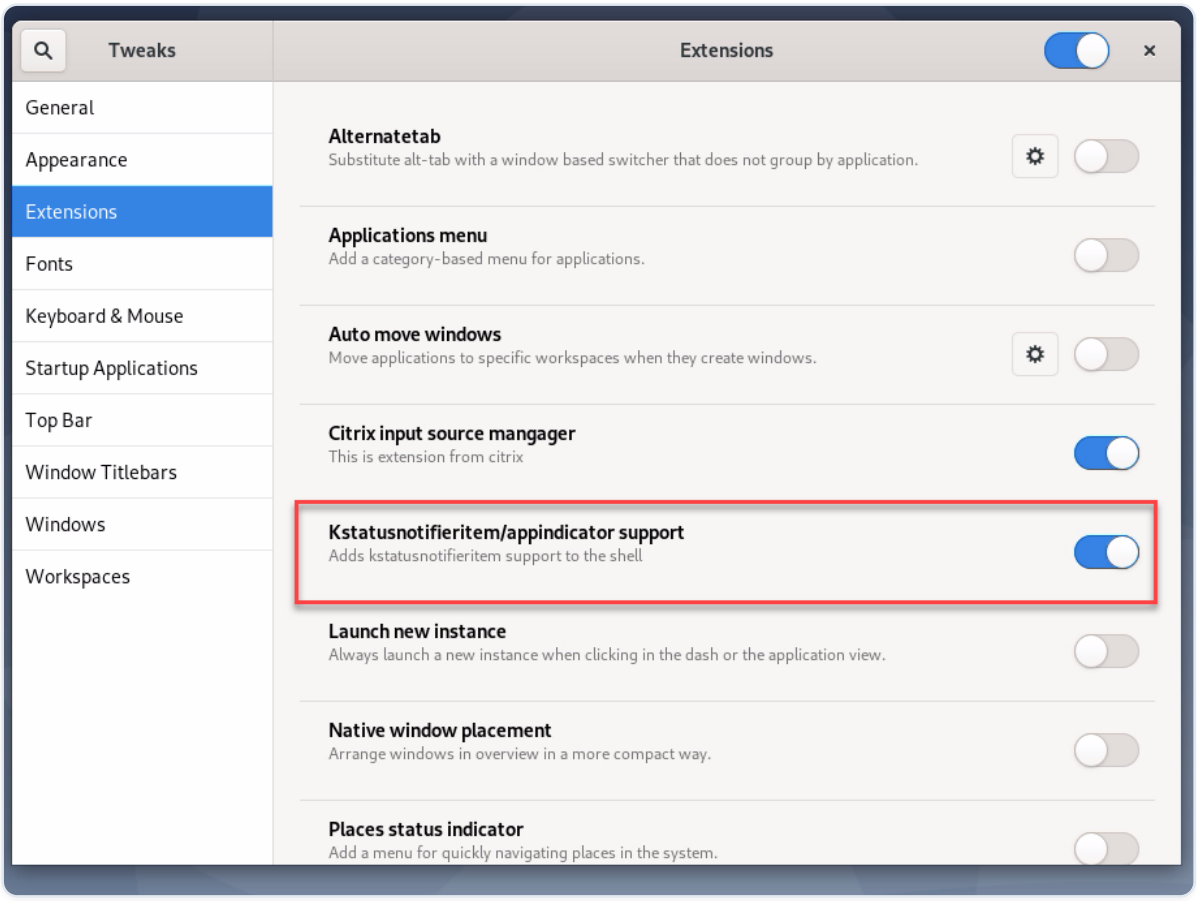
2. Wenn Sie Debian 11.3 mit GNOME verwenden, führen Sie die folgenden Schritte aus, um GNOME-Systemleistensymbole zu installieren und zu aktivieren:

   a. Führen Sie den Befehl `sudo apt install gnome-shell-extension-appindicator` aus. Möglicherweise müssen Sie sich ab- und wieder anmelden, damit GNOME die Erweiterung erkennt.

   b. Suchen Sie auf Ihrem **Aktivitäten**-Bildschirm nach Tweaks.

   c. Wählen Sie im Tweaks-Tool **Erweiterungen** aus.

   d. Aktivieren Sie **Kstatusnotifieritem/appindicator support**.



Grafikkonfiguration und Feinabstimmung

Dieser Artikel beschreibt die Grafikkonfiguration und Feinabstimmung des Linux VDA.

Weitere Informationen finden Sie unter Systemanforderungen und im Abschnitt Installationsübersicht.

Konfiguration

Für 3D-Grafik-Workload optimieren

Diese Einstellung konfiguriert die entsprechenden Standardwerte, die am besten für grafikintensive Workloads geeignet sind. Aktivieren Sie diese Einstellung für Benutzer, deren Workload sich auf grafikintensive Anwendungen konzentriert. Wenden Sie diese Richtlinie nur an, wenn eine GPU für die Sitzung verfügbar ist. Alle anderen Einstellungen, die die durch diese Richtlinie festgelegten Standardeinstellungen explizit überschreiben, haben Vorrang.

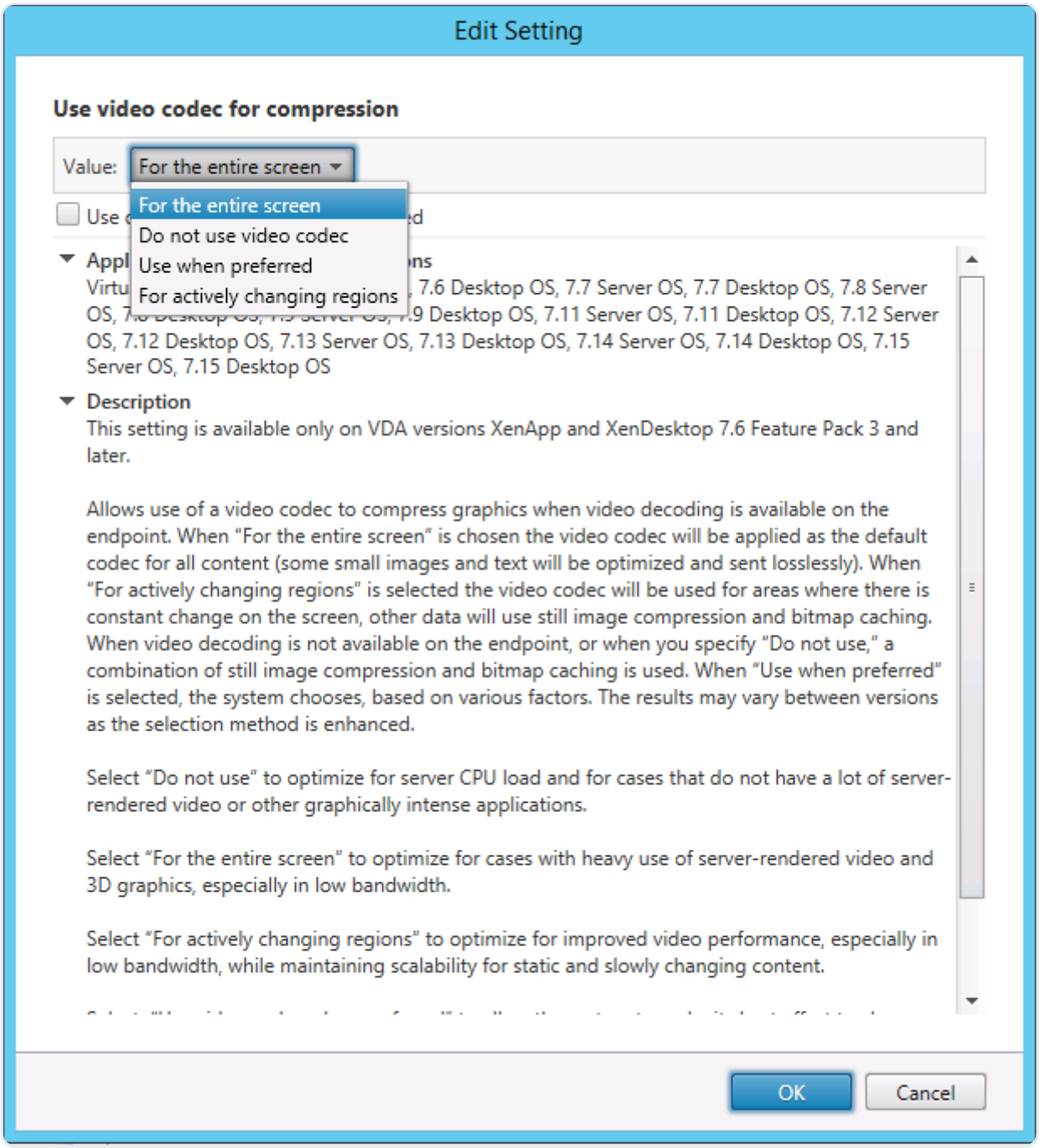
Standardmäßig ist **Für 3D-Grafik-Workload optimieren** deaktiviert.

Videocodec für Komprimierung

Thinwire ist die im Linux VDA verwendete Display-Remoting-Technologie. Die Technologie ermöglicht die Übertragung von auf einem Computer generierten Grafiken, typischerweise über ein Netzwerk, an einen anderen Computer zur Anzeige.

Die Grafikrichtlinie Videocodec für Komprimierung verwenden legt den Standard-Grafikmodus fest und bietet die folgenden Optionen für verschiedene Anwendungsfälle:

- **Bei Präferenz verwenden**. Diese Einstellung ist die Standardeinstellung. Es ist keine zusätzliche Konfiguration erforderlich. Sie stellt sicher, dass Thinwire für alle Citrix®-Verbindungen ausgewählt und für Skalierbarkeit, Bandbreite und überragende Bildqualität bei typischen Desktop-Workloads optimiert wird.
- **Für den gesamten Bildschirm**. Liefert Thinwire mit Vollbild-H.264 oder H.265, um die Benutzererfahrung und Bandbreite zu optimieren, insbesondere bei intensiver Nutzung von 3D-Grafiken. Sitzungswasserzeichen wird unterstützt, wenn **Für den gesamten Bildschirm** ausgewählt ist oder wenn **Bei Präferenz verwenden** ausgewählt und Für 3D-Grafik-Workload optimieren aktiviert ist.
- **Für sich aktiv ändernde Bereiche**. Die adaptive Anzeigetechnologie in Thinwire identifiziert bewegte Bilder (Video, 3D in Bewegung). Sie verwendet H.264 oder H.265 nur in dem Teil des Bildschirms, in dem sich das Bild bewegt. Die selektive Verwendung des H.264- oder H.265-Videocodecs ermöglicht es HDX Thinwire, häufig aktualisierte Bildschirmbereiche zu erkennen und mit dem H.264- oder H.265-Videocodec zu kodieren. Für den Rest des Bildschirms, einschließlich Text und fotografischer Bilder, werden weiterhin Standbildkomprimierung (JPEG, RLE) und Bitmap-Caching verwendet. Benutzer profitieren von einem geringeren Bandbreitenverbrauch und einer besseren Qualität für Videoinhalte in Kombination mit verlustfreiem Text oder hochwertigen Bildern an anderer Stelle. Die selektive Verwendung von H.265 wird nicht unterstützt, wenn die Richtlinie **Visuelle Qualität** auf **Immer verlustfrei** oder **Verlustfrei aufbauen** eingestellt ist.



Einige andere Richtlinieneinstellungen, einschließlich der folgenden Richtlinieneinstellungen für die visuelle Anzeige, können zur Feinabstimmung der Leistung des Display-Remotings verwendet werden:

- **Bevorzugte Farbtiefe für einfache Grafiken**
- **Zielbildrate**
- **Visuelle Qualität**

H.265/H.264 Hardware-Kodierung

Die Richtlinie **Hardwarekodierung für Videocodec verwenden** ermöglicht die Nutzung der GPU-Hardwarebeschleunigung, sofern verfügbar, um Bildschirmelemente mit dem Videocodec zu komprimieren. Die GPU-Hardwarebeschleunigung optimiert die Hardware-Ressourcennutzung und verbessert die Leistung in Bildern pro Sekunde (FPS) erheblich.

Die GPU-Hardwarebeschleunigung deckt alle Grafikmodi ab, die durch die Richtlinie Videocodec für Komprimierung verwenden festgelegt sind:

- **Bei Präferenz verwenden**
- **Für den gesamten Bildschirm**
- **Für sich aktiv ändernde Bereiche**

Führen Sie die folgenden Schritte aus, um die Hardware-Videokomprimierung zu aktivieren:

1. Setzen Sie die Richtlinie **Hardwarekodierung für Videocodec verwenden** auf **Aktiviert**.
2. Setzen Sie **Videocodec für Komprimierung verwenden** auf **Bei Präferenz verwenden**, **Für den gesamten Bildschirm** oder **Für sich aktiv ändernde Bereiche**. Stellen Sie sicher, dass sie nicht auf **Videocodec nicht verwenden** gesetzt ist.

Der H.265-Videocodec muss sowohl auf dem VDA als auch in der Citrix Workspace-App unterstützt und aktiviert sein. Wenn der H.265-Videocodec weder auf dem Linux VDA noch in der Citrix Workspace-App unterstützt wird, wird die Richtlinieneinstellung **H.265-Dekodierung für Grafiken** ignoriert, und die Sitzungen greifen auf den H.264-Videocodec zurück. Wenn keine GPU-Hardware verfügbar ist, greift der VDA auf die CPU-basierte Kodierung mit dem Software-Videocodec zurück.

Informationen zum Aktivieren der H.265-Hardwarekodierung auf Ihrem Client finden Sie unter H.265-Videokodierung.

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

H.265/H.264 verlustfreie Komprimierung

Die verlustfreie H.265/H.264-Komprimierung ist für die HDX 3D PRO-Hardwarebeschleunigung durch NVIDIA-GPUs verfügbar. Die verlustfreie H.265-Komprimierung erfordert Citrix Workspace-

App 2305 für Windows und höher. Die verlustfreie H.264-Komprimierung erfordert die folgenden Clients:

- Citrix Workspace-App 2303 für Windows und höher
- Citrix Workspace-App 2301 für Mac und höher mit dem Apple M1-Chip

Führen Sie die folgenden Schritte aus, 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 für Komprimierung verwenden** auf **Für den gesamten Bildschirm** fest.
3. Legen Sie die Richtlinie **Visuelle Qualität** auf **Immer verlustbehaftet** oder **Verlustfrei aufbauen** fest.

Visuell verlustfreie Komprimierung zulassen

Die Richtlinie **Visuell verlustfreie Komprimierung zulassen** ermöglicht die Verwendung einer **visuell** verlustfreien Komprimierung anstelle einer echten verlustfreien Komprimierung für Grafiken. Visuell verlustfrei verbessert die Leistung gegenüber echter verlustfreier Komprimierung, weist jedoch geringfügige, mit bloßem Auge nicht wahrnehmbare Verluste auf. Diese Einstellung ändert die Art und Weise, wie die Werte der Einstellung **Visuelle Qualität** verwendet werden.

Die Richtlinie **Visuell verlustfreie Komprimierung zulassen** ist standardmäßig deaktiviert. Um die **visuell** verlustfreie Komprimierung zu aktivieren, legen Sie **Visuell verlustfreie Komprimierung zulassen** auf **Aktiviert** und die Richtlinie **Visuelle Qualität** auf **Verlustfrei aufbauen** fest.

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.

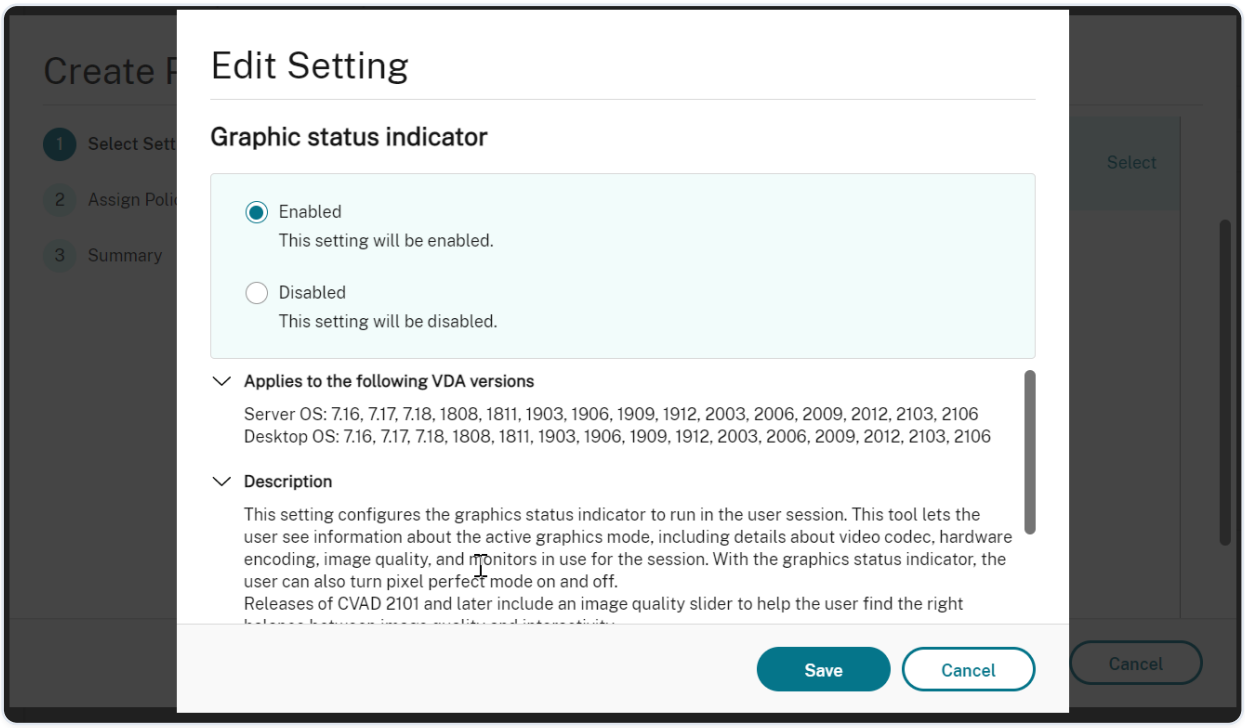
Weitere Informationen zu den Richtlinieneinstellungen **Visuelle Qualität** und **Videocodec für Komprimierung verwenden** finden Sie unter Richtlinieneinstellungen für die visuelle Anzeige und Richtlinieneinstellungen für Grafiken.

Schieberegler für Grafikqualität

Wir haben einen Schieberegler für die Grafikqualität in das Grafikstatusanzeigetool integriert, das in Ihren virtuellen Linux-Sitzungen ausgeführt wird. Der Schieberegler hilft, die richtige Balance zwischen Bildqualität und Interaktivität zu finden.

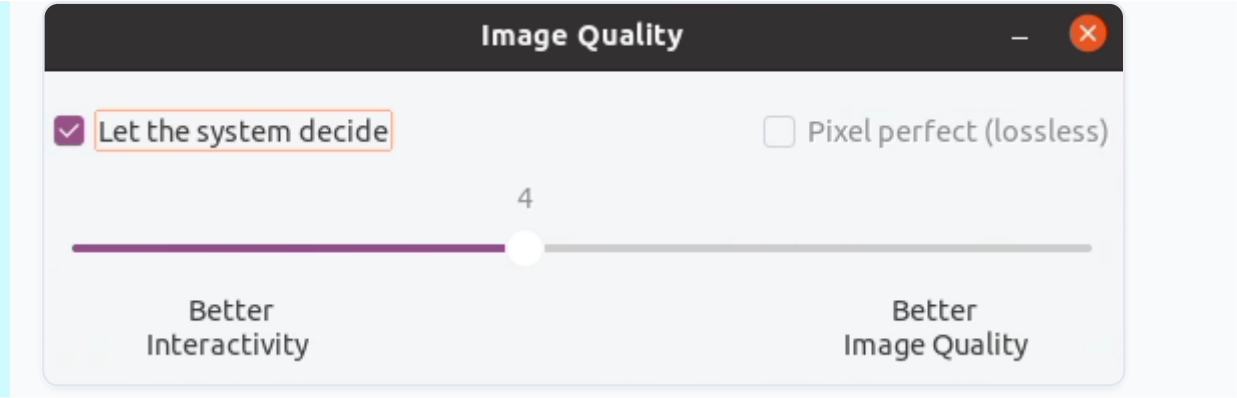
Führen Sie die folgenden Schritte aus, um den Schieberegler zu verwenden:

1. Aktivieren Sie die Richtlinie **Grafikstatusanzeige** in Citrix Studio.



2. Öffnen Sie das Terminal und führen Sie den Befehl `ctxslider` aus. Die Schieberegler-Benutzeroberfläche wird angezeigt.

> **Hinweis:**
>
> - Wenn Sie die Richtlinie **Visuelle Qualität** auf **Immer verlustfrei** oder **Verlustfrei erstellen** eingestellt haben, wird die Schieberegler-Benutzeroberfläche nicht angezeigt.
> - Sie können die Schieberegler-Benutzeroberfläche sowohl über das Terminal als auch über die Systemleiste starten.



Die folgenden Optionen sind jetzt verfügbar:

- Um die Bildqualität zu ändern, bewegen Sie den Schieberegler. Der Schieberegler unterstützt einen Bereich von 0–9.
- 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-Hardwarekodierung durch Anpassen der durchschnittlichen Bitraten basierend auf Bandbreitenschätzungen.

Wenn die HDX 3D Pro-Hardwarekodierung verwendet wird, kann der VDA die Bandbreite des Netzwerks intermittierend schätzen und die Bitraten der kodierten Frames entsprechend anpassen. Diese neue Funktion bietet einen Mechanismus, um ein Gleichgewicht zwischen Schärfe und Flüssigkeit herzustellen.

Diese Funktion ist standardmäßig aktiviert. Um sie zu deaktivieren, führen Sie den folgenden Befehl aus:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "DisableReconfigureEncoder" -d "0x00000001" --force
```

Zusätzlich zur Verwendung dieser Funktion können Sie auch die folgenden Befehle ausführen, um zwischen Schärfe und Flüssigkeit zu wechseln. Die Parameter **AverageBitRatePercent** und **MaxBitRatePercent** legen den Prozentsatz der Bandbreitennutzung fest. Je höhere Werte Sie einstellen, desto schärfer sind die Grafiken und desto geringer ist die Flüssigkeit. Der empfohlene Einstellungsbereich liegt bei 50–100.

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "AverageBitRatePercent" -d "90" --force



sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "MaxBitRatePercent" -d "100" --force
```

Bei der Anpassung der durchschnittlichen Bitrate bleibt der aktuellste Frame in einem Zustand niedriger Qualität, wenn der Bildschirm stillsteht, da keine neuen Frames gesendet werden. Die Schärfungsunterstützung kann dieses Problem beheben, indem der aktuellste Frame neu konfiguriert und sofort in höchster Qualität gesendet wird.

Eine vollständige Liste der vom Linux VDA Thinwire unterstützten Richtlinien finden Sie unter Liste der unterstützten Richtlinien.

Informationen zur Konfiguration der Multi-Monitor-Unterstützung auf dem Linux VDA finden Sie unter CTX220128.

Parallele Verarbeitung

Thinwire kann die Anzahl der Frames pro Sekunde (FPS) durch Parallelisierung bestimmter Aufgaben verbessern, was jedoch mit einem leicht höheren CPU-Gesamtverbrauch einhergeht. Diese Funktion ist standardmäßig deaktiviert. Um die Funktion zu aktivieren, führen Sie den folgenden Befehl auf Ihrem VDA aus:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"ParallelProcessing" -d "0x00000001" --force
```

Problembehandlung

Prüfen, welcher Grafikmodus verwendet wird

Führen Sie den folgenden Befehl aus, um zu prüfen, welcher Grafikmodus verwendet wird (**0** bedeutet TW+, **1** bedeutet Vollbild-Videocodec):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

Das Ergebnis sieht ähnlich aus:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000000" --force
```

Überprüfen, ob H.264 verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob H.264 verwendet wird (**0** bedeutet nicht in Verwendung. **1** bedeutet in Verwendung):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H264
```

Das Ergebnis kann beispielsweise wie folgt aussehen:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000000" --force
```

Überprüfen, ob H.265 verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Vollbild-H.265 verwendet wird (**0** bedeutet nicht in Verwendung. **1** bedeutet in Verwendung):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep H265
```

Das Ergebnis kann beispielsweise wie folgt aussehen:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H265" -d "0x00000000" --force
```

Prüfen, welches YUV-Kodierungsschema verwendet wird

Führen Sie den folgenden Befehl aus, um zu überprüfen, welches YUV-Kodierungsschema verwendet wird (**0** bedeutet YUV420. **1** bedeutet YUV422. **2** bedeutet YUV444):

> **Hinweis:**
>
> Der Wert von **YUVFormat** ist nur aussagekräftig, wenn ein Videocodec verwendet wird.

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep YUVFormat
```

Das Ergebnis kann beispielsweise wie folgt aussehen:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000000" --force`

Überprüfen, ob 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
```

Wenn YUV444 verwendet wird, sieht das Ergebnis wie folgt aus:

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "GraphicsMode" -d "0x00000001" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "H264" -d "0x00000001" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "HardwareEncoding" -d "0x00000000" --force`

`create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics" -t "REG_DWORD" -v "YUVFormat" -d "0x00000002" --force`

Überprüfen, ob 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
```

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 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 |

+-----------------------------------------------------------------------------
----+
```

Überprüfen, ob die Hardwarekodierung für 3D Pro verwendet wird

Führen Sie den folgenden Befehl aus (**0** bedeutet nicht in Gebrauch. **1** bedeutet in Gebrauch):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep HardwareEncoding
```

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`

Überprüfen, ob der NVIDIA GRID-Grafiktreiber korrekt installiert ist

Um zu überprüfen, ob der NVIDIA GRID-Grafiktreiber korrekt installiert ist, führen Sie **nvidia-smi** aus. Das Ergebnis sieht 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
                                 |

+-----------------------------------------------------------------------------
----+
```

Legen Sie die richtige Konfiguration für die Karte fest:

`etc/X11/ctx-nvidia.sh`

HDX 3D Pro: Probleme beim Neuzeichnen auf mehreren Monitoren

Wenn Sie Probleme beim Neuzeichnen auf anderen Bildschirmen als dem primären Monitor feststellen, überprüfen Sie, ob die NVIDIA GRID-Lizenz verfügbar ist.

Xorg-Fehlerprotokolle prüfen

Die Protokolldatei von Xorg heißt ähnlich wie **Xorg.{DISPLAY}.log** im Ordner **/var/log/**.

Bekannte Probleme und Einschränkungen

Bei vGPU zeigt die lokale Konsole von Citrix Hypervisor™ den ICA-Desktopsitzungsbildschirm an

Problemumgehung: Deaktivieren Sie die lokale VGA-Konsole der VM, indem Sie die folgenden Befehle ausführen:

Für Citrix Hypervisor 8.1 und höher:

```
[root@xenserver® ~]# xe vgpu-param-set uuid=vgpu-uuid
extra_args=disable_vnc=1
```

Für Citrix Hypervisor vor 8.1:

```
xe vm-param-set uuid=<vm-uuid> platform:vgpu_extra_args="disable_vnc=1"
```

Gnome 3-Desktop-Popups langsam beim Anmelden

Dies ist eine Einschränkung des Startvorgangs der Gnome 3-Desktopsitzung.

Einige OpenGL/WebGL-Anwendungen werden beim Ändern der Größe des Citrix Workspace-App-Fensters nicht korrekt gerendert

Das Ändern der Größe des Fensters der Citrix Workspace-App ändert die Bildschirmauflösung. Der proprietäre NVIDIA-Treiber ändert einige interne Zustände und erfordert möglicherweise, dass Anwendungen entsprechend reagieren. Zum Beispiel könnte das WebGL-Bibliothekselement **lightgl.js** einen Fehler ausgeben, der besagt, dass **Das Rendern auf diese Textur wird nicht unterstützt (unvollständiger Framebuffer)**.

HDX™-Bildschirmfreigabe

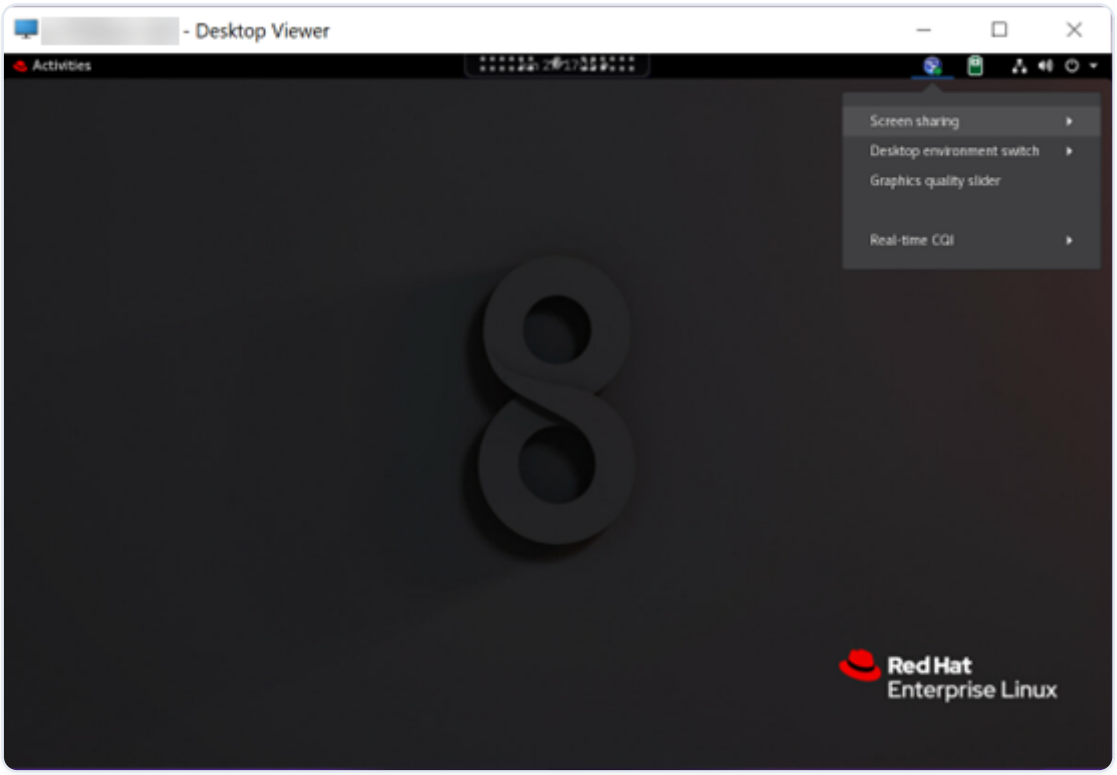
Übersicht

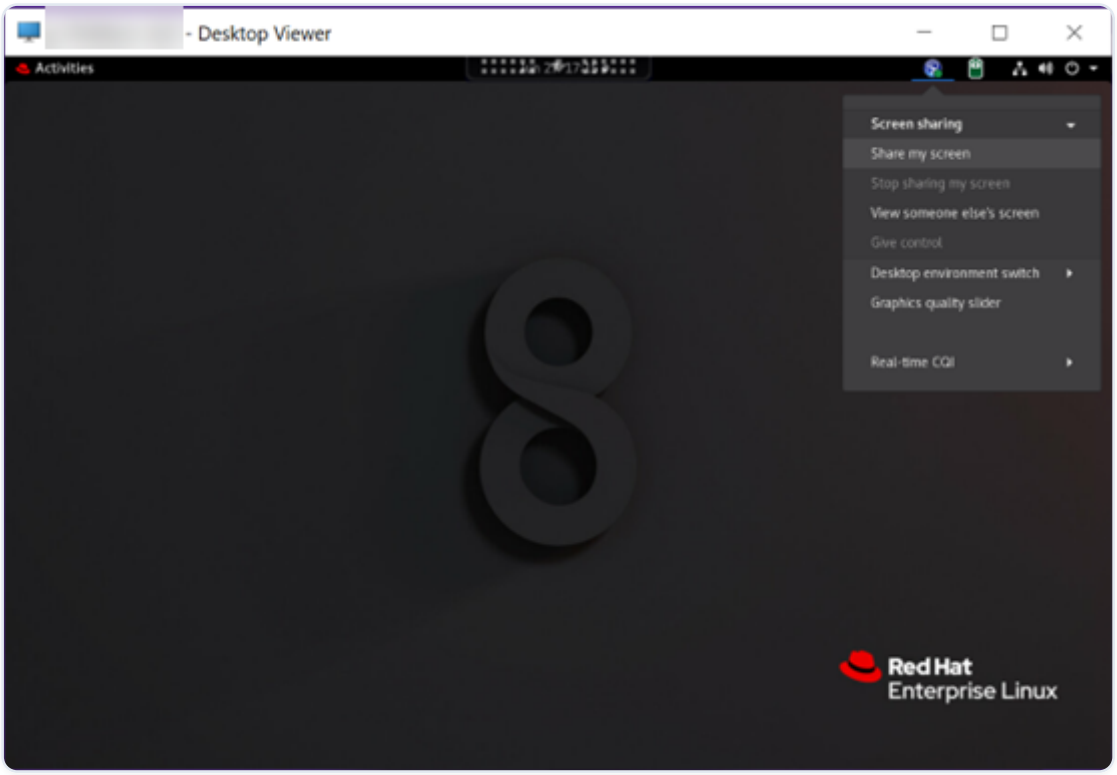
Mit dem Linux VDA können Sie den Bildschirm Ihres virtuellen Desktops für Sitzungsbenutzer auf anderen virtuellen Desktops freigeben.

Das folgende Beispiel führt Sie durch die Vorgehensweise zum Freigeben eines Bildschirms und zum Anzeigen des Bildschirms einer anderen Person.

So geben Sie einen Bildschirm frei:

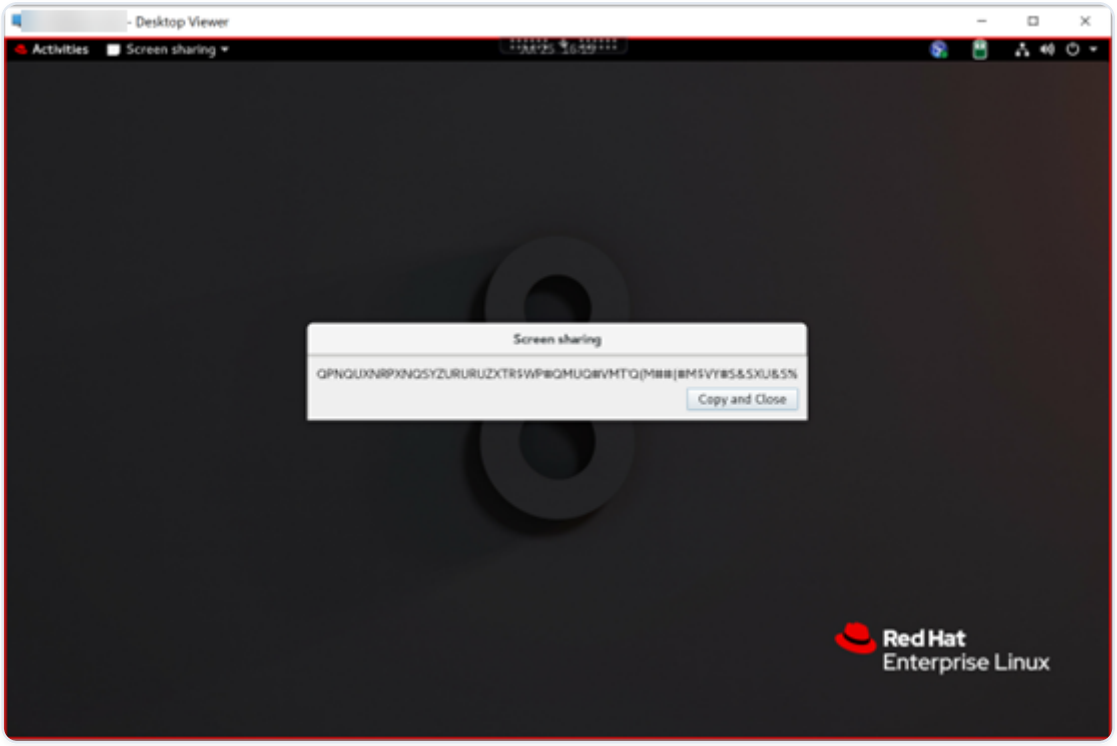
1. Klicken Sie im Infobereich Ihres virtuellen Desktops auf das folgende Systemtray-Symbol und wählen Sie **Bildschirmfreigabe > Meinen Bildschirm freigeben**.





2. Klicken Sie auf **Kopieren und schließen**.

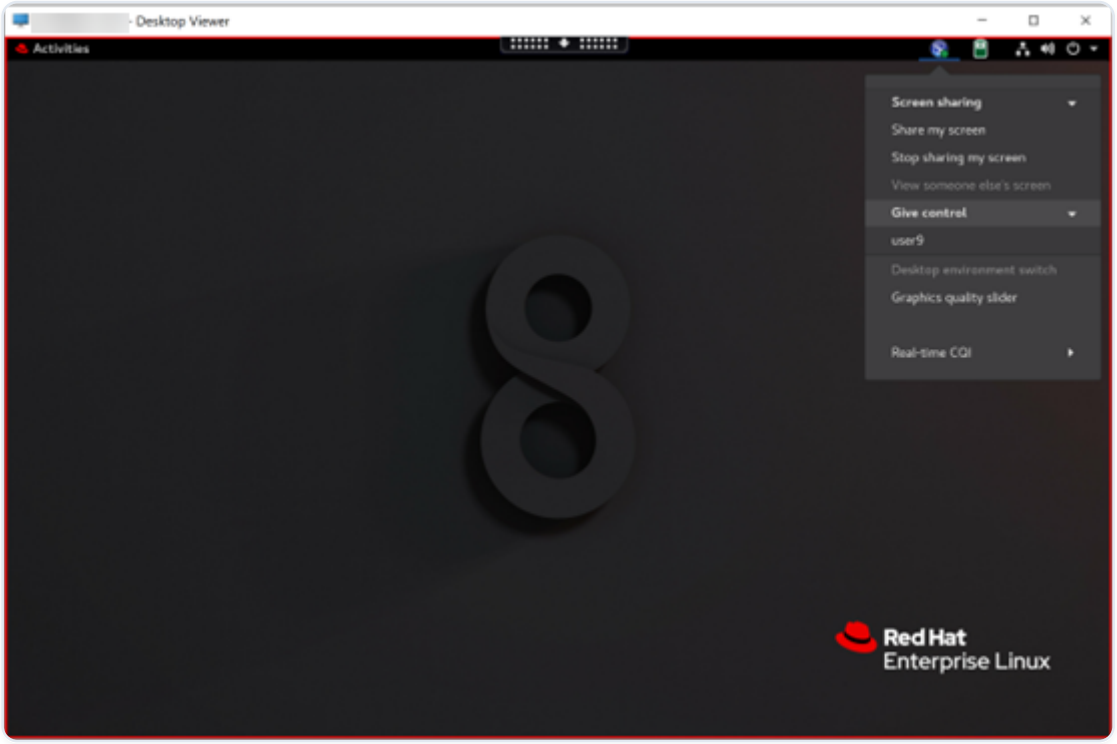
   Der aktuelle Bildschirmfreigabecode bleibt bestehen, bis Sie die Bildschirmfreigabe beenden und neu starten.



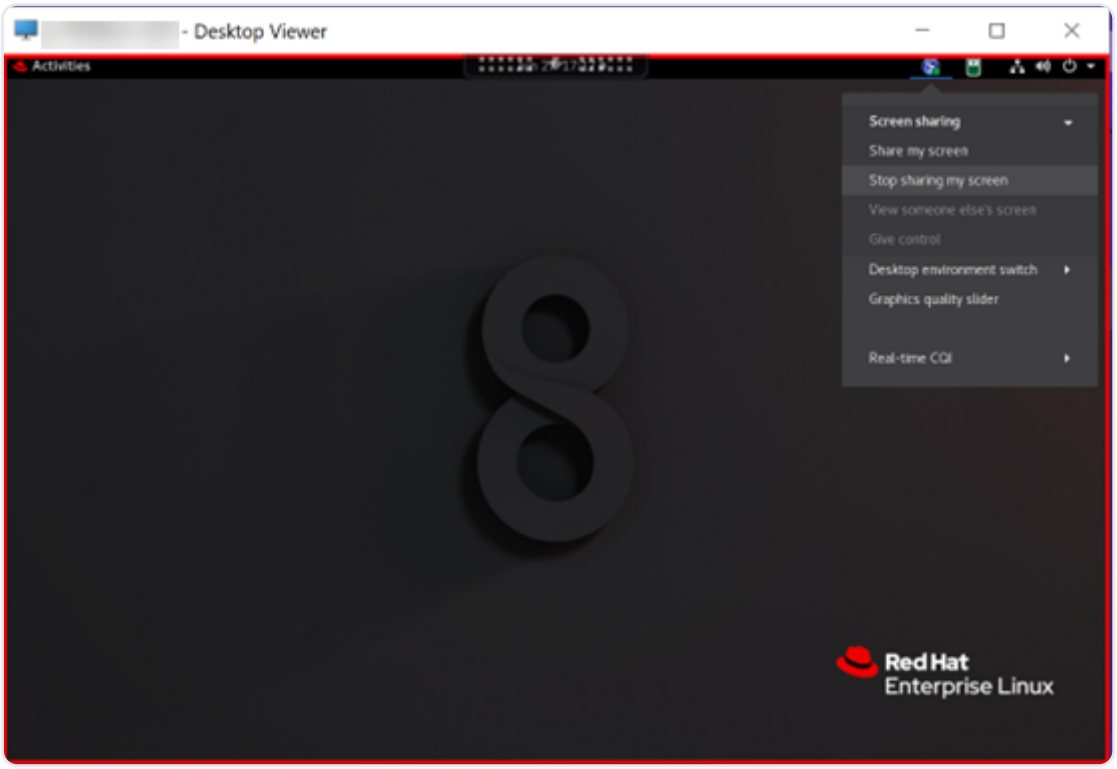
> **Tipp:**

> Während Sie Ihren Bildschirm freigeben, wird er von einem roten Rahmen umgeben, der anzeigt, dass die Freigabe läuft.

3. Geben Sie den kopierten Code für Sitzungsbenutzer auf anderen virtuellen Desktops frei, mit denen Sie Ihren Bildschirm teilen möchten.
4. Um einem Betrachter die Kontrolle über Ihren Bildschirm zu ermöglichen, wählen Sie **Steuerung übergeben** und dann den Namen des Betrachters. Um die Steuerung zu beenden, deaktivieren Sie den Namen des Betrachters.

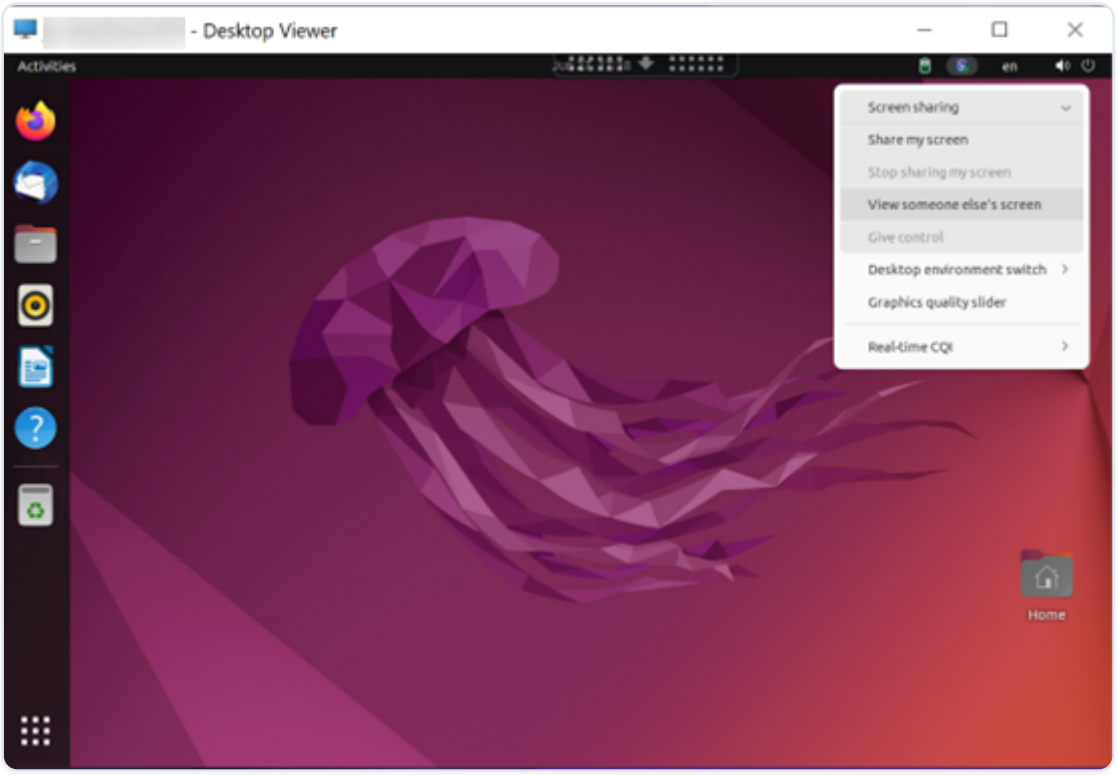


5. Um die Bildschirmfreigabe zu beenden, wählen Sie **Meinen Bildschirm nicht mehr freigeben**.

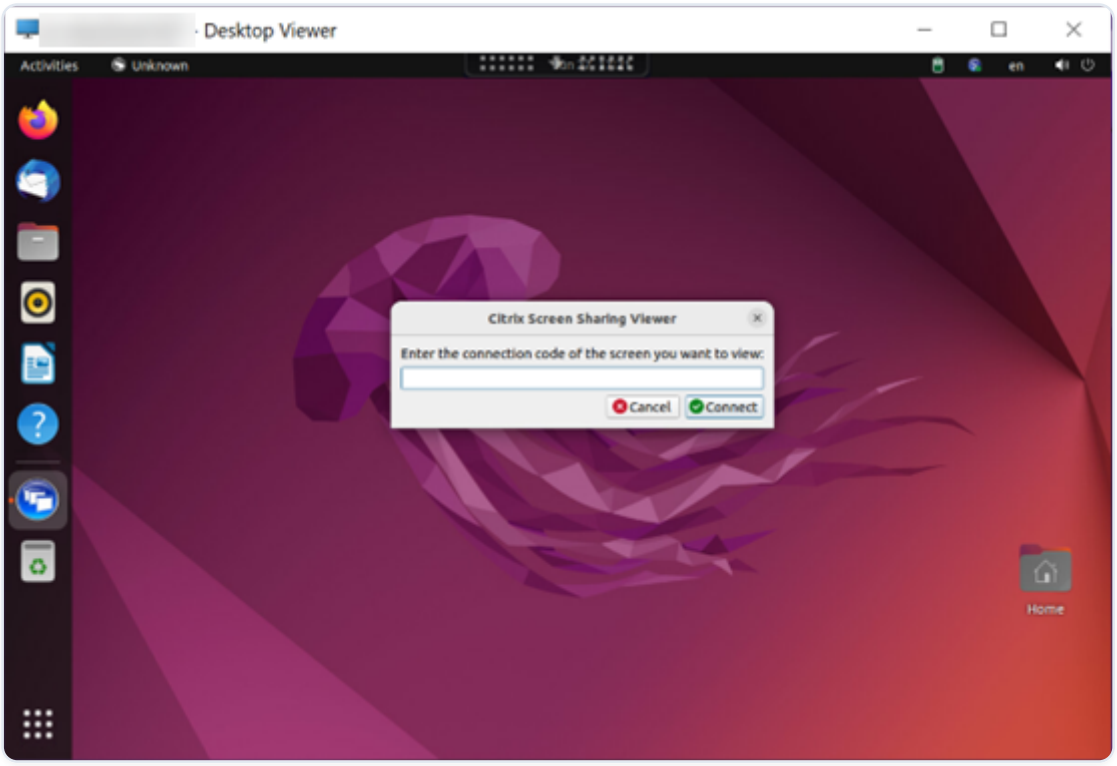


So zeigen Sie den Bildschirm einer anderen Person an:

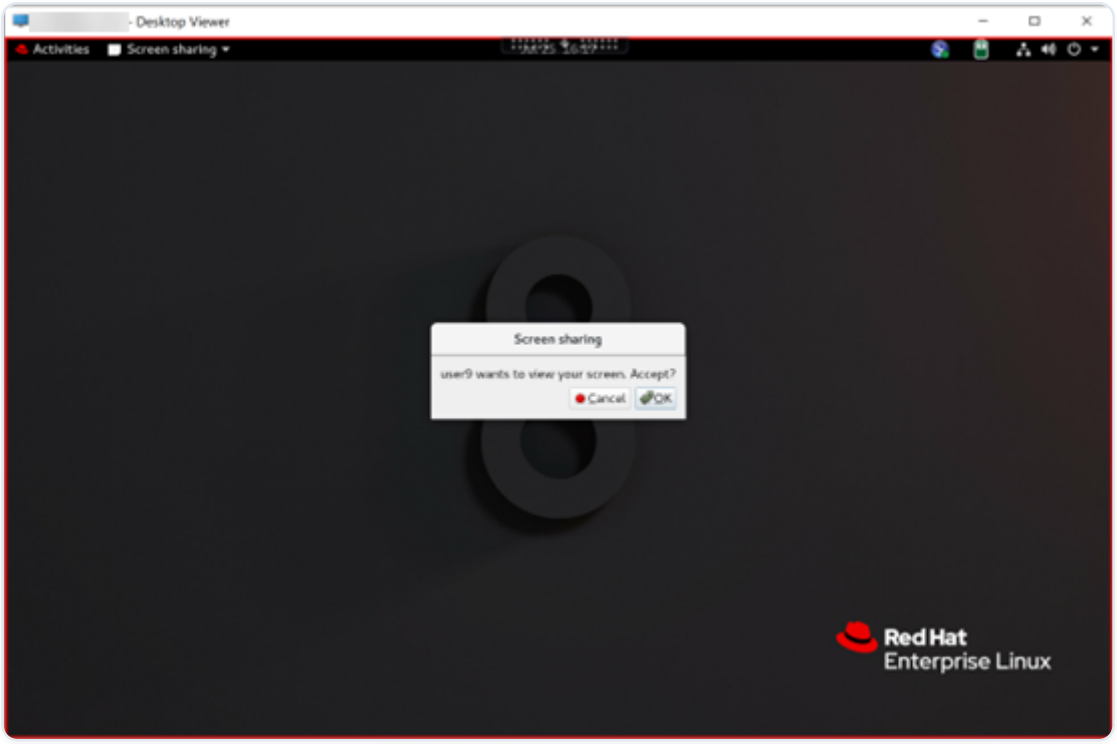
1. Klicken Sie im Infobereich Ihres virtuellen Desktops auf das Symbol für die **Bildschirmfreigabe** und wählen Sie **Bildschirm einer anderen Person anzeigen**.



2. Geben Sie den Verbindungscode des Bildschirms ein, den Sie anzeigen möchten, und klicken Sie dann auf **Verbinden**.



3. Warten Sie, bis der Bildschirmfreigebende Ihre Anfrage akzeptiert. Beispiel:

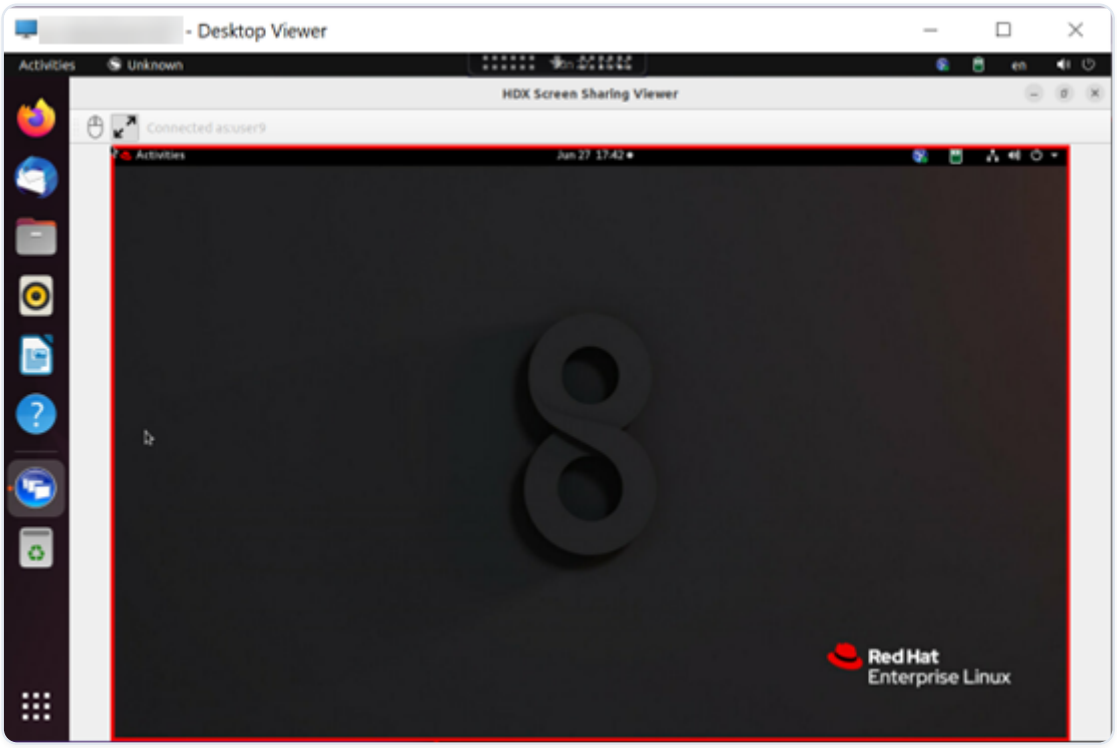


Tipp:

- Auf der Seite des Freigebenden gibt das Linux-System eine Benachrichtigung über Ihre Anfrage aus.

- Wenn der Freigebende Ihre Anfrage nicht innerhalb von 30 Sekunden akzeptiert, läuft Ihre Anfrage ab und eine Eingabeaufforderung wird angezeigt.

4. Nachdem der Bildschirmfreigebende Ihre Anfrage durch Klicken auf **OK** akzeptiert hat, wird der freigegebene Bildschirm in Ihrem Desktop Viewer angezeigt. Sie sind als Betrachter mit einem automatisch zugewiesenen Benutzernamen verbunden.

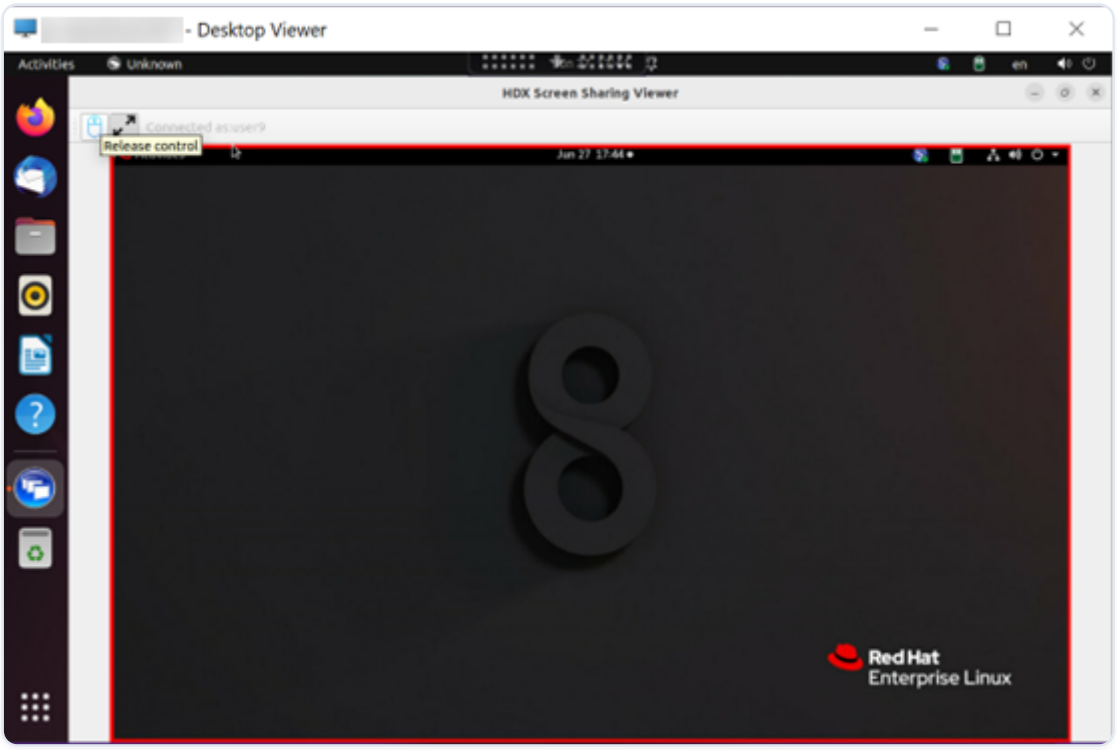


5. Um die Kontrolle über den freigegebenen Bildschirm anzufordern, klicken Sie auf das Maussymbol in der oberen linken Ecke.

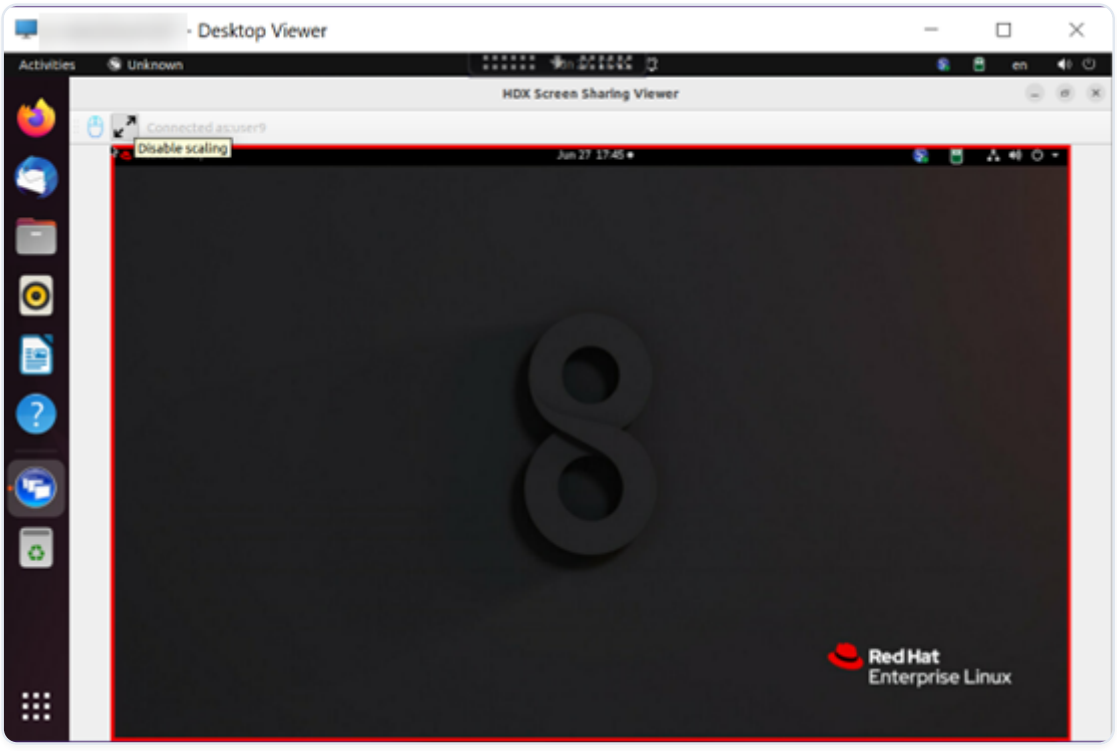
Tipp:

- Wenn der Freigebende Ihre Anfrage nicht innerhalb von 30 Sekunden akzeptiert, läuft Ihre Anfrage ab.
- Es ist jeweils nur einem Betrachter gestattet, einen freigegebenen Bildschirm zu steuern.

Klicken Sie erneut auf das Maussymbol, um die Kontrolle über den freigegebenen Bildschirm freizugeben.



6. Um die Anzeigeskalierung zu deaktivieren oder an die Fenstergröße anzupassen, klicken Sie auf das Symbol neben dem Maussymbol.



Konfiguration

Die Bildschirmfreigabefunktion ist standardmäßig deaktiviert. Um sie zu aktivieren, nehmen Sie die folgenden Einstellungen vor:

1. Aktivieren Sie die Richtlinie für die Grafikanzeige in Citrix Studio.

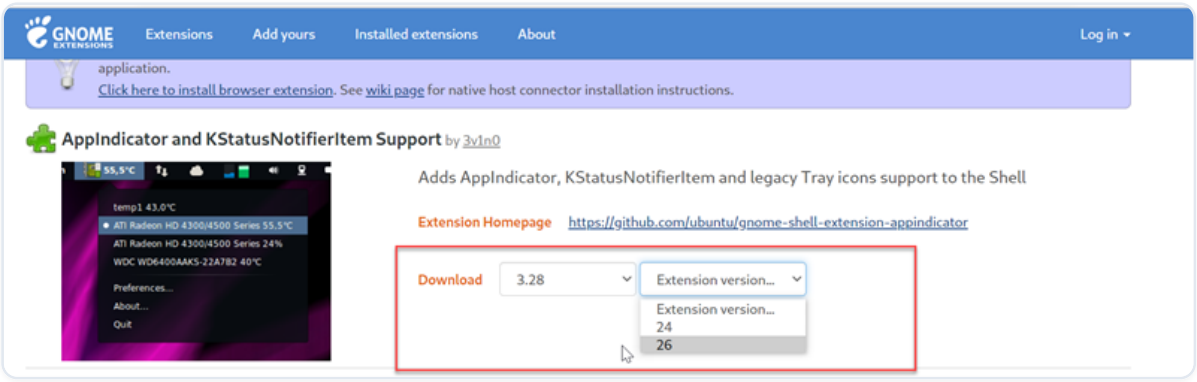
2. Aktivieren Sie für Citrix Virtual Apps and Desktops™ 2112 und höher die Richtlinie **ScreenSharing** in Citrix Studio.
3. (Optional) Aktivieren Sie für Citrix Virtual Apps™ and Desktops 2109 und früher die Bildschirmfreigabe auf dem Linux VDA, indem Sie den folgenden Befehl ausführen:

```
sudo /opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -v
"EnableScreenSharing" -d "0x00000001"
```

4. Lassen Sie die Ports 52525–52625 in Ihrer Firewall zu.
5. (Optional) Wenn Sie RHEL 8.x, Debian 11 oder SUSE 15.x mit GNOME verwenden, installieren Sie eine kompatible Erweiterung für Ihre GNOME Shell, um die AppIndicator-Unterstützung zu aktivieren:

   a. Führen Sie den Befehl `gnome-shell --version` aus, um Ihre GNOME Shell-Version zu überprüfen.

   b. Laden Sie eine kompatible Erweiterung für Ihre GNOME Shell von `<https://extensions.gnome.org/extension/615/appindicator-support>` herunter. Wenn Ihre Shell-Version beispielsweise 3.28 ist, können Sie 24 oder 26 für die Erweiterungsversion auswählen.



   c. Entpacken Sie das heruntergeladene Paket. Vergewissern Sie sich, 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` an den Speicherort unter `/usr/share/gnome-shell/extensions/` zu verschieben.

   e. Führen Sie den Befehl `chmod a+r metadata.json` aus, um die Datei **metadata.json** für andere Benutzer lesbar zu machen.

> **Tipp:**
>
> Standardmäßig ist die Datei **metadata.json** im Verzeichnis `appindicatorsupport@rgcjonas.gmail.com` nur für den Root-Benutzer lesbar. 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 Desktop-Umgebung Ihre GNOME-Shell neu, indem Sie nacheinander die Tasten `Alt+F2`, `r` und `Enter` drücken oder den Befehl `killall -SIGQUIT gnome-shell` ausführen.

h. Führen Sie in der Desktop-Umgebung GNOME Tweaks aus und aktivieren Sie dann **KStatusNotifierItem/AppIndicator Support** im Tweaks-Tool.

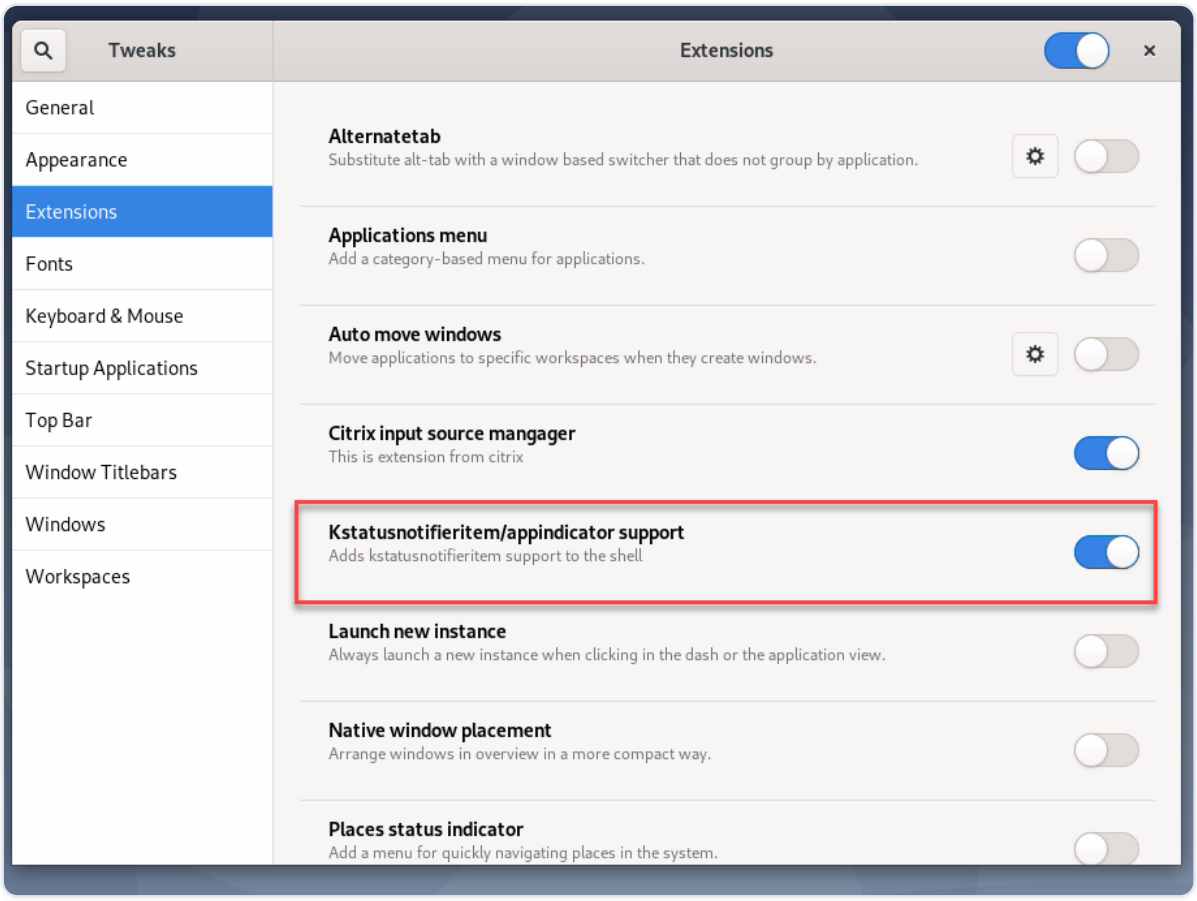
6. (Optional) Wenn Sie Debian 11.3 mit GNOME verwenden, führen Sie die folgenden Schritte aus, um GNOME-Systemleistensymbole zu installieren und zu aktivieren:

   a. Führen Sie den Befehl `sudo apt install gnome-shell-extension-appindicator` aus. Möglicherweise müssen Sie sich ab- und wieder anmelden, damit GNOME die Erweiterung erkennt.

   b. Suchen Sie in Ihrem **Aktivitäten**-Bildschirm nach Tweaks.

   c. Wählen Sie **Erweiterungen** im Tweaks-Tool.

   d. Aktivieren Sie **Kstatusnotifieritem/appindicator support**.



Überlegungen

- Die Bildschirmfreigabefunktion unterstützt den H.265-Videocodec nicht.
- Die Bildschirmfreigabefunktion ist für App-Sitzungen nicht verfügbar.
- Benutzer von Desktopsitzungen können ihre Sitzungsbildschirme standardmäßig mit bis zu 10 Betrachtern teilen. Die maximale Anzahl der Betrachter kann über `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -v "ScreenSharingViewerMaxNum" -d <hex_value>` konfiguriert werden. Wenn die maximale Anzahl erreicht ist, wird eine Aufforderung angezeigt, wenn Benutzer versuchen, zusätzliche Verbindungsanfragen anzunehmen.

Multi-Monitor-Unterstützung

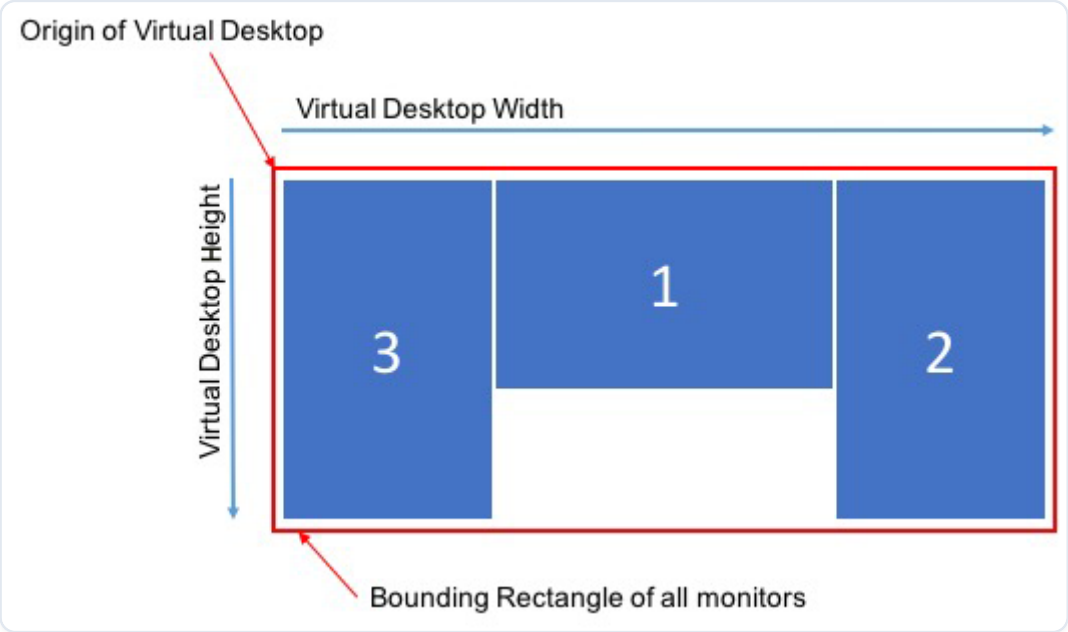
Übersicht

Der Linux VDA bietet sofortige Multi-Monitor-Unterstützung 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.

Dieser Artikel beschreibt, wie der Linux VDA für verschiedene Monitorauflösungen und -layouts konfiguriert wird.

Virtueller Sitzungsdesktop

Wie der Windows VDA verfügt auch der Linux VDA über das Konzept eines virtuellen Multi-Monitor-Desktops. Dieser basiert auf dem umschließenden Rechteck aller Monitore, nicht auf dem tatsächlichen Layout der Monitore. Somit kann der Bereich des virtuellen Desktops theoretisch größer sein als der von den Monitoren des Clients abgedeckte Bereich.



Größe des virtuellen Sitzungsdesktops

Der Ursprung des virtuellen Sitzungsdesktops wird aus der oberen linken Ecke des umschließenden Rechtecks aller Monitore berechnet. Dieser Punkt befindet sich bei X = 0, Y = 0, wobei X und Y die horizontale bzw. vertikale Achse sind.

Die Breite des virtuellen Sitzungsdesktops ist der horizontale Abstand in Pixeln vom Ursprung zur oberen rechten Ecke des umschließenden Rechtecks aller Monitore.

Ähnlich ist die Höhe des virtuellen Sitzungsdesktops der vertikale Abstand in Pixeln vom Ursprung zur unteren linken Ecke des umschließenden Rechtecks aller Monitore.

Diese Berechnung ist aus den folgenden Gründen wichtig:

- Ermöglichen unterschiedlicher Client-Monitor-Layouts
- Verständnis der Speichernutzung auf dem Linux VDA

Ermöglichen unterschiedlicher Client-Monitor-Konfigurationen

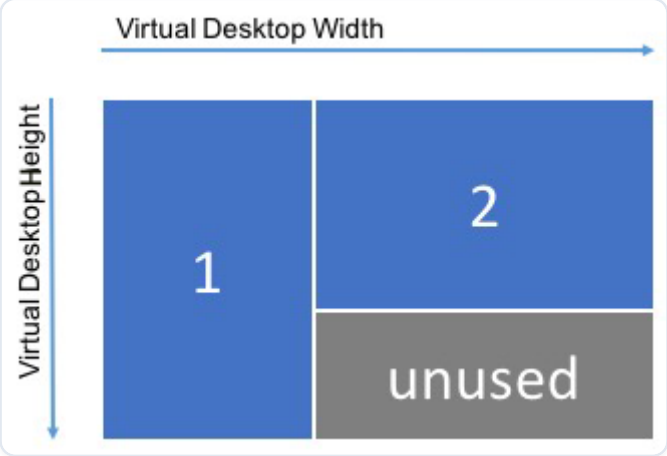
Wenn Sie die maximale Größe des virtuellen Desktops für Ihre verschiedenen Client-Monitor-Konfigurationen kennen, können Sie den Linux VDA so konfigurieren, dass er flexibel auf Client-Monitor-Konfigurationen reagiert.

Betrachten Sie die folgende Client-Monitor-Konfiguration:



Das obige Diagramm zeigt eine sofort einsatzbereite Multi-Monitor-Konfiguration mit zwei Monitoren, jeder mit einer Auflösung von 2560×1600.

Stellen Sie sich nun vor, Sie verbinden sich mit demselben Linux VDA mit der folgenden Client-Monitor-Konfiguration:



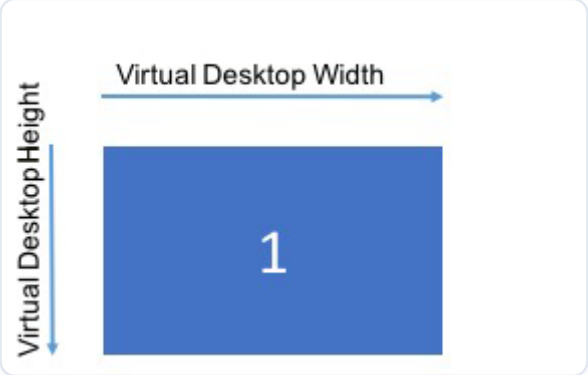
Wenn jeder Monitor im obigen Diagramm eine Auflösung von 2560×1600 hat, sind die sofort einsatzbereiten Multi-Monitor-Konfigurationsparameter unzureichend. Die maximale Höhe ist zu gering, um den virtuellen Sitzungsdesktop für dieses Monitorlayout aufzunehmen. Um die Client-Monitor-Konfiguration in diesem Beispiel zu berücksichtigen, müssen Sie den virtuellen Desktop des Linux VDA auf eine Größe von 4160×2560 einstellen.

Für die größte Flexibilität in einer Multi-Monitor-Konfiguration finden Sie das kleinste umschließende Rechteck aller Monitorlayouts, die Sie unterstützen möchten. Für Konfigurationen mit zwei 2560×1600-Monitoren umfassen die möglichen Layouts:

- **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 zu berücksichtigen, benötigen Sie einen virtuellen Sitzungsdesktop von 5120×2560. Dies ist das kleinste umschließende Rechteck, das alle gewünschten Layouts enthalten kann.

Wenn alle Ihre Benutzer nur einen Monitor im typischen Querformat haben, stellen Sie die maximale Größe des virtuellen Desktops auf die höchste Auflösung des Monitors ein.



In diesem Beispiel muss der virtuelle Desktop auf eine Größe von 2560×1600 eingestellt werden. Da die Standardkonfiguration 5120×1600 und 2 Monitore beträgt, ist eine Konfigurationsänderung erforderlich, um die Speichernutzung für Einzelmonitor-Bereitstellungen zu optimieren.

> **Hinweis:**

> Wenn ein Desktop in einem Multi-Monitor-Setup mit einer falschen Auflösung angezeigt wird, 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

Die Kenntnis der Größe des virtuellen Desktops ermöglicht es Ihnen, die Speichermenge zu berechnen, die von jeder HDX-Sitzung verwendet wird. Dieser Speicher ist der Speicher, der jeder Sitzung für ihre Grafikdaten zugewiesen wird, wenn die Sitzung beginnt. Er ändert sich nicht während der gesamten Lebensdauer der Sitzung. Obwohl dieser Speicher nicht die gesamte für die Sitzung verwendete Speichermenge ist, ist er die einfachste Methode zur Berechnung des Speicherverbrauchs pro Sitzung.

Um zu berechnen, wie viel Speicher jeder HDX-Sitzung zugewiesen wird, verwenden Sie die folgende Formel:

M = X × Y × Z,

Wo:

- **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 ist in Bytes, nicht in Bits, verwenden Sie daher 4 für 32-Bit-Farbe.

HINWEIS:

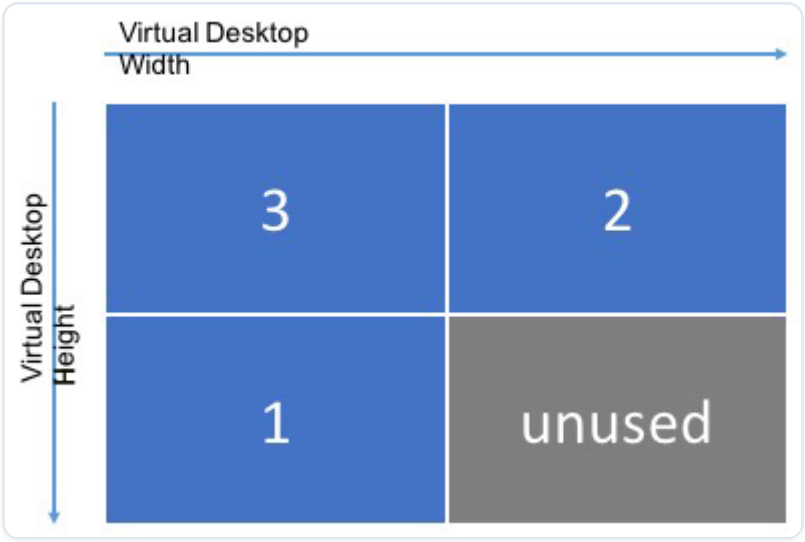
Die Farbtiefe des X-Servers beginnt und kann sich während der Lebensdauer der Sitzung nicht ändern (**vom Login über Trennungen/Wiederverbindungen bis zum Logoff**). Daher weist der Linux VDA den virtuellen Sitzungsdesktop immer als 32-Bit zu und skaliert auf die für die Sitzung angeforderte Farbtiefe herunter.

Zum Beispiel beträgt für eine 1024×768-Sitzung der verwendete Speicher:

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 Client-Monitor-Konfiguration:



Wenn jeder Monitor eine Auflösung von 2560×1600 hat, muss die Größe des virtuellen Sitzungsdesktops 5120×3200 betragen, um diese Client-Monitor-Konfiguration zu berücksichtigen.

Beachten Sie, dass der graue Bereich ungenutzt ist und 16.384.000 (d.h. 2560 x 1600 x 4) Bytes verschwendeten Speichers entspricht.

Citrix® Multi-Monitor-Konfigurationsparameter

Sie können die Multi-Monitor-Funktionalität des Linux VDA mithilfe der folgenden Konfigurationsparameter steuern:

- `MaxScreenNum`

  Parameter: HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/Thinwire/MaxScreenNum

  Beschreibung: Anzahl der zu unterstützenden Monitore

  Typ: DWORD

  Standard: 2

  Maximal: 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

  Maximal: 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

  Standardwert: 1.600

  Maximalwert: 16.384 (8.192 x 2)

Ändern der Linux VDA Multi-Monitor-Konfiguration

Der folgende Abschnitt beschreibt, wie Sie die Multi-Monitor-Funktionalität auf dem Linux VDA aktivieren, konfigurieren und deaktivieren.

Legen Sie die maximale Anzahl der Monitore fest mit:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE
\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"MaxScreenNum" -d "NumMons" --force
```

Dabei ist `NumMons` ein Wert zwischen 1 und 9 für Standard-VDA oder 1 und 4 für HDX 3D Pro VDA.

Legen Sie die maximale Breite eines virtuellen Sitzungsdesktops fest mit:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE
\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"MaxFbWidth" -d " MaxWidth" --force
```

Dabei ist `MaxWidth` ein Wert zwischen `1,024` und `16,384`.

Legen Sie die maximale Höhe eines virtuellen Sitzungsdesktops fest mit:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE
\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v
"MaxFbHeight" -d " MaxHeight" --force
```

Dabei ist `MaxHeight` ein Wert zwischen `1,024` und `16,384`.

Nicht-virtualisierte GPUs

In der Linux VDA-Dokumentation beziehen sich nicht-virtualisierte GPUs auf:

- GPUs, die in Remote PC Access-Szenarien verwendet werden
- GPUs, die von einem Hypervisor durchgereicht werden

Dieser Artikel enthält Informationen zur Unterstützung nicht-virtualisierter GPUs.

HDX™ 3D Pro für NVIDIA GPUs aktivieren, die das NVIDIA Capture SDK für Linux unterstützen

Für NVIDIA GPUs, die das NVIDIA Capture SDK für Linux unterstützen, aktivieren Sie HDX 3D Pro einfach, indem Sie **CTX_XDL_HDX_3D_PRO** bei der Installation des Linux VDA auf **Y** setzen. Es ist keine zusätzliche Konfiguration erforderlich. Die Hardwarebeschleunigung ist standardmäßig aktiviert, nachdem Sie HDX 3D Pro aktiviert haben.

Kompatibel mit NVIDIA GPUs, die das NVIDIA Capture SDK für Linux nicht unterstützen, und GPUs anderer Hersteller wie AMD und Intel

> **Hinweis:**
>
> In diesem Szenario wird nur Software-Kodierung unterstützt.

Schritt 1: Setzen Sie CTX_XDL_HDX_3D_PRO bei der Installation des Linux VDA auf Y

Informationen zu Umgebungsvariablen finden Sie unter Schritt 8: Einrichten der Laufzeitumgebung zur Vervollständigung der Installation.

Schritt 2: Xdamage installieren

Sie können beispielsweise **sudo apt-get install -y libxdamage1** ausführen, um XDamage unter Ubuntu 20.04 zu installieren. Typischerweise existiert XDamage als Erweiterung von XServer.

Schritt 3: XDamage durch Ausführen des folgenden Befehls aktivieren

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
"REG_DWORD" -v "XDamageEnabled" -d "0x00000001" --force
```

Schritt 4: Xorg-Konfigurationsdateien ändern

Die folgenden vier Vorlagen-Konfigurationsdateien finden Sie unter **/etc/X11**. Je nach Anzahl der angeschlossenen Monitore ändern Sie eine der Vorlagen-Konfigurationsdateien mit der entsprechenden Nummer im Namen. Wenn beispielsweise nur ein Monitor angeschlossen ist, ändern Sie die Vorlagen-Konfigurationsdatei mit der Nummer 1 im Namen, d. h. ctx-driver_name-1.conf. Wenn zwei Monitore angeschlossen sind, ändern Sie die Vorlagen-Konfigurationsdatei mit der Nummer 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

Am Beispiel von **ctx-driver_name-1.conf** gehen Sie wie folgt vor, um die Vorlagen-Konfigurationsdateien zu ändern:

1. Ersetzen Sie ***driver_name*** durch Ihren tatsächlichen Treibernamen.

   Wenn Ihr Treibername beispielsweise `intel` lautet, können Sie den Namen der Konfigurationsdatei in `ctx-intel-1.conf` ändern.

2. Fügen Sie die Informationen zum Videotreiber hinzu.

   Jede Vorlagen-Konfigurationsdatei enthält einen Abschnitt namens „Device“, der auskommentiert ist. Dieser Abschnitt beschreibt die Informationen zum Videotreiber. Aktivieren Sie diesen Abschnitt, bevor Sie Ihre Videotreiberinformationen hinzufügen. So aktivieren Sie diesen Abschnitt:

   a. Informationen zur Konfiguration finden Sie im Handbuch des GPU-Herstellers. Eine native Konfigurationsdatei kann generiert werden. Stellen Sie sicher, dass Ihre GPU in einer lokalen Umgebung mit der nativen Konfigurationsdatei funktioniert.

   b. Kopieren Sie den Abschnitt „Device“ der nativen Konfigurationsdatei in **ctx-driver_name-1.conf**.

3. Führen Sie den folgenden Befehl aus, um den Registrierungsschlüssel festzulegen, damit der Linux VDA den in Schritt 1 festgelegten Namen der Konfigurationsdatei erkennen kann.

   ```
   /opt/Citrix/VDA/bin/ctxreg create -k
   "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\XDamage" -t
   "REG_SZ" -v "DriverName" -d "intel" --force
   ```

Monitorabschaltung für Remote-PC-Zugriff-VDAs

Der Linux VDA unterstützt die physische Monitorabschaltung für Remote-PC-Zugriff-VDAs, die nicht-virtualisierte GPUs verwenden.

Vollständig getestete Linux-Distributionen, die die Funktion unterstützen, sind Ubuntu 20.04 und Debian 11.3.

Die Funktion ist standardmäßig deaktiviert. Um sie zu aktivieren, führen Sie die folgenden zwei Schritte aus:

1. Installieren Sie das `evdi-dkms`-Paket basierend auf Ihrer Linux-Distribution:

   ```
   sudo apt install evdi-dkms
   ```

2. Aktivieren Sie die Auslagerung 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
   ```

3. Wenn Sie eine Intel-GPU verwenden, deaktivieren Sie den Display-Manager. Andernfalls belegt der Display-Manager die Intel-GPU und macht sie für Citrix®-Remotesitzungen unzugänglich.

   ```
   sudo systemctl disable --now gdm
   ```

Problembehandlung

Keine oder fehlerhafte Grafikausgabe

Wenn Sie 3D-Anwendungen lokal ausführen können und alle Konfigurationen korrekt sind, ist eine fehlende oder fehlerhafte Grafikausgabe das Ergebnis eines Fehlers. Verwenden Sie /opt/Citrix/VDA/bin/setlog und setzen Sie GFX_X11 auf verbose, um die Trace-Informationen für das Debugging zu sammeln.

Sitzungswasserzeichen

Das Sitzungswasserzeichen hilft, Datendiebstahl abzuschrecken und dessen Nachverfolgung zu ermöglichen. Nachverfolgbare Informationen erscheinen auf Sitzungsdesktops als Abschreckung für Benutzer, die Fotos und Bildschirmaufnahmen verwenden, um Daten zu stehlen. Sie können ein Wasserzeichen als Textebene oder als PNG-Bild mit Alphakanal angeben. Das Wasserzeichen wird über dem gesamten Sitzungsbildschirm angezeigt, ohne den Inhalt des Originaldokuments zu ändern.

Wichtig:

> Das Sitzungswasserzeichen ist keine Sicherheitsfunktion. Es verhindert Datendiebstahl nicht vollständig, bietet aber ein gewisses Maß an Abschreckung und Nachverfolgbarkeit. Wir garantieren keine vollständige Nachverfolgbarkeit von Informationen bei Verwendung dieser Funktion. Stattdessen empfehlen wir, diese Funktion gegebenenfalls mit anderen Sicherheitslösungen zu kombinieren.

> Das Sitzungswasserzeichen enthält Informationen zur Nachverfolgung von Datendiebstahl. Die wichtigsten Daten sind die Identität des Benutzers, nachverfolgt durch dessen Anmeldeinformationen, der Sitzung, in der das Bildschirmbild aufgenommen wurde. Um Datenlecks effektiver nachzuverfolgen, fügen Sie weitere Informationen hinzu, wie die Internetprotokolladresse des Servers oder Clients und eine Verbindungszeit.

Um die Benutzererfahrung anzupassen, verwenden Sie die folgenden Richtlinieneinstellungen für Sitzungswasserzeichen, um die Platzierung und das Erscheinungsbild des Wasserzeichens auf dem Bildschirm zu konfigurieren:

Richtlinieneinstellungen für Sitzungswasserzeichen

Sitzungswasserzeichen aktivieren

Wenn Sie diese Einstellung aktivieren, zeigt die Sitzungsanzeige ein undurchsichtiges Wasserzeichen mit sitzungsspezifischen Informationen an. Die anderen Wasserzeicheneinstellungen hängen davon ab, dass diese aktiviert ist.

Standardmäßig ist das Sitzungswasserzeichen deaktiviert.

Client-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, zeigt die Sitzung die aktuelle Client-IP-Adresse als Wasserzeichen an.

Standardmäßig ist **Client-IP-Adresse einschließen** deaktiviert.

Verbindungszeit einschließen

Wenn Sie diese Einstellung aktivieren, zeigt das Sitzungswasserzeichen eine Verbindungszeit an. Das Format ist JJJJ/MM/TT HH:MM. Die angezeigte Zeit basiert auf der Systemuhr und der Zeitzone.

Standardmäßig ist **Verbindungszeit einschließen** deaktiviert.

Anmeldebenutzernamen einschließen

Wenn Sie diese Einstellung aktivieren, zeigt die Sitzung den aktuellen Anmeldebenutzernamen als Wasserzeichen an. Das Anzeigeformat ist BENUTZERNAME@DOMÄNENNAME. Wir empfehlen, dass der Benutzername maximal 20 Zeichen lang ist. Wenn ein Benutzername länger als 20 Zeichen ist, können kleinere Schriftgrößen oder eine Kürzung auftreten, was die Wirksamkeit des Wasserzeichens verringert.

Standardmäßig ist **Anmeldebenutzername einschließen** aktiviert.

VDA-Hostnamen einschließen

Wenn Sie diese Einstellung aktivieren, zeigt die Sitzung den VDA-Hostnamen der aktuellen ICA®-Sitzung als Wasserzeichen an.

Standardmäßig ist **VDA-Hostname einschließen** aktiviert.

VDA-IP-Adresse einschließen

Wenn Sie diese Einstellung aktivieren, zeigt die Sitzung die VDA-IP-Adresse der aktuellen ICA-Sitzung als Wasserzeichen an.

Standardmäßig ist **VDA-IP-Adresse einschließen** deaktiviert.

Sitzungswasserzeichenstil

Diese Einstellung steuert, ob Sie eine einzelne Wasserzeichen-Textbeschriftung oder mehrere Beschriftungen anzeigen. Wählen Sie **Mehrfach** oder **Einzeln** aus dem Dropdown-Menü **Wert**. Weitere Stiloptionen finden Sie im Abschnitt **Benutzerdefinierter Wasserzeichentext** in diesem Artikel.

Mehrfach zeigt fünf Wasserzeichenbeschriftungen in der Sitzung an. Eine in der Mitte und vier in den Ecken.

Einfach zeigt eine einzelne Wasserzeichenbeschriftung in der Mitte der Sitzung an.

Standardmäßig ist der **Sitzungswasserzeichenstil Mehrfach**.

Transparenz des Wasserzeichens

Sie können die Wasserzeichen-Deckkraft von 0 bis 100 angeben. Je größer der angegebene Wert, desto undurchsichtiger ist das Wasserzeichen.

Standardmäßig ist der Wert 17.

Benutzerdefinierter Wasserzeichentext

Der Wert ist standardmäßig leer. Sie können eine nicht leere Zeichenfolge eingeben, eine Syntax zum Bilden einer Zeichenfolge festlegen oder die Kombination verwenden, um sie im Sitzungswasserzeichen anzuzeigen. Nicht leere Zeichenfolgen unterstützen bis zu 25 Unicode-Zeichen pro Zeile. Längere Zeichenfolgen werden auf 25 Zeichen gekürzt.

Zum Beispiel können Sie die Richtlinie auf den folgenden Wert setzen:

```
<date>
<time><newline><username><style=single><fontsize=40><font=Ubuntu><position=center><rotation
Linux VDA<newline>Version 2207
```

Eine Beschreibung aller Syntaxoptionen finden Sie in der folgenden Tabelle:

SYNTAXOPTION	BESCHREIBUNG	GÜLTIGE EINSTELLUNG (GROSS-/KLEINSCHREIBUNG BEACHTEN)	STANDARDWERT	ANMERKUNGEN
`<style>`	Layoutstil des Wasserzeichens	`xstyle`, `single`, `tile`, `horizontal`	`xstyle`	-
`<position>`	Position des Wasserzeichens	`center`, `topleft`, `topright`, `bottomleft`, `bottomright`	`center`	Nur gültig, wenn der Layoutstil auf **single** eingestellt ist.
`<rotation>`	Drehung des Wasserzeichens um einen bestimmten Winkel	-180–180	0	-
`<transparency>`	Deckkraft des Wasserzeichens	0–100	17	-

SYNTAXOPTION	BESCHREIBUNG	GÜLTIGE EINSTELLUNG (GROSS-/KLEINSCHREIBUNG BEACHTEN)	STANDARDWERT	ANMERKUNGEN
`<font>`	-	Eine vom System unterstützte Schriftart	Sans	-
`<fontsize>`	-	20–50	0 (automatisch berechnet)	-
`<fontzoom>`	Prozentsatz der Schrift- und Bildgrößen, die Sie über `<fontsize>` und `<image>` festlegen	0 –	100	-
`<image>`	PNG-Wasserzeichen	Pfad zu einem PNG-Bild auf dem VDA	N/A	Diese Syntax konfiguriert ein PNG-Wasserzeichen. Es werden nur PNGs mit Alphakanal unterstützt. Wenn ein PNG-Wasserzeichen verwendet wird, sind nur die Syntaxoptionen `<style>`, `<position>`, `<rotation>`, `<transparency>` und `<fontzoom>` wirksam.

SYNTAXOPTION	BESCHREIBUNG	GÜLTIGE EINSTELLUNG (GROSS-/KLEINSCHREIBUNG BEACHTEN)	STANDARDWERT	ANMERKUNGEN
`<date>`	Platzhalter für das Sitzungsverbindungsdatum (JJJJ/MM/TT)	N/A	N/A	-
`<time>`	Platzhalter für die Sitzungsverbindungszeit (HH:MM)	N/A	N/A	-
`<domain>`	Platzhalter für die Benutzerkontodomäne	N/A	N/A	-
`<username>`	Platzhalter für den aktuellen Anmeldebenutzernamen (ohne die Benutzerkontodomäne)	N/A	N/A	-
`<hostname>`	Platzhalter für den Hostnamen des VDA	N/A	N/A	-
`<clientip>`	Platzhalter für die IP-Adresse des Clients	N/A	N/A	-
`<serverip>`	Platzhalter für die IP-Adresse des VDA	N/A	N/A	-

> **Hinweis:**

> Wenn **Benutzerdefinierter Wasserzeichentext** mit einer gültigen Syntaxeinstellung angegeben wird, werden alle anderen Sitzungswasserzeichenrichtlinien – mit Ausnahme von **Sitzungswasserzeichen aktivieren** – ignoriert.

> Wenn Sie eine Syntaxoption nicht angeben oder auf einen nicht unterstützten Wert setzen, wird der Standardwert verwendet.

Einschränkungen

- Das Sitzungswasserzeichen wird in einem der folgenden Fälle unterstützt:
  - Wenn **Videocodec für Komprimierung verwenden** auf **Für den gesamten Bildschirm** eingestellt ist.
  - Wenn **Videocodec für Komprimierung verwenden** auf **Verwenden, wenn bevorzugt** eingestellt und Für 3D-Grafik-Workload optimieren aktiviert ist.
- Das Sitzungswasserzeichen wird in Sitzungen, in denen die Browserinhaltsumleitung verwendet wird, nicht unterstützt. Um die Sitzungswasserzeichenfunktion zu verwenden, stellen Sie sicher, dass die Browserinhaltsumleitung deaktiviert ist.
- Das Sitzungswasserzeichen wird nicht unterstützt und erscheint nicht, wenn die Sitzung im hardwarebeschleunigten H.264- oder H.265-Vollbild-Codierungsmodus mit älteren NVIDIA-Treibern ausgeführt wird. (In diesem Fall ist NvCaptureType in der Registrierung auf 2 gesetzt.)
- Das Wasserzeichen ist bei der Sitzungsschattenfunktion nicht sichtbar.
- Wenn Sie die Drucktaste drücken, um einen Bildschirm zu erfassen, enthält der auf der VDA-Seite erfasste Bildschirm das Wasserzeichen nicht. Wir empfehlen Ihnen, Maßnahmen zu ergreifen, um das Kopieren von Bildschirmaufnahmen zu verhindern.

Gemeinsame GPU-Beschleunigung auf einem Multi-Session Linux VDA

HDX™ 3D PRO unterstützt nur die Linux VDAs, die für VDI-Desktops (Einzel-Sitzungs-Modus) konfiguriert sind. Für einen Multi-Session Linux VDA können Sie die gemeinsame GPU-Beschleunigung aktivieren, um OpenGL 3D-Anwendungen zu beschleunigen.

> **Hinweis:**

> Der Wayland-Display-Server wird für die gemeinsame GPU-Beschleunigung nicht unterstützt.

Konfiguration

Um die gemeinsame GPU-Beschleunigung auf einem Multi-Session Linux VDA zur Beschleunigung von OpenGL 3D-Anwendungen zu aktivieren, führen Sie die folgenden Konfigurationsschritte aus:

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-Display-Manager, z. B. LightDM oder GNOME Display Manager (GDM).
2. Führen Sie das VirtualGL-Konfigurationsskript aus, indem Sie Folgendes ausführen:

   ```
   #/opt/VirtualGL/bin/vglserver_config
   ```

   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)“ (Server zur Verwendung mit VirtualGL konfigurieren (GLX + EGL Backends))
   - Wählen Sie „n“ für „Zugriff auf 3D-X-Server auf die Gruppe **vglusers** beschränken“
   - Wählen Sie „n“ für „Zugriff auf Framebuffer-Geräte auf die Gruppe **vglusers** beschränken“
   - Wählen Sie „n“ für „Disable XTEST extension“ (XTEST-Erweiterung deaktivieren)
3. Beenden Sie das Konfigurationsskript und starten Sie den Linux-Display-Manager neu.

Schritt 3: OpenGL-3D-Anwendungen mit GPU-Beschleunigung ausführen

Es gibt zwei Methoden, um OpenGL-3D-Anwendungen mit GPU-Beschleunigung in einer Linux-VDA-Sitzung auszuführen:

- **Methode 1:** Gemeinsame GPU-Beschleunigung für alle OpenGL-3D-Anwendungen aktivieren

Öffnen Sie dazu ein Bash-Terminal auf dem Linux VDA, führen Sie den folgenden Befehl aus und starten Sie das Bash-Terminal anschließend neu. Dieser Ansatz aktiviert die gemeinsame GPU-Beschleunigung für alle OpenGL-3D-Anwendungen, die vom Bash-Terminal aus gestartet werden.

```
#/opt/Citrix/VDA/sbin/ctxgpushare.sh enable
```

- **Methode 2:** Gemeinsame GPU-Beschleunigung für eine bestimmte OpenGL-3D-Anwendung aktivieren:

  Öffnen Sie dazu ein Terminal auf dem Linux VDA und führen Sie den folgenden Befehl mit dem angegebenen Anwendungsnamen aus:

```
#vglrun <AppName>
```

Einschränkungen

- Die gemeinsame GPU-Beschleunigung arbeitet eng mit dem Display-Manager auf dem Linux VDA zusammen. Es wird empfohlen, LightDM als Display-Manager für die gemeinsame GPU-Beschleunigung zu verwenden, um die erwartete Funktionalität und Leistung zu erzielen.
- WebGL-Hardwarebeschleunigung wird nur in Firefox unter Ubuntu und Debian unterstützt.

Skalierbarkeit

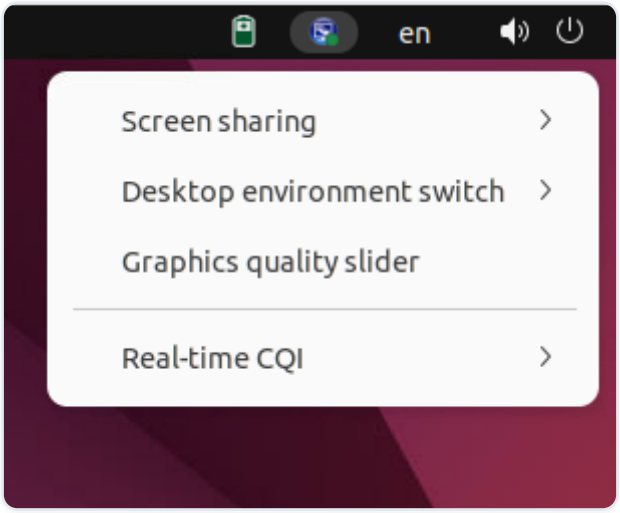
Die maximal unterstützte Anzahl gleichzeitiger Sitzungen, die eine GPU gemeinsam nutzen können, hängt von der CPU und dem Systemspeicher ab. Sie hängt auch stark vom maximalen Videospeicher der GPU ab.

Zum Beispiel:

WENN	DANN
die NVIDIA **M10-2B** vGPU über 2.048 MB Videospeicher verfügt und eine OpenGL-Anwendung wie der VariCAD Viewer 100 MB Videospeicher für ihre Arbeitslast in jeder Sitzung verwendet,	kann die maximal unterstützte Anzahl gleichzeitiger Sitzungen theoretisch 20 nicht überschreiten.

Systemleiste

Sitzungsbenutzer können auf das folgende Symbol in der Systemleiste klicken, um auf die Menüelemente zuzugreifen und die entsprechenden Aktionen auszuführen:



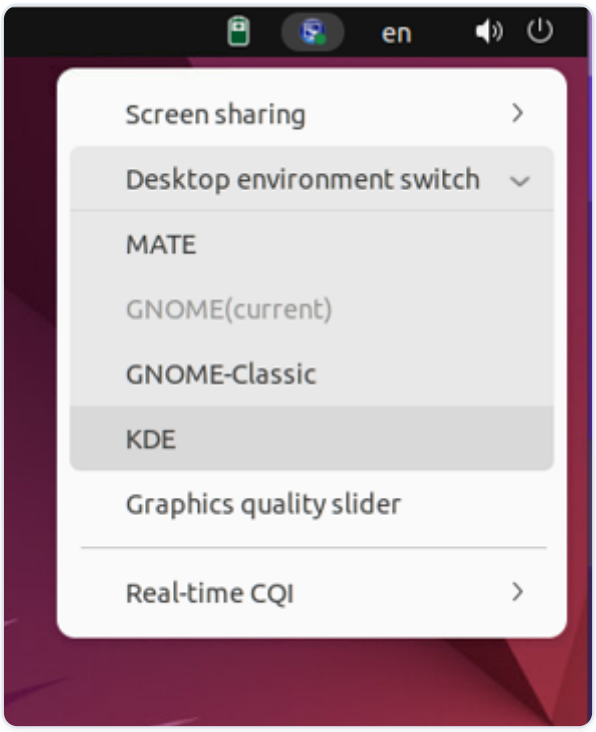
Jedes Menüelement entspricht einer Funktion mit einem Umschalter. Wenn die einem Menüelement entsprechende Funktion deaktiviert ist, wird das Menüelement ausgeblendet und nicht angezeigt.

- **Bildschirmfreigabe**

  Weitere Informationen zu dieser Funktion finden Sie unter HDX-Bildschirmfreigabe.

- **Desktop-Umgebung wechseln**

  Dieses Menüelement ist eine GUI für **ctxdesktopswitch.sh**. Weitere Informationen finden Sie unter Benutzerdefinierte Desktop-Umgebungen für Sitzungsbenutzer.



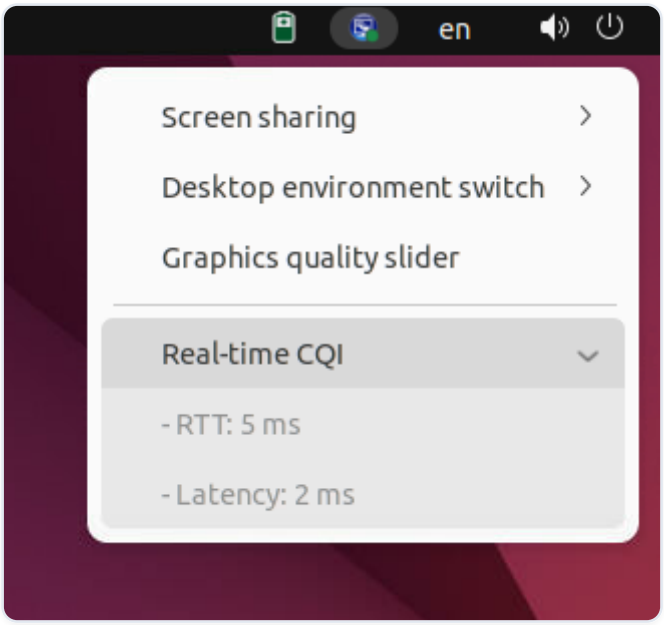
Die Anpassung der Desktop-Umgebung durch Sitzungsbenutzer ist standardmäßig aktiviert. Um sie zu deaktivieren, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "EnableDesktopSwitch" -d "0x00000000" --force
```

- **Schieberegler für Grafikqualität**

  Weitere Informationen finden Sie im Abschnitt Schieberegler für Grafikqualität im Artikel zur Grafikkonsfiguration.

- **Echtzeit-CQI**



Derzeit werden Round Trip Time (RTT)- und Latenzdaten angezeigt. Weitere Informationen finden Sie unter Dienstprogramm zur Abfrage von Sitzungsdaten.

Das Symbol in der Taskleiste wird je nach Echtzeit-CQI-Status unterschiedlich angezeigt:



Es gibt Schwellenwerte, die steuern, wann das Symbol seine Anzeige ändert. Standardmäßig sind sie wie folgt festgelegt:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "HighLatencyThreshold" -d "0x000000dc" --force
```

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "HighRttThreshold" -d "0x00000104" --force
```

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "LowLatencyThreshold" -d "0x00000078" --force
```

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "LowRttThreshold" -d "0x00000096" --force
```

Wenn der tatsächliche RTT kleiner oder gleich **LowRttThreshold** und die tatsächliche Latenz kleiner oder gleich **LowLatencyThreshold** ist, wird das Symbol grün markiert. Wenn der tatsächliche RTT größer als **HighRttThreshold** oder die tatsächliche Latenz größer als **HighLatencyThreshold** ist, wird das Symbol rot markiert. In anderen Fällen wird das Symbol gelb markiert. Wenn der Echtzeit-CQI deaktiviert ist, hat das Symbol keine Farbmarkierung.

Der Echtzeit-CQI ist standardmäßig aktiviert und wird angezeigt. Um ihn zu deaktivieren und auszublenden und das Taskleistensymbol ohne Farbmarkierung anzuzeigen, führen Sie den folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD"
-v "EnableCqiShow" -d "0x00000000" --force
```

Thinwire progressive Darstellung

Die Sitzungsinteraktivität kann sich bei Verbindungen mit geringer Bandbreite oder hoher Latenz verschlechtern. Zum Beispiel kann das Scrollen auf einer Webseite langsam, nicht reagierend oder ruckelig werden. Tastatur- und Mausoperationen können hinter Grafikaktualisierungen zurückbleiben.

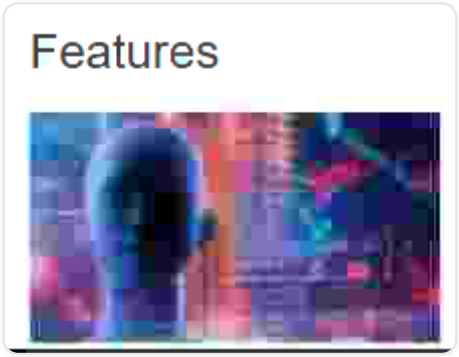
Bis Version 7.17 konnten Sie Richtlinieneinstellungen verwenden, um den Bandbreitenverbrauch zu reduzieren, indem Sie die Sitzung auf die visuelle Qualität **Niedrig** konfigurierten oder eine geringere Farbtiefe (16-Bit- oder 8-Bit-Grafiken) einstellten. Sie mussten jedoch wissen, dass ein Benutzer eine schwache Verbindung hatte. HDX Thinwire passte die statische Bildqualität nicht dynamisch an die Netzwerkbedingungen an.

Ab Version 7.18 wechselt HDX Thinwire standardmäßig in einem der folgenden Fälle in einen progressiven Aktualisierungsmodus:

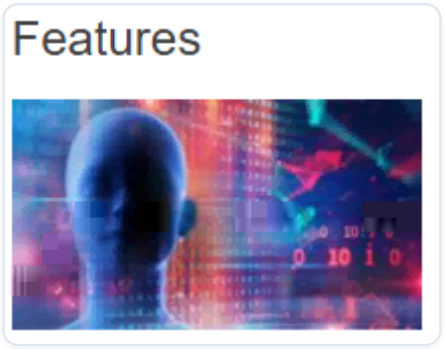
- Die verfügbare Bandbreite unterschreitet 2 Mbit/s.
- Die Netzwerklatenz überschreitet 200 ms.

In diesem Modus:

Zum Beispiel haben in der folgenden Grafik, wo der progressive Aktualisierungsmodus aktiv ist, die Buchstaben **F** und **e** blaue Artefakte, und das Bild ist stark komprimiert. Dieser Ansatz reduziert den Bandbreitenverbrauch erheblich, was den schnelleren Empfang von Bildern und Text ermöglicht und die Sitzungsinteraktivität verbessert.



Wenn Sie die Interaktion mit der Sitzung beenden, werden die verschlechterten Bilder und Texte schrittweise verlustfrei geschärft. Zum Beispiel enthalten in der folgenden Grafik die Buchstaben keine blauen Artefakte mehr, und das Bild erscheint in Quellqualität.



Für Bilder verwendet das Schärfen eine zufällige blockartige Methode. Für Text werden einzelne Buchstaben oder Wortteile geschärft. Der Schärfungsprozess erfolgt über mehrere Frames. Dieser Ansatz vermeidet die Einführung einer Verzögerung durch einen einzelnen großen Schärfungsframe.

Transiente Bilder (Video) werden weiterhin mit adaptiver Anzeige oder selektivem H.264 verwaltet.

Wie der progressive Modus verwendet wird

Standardmäßig ist der progressive Modus für die Richtlinieneinstellungen der **visuellen Qualität** im Standby: **Hoch**, **Mittel** (Standard) und **Niedrig**.

Der progressive Modus wird erzwungen deaktiviert (nicht verwendet), wenn:

- **Visuelle Qualität** = **Immer verlustfrei** oder **Verlustfrei aufbauen**
- **Bevorzugte Farbtiefe für einfache Grafiken** = 8-Bit

- **Videocodec für Komprimierung verwenden** = **Für den gesamten Bildschirm** (wenn H.264 im Vollbildmodus gewünscht wird)

Wenn der progressive Modus im Standby ist, wird er standardmäßig aktiviert, wenn eine der folgenden Bedingungen eintritt:

- Verfügbare Bandbreite fällt unter 2 Mbit/s
- Netzwerklatenz steigt über 200 ms

Nach einem Moduswechsel wird mindestens 10 s in diesem Modus verbracht, selbst wenn die ungünstigen Netzwerkbedingungen nur vorübergehend sind.

Verhalten des progressiven Modus ändern

Sie können das Verhalten des progressiven Modus ändern, indem Sie den folgenden Befehl ausführen:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplay" -d "<value>" --force
```

Wobei \<value\>:

0 = Immer aus (unter keinen Umständen verwenden)

1 = Automatisch (Umschaltung basierend auf Netzwerkbedingungen, Standardwert)

2 = Immer ein

Im automatischen Modus (1) können Sie einen der folgenden Befehle ausführen, um die Schwellenwerte zu ändern, bei denen der progressive Modus umgeschaltet wird:

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
```

Wobei \<value\> der \<Schwellenwert in Kbit/s\> ist (Standard = 2.048)

Beispiel: 4096 = progressiven Modus einschalten, wenn die Bandbreite unter 4 Mbit/s fällt

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\CurrentControlSet\Control\Citrix\Thinwire" -t
"REG_DWORD" -v "ProgressiveDisplayLatencyThreshold" -d "<value>" --force
```

Wobei \<value\> der \<Schwellenwert in ms\> ist (Standard = 200)

Beispiel: 100 = progressiven Modus einschalten, wenn die Netzwerklatenz unter 100 ms fällt.

Allgemeine Inhaltsweiterleitung

Clientlaufwerkszuordnung und Clientordnerumleitung

WENN	DANN
Sie nur die Clientlaufwerkszuordnung auf dem Host (VDA) aktivieren,	clientseitige vollständige Volumes werden automatisch den Sitzungen unter dem Unterverzeichnis **ctxmnt** im Basisverzeichnis zugeordnet.
Sie die Clientordnerumleitung auf dem Host (VDA) aktivieren und der Benutzer sie auf dem Benutzergerät (Client) konfiguriert,	der vom Benutzer angegebene Teil des lokalen Volumes wird umgeleitet.

USB-Geräteumleitung

USB-Geräte werden zwischen der Citrix Workspace™-App und dem Linux VDA-Desktop geteilt. Wenn ein USB-Gerät auf den Desktop umgeleitet wird, können Sie das USB-Gerät verwenden, als wäre es lokal verbunden.

Clientlaufwerkzuordnung

Sie können die Clientlaufwerkzuordnung und die Clientordnerumleitung verwenden, um clientseitige Dateien in der Host-Sitzung zugänglich zu machen. Der Vergleich zwischen Clientlaufwerkzuordnung und Clientordnerumleitung ist wie folgt:

WENN	DANN
Sie nur die Clientlaufwerkzuordnung auf dem Host (VDA) aktivieren,	werden clientseitige vollständige Volumes automatisch den Sitzungen unter dem Unterverzeichnis **ctxmnt** im Basisverzeichnis zugeordnet.

WENN	DANN
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, legen Sie die Richtlinie **Clientlaufwerkumleitung** in Citrix Studio auf **Zulässig** fest. Weitere Informationen zur Richtlinie finden Sie unter Richtlinieneinstellungen für die Dateiumleitung.

Clientordnerumleitung aktivieren und umzuleitende Ordner angeben

Um die Clientordnerumleitung zu aktivieren, führen Sie den 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 "0x00000001" --force
```

Um anzugeben, welche Ordner vom Client zur Host-Sitzung umgeleitet werden sollen, führen Sie die folgenden Schritte auf dem Benutzergerät aus:

1. Stellen Sie sicher, dass die neueste Version der Citrix Workspace™-App installiert ist.
2. Starten Sie aus dem Installationsverzeichnis der Citrix Workspace-App die Datei **CtxCFRUI.exe**.
3. Wählen Sie das Optionsfeld **Benutzerdefiniert** und fügen Sie Ordner hinzu, bearbeiten oder entfernen Sie sie.
4. trennen und verbinden Sie Ihre Sitzungen erneut, damit die Einstellung wirksam wird.

USB-Geräteumleitung

USB-Geräte werden zwischen der Citrix Workspace™-App und dem Linux VDA-Desktop gemeinsam genutzt. Wenn ein USB-Gerät auf den Desktop umgeleitet wird, können Sie das USB-Gerät so verwenden, als wäre es lokal angeschlossen.

Tipp:

> Wir empfehlen die Verwendung der USB-Geräteumleitung, wenn die Netzwerklatenz unter 100 Millisekunden liegt. Verwenden Sie die USB-Geräteumleitung nicht, wenn die Netzwerklatenz über 200 Millisekunden liegt.

> Die USB-Geräteumleitung umfasst drei Hauptfunktionsbereiche:

- Open-Source-USB/IP-Projekt
- Citrix USB-Sitzungsmodul
- Citrix USB-Dienstmodul

Open-Source-USB/IP-Projekt:

Das USB/IP-Projekt besteht aus einem Linux-Kernel-Treiber und einigen Benutzermodus-Bibliotheken, die die Kommunikation mit dem Kernel-Treiber ermöglichen, um alle USB-Daten zu erhalten.

Der Linux VDA implementiert die USB-Geräteumleitung basierend auf dem Open-Source-USB/IP-Projekt und verwendet den Kernel-Treiber und die Benutzermodus-Bibliotheken von USB/IP wieder. Alle USB-Datenübertragungen zwischen dem Linux VDA und der Citrix Workspace-App werden jedoch durch das Citrix ICA USB-Protokoll gekapselt.

Citrix USB-Sitzungsmodul:

Das Citrix USB-Sitzungsmodul fungiert als Kommunikationsbrücke zwischen dem USB/IP-Kernelmodul und der Citrix Workspace-App.

Citrix USB-Dienstmodul:

Das Citrix USB-Dienstmodul verwaltet alle Vorgänge an USB-Geräten, z. B. das Anschließen oder Trennen von USB-Geräten.

So funktioniert die USB-Geräteumleitung

Wenn ein USB-Gerät erfolgreich an den Linux VDA umgeleitet wird, werden typischerweise ein oder mehrere Geräteknoten im Systempfad /dev erstellt. Manchmal ist das umgeleitete Gerät jedoch für eine aktive Linux VDA-Sitzung nicht nutzbar. USB-Geräte sind auf Treiber angewiesen, um ordnungsgemäß zu funktionieren, und einige Geräte erfordern spezielle Treiber. Wenn keine Treiber bereitgestellt werden, sind die umgeleiteten USB-Geräte für die aktive Linux VDA-Sitzung nicht zugänglich. Um die Konnektivität von USB-Geräten sicherzustellen, installieren Sie die Treiber und konfigurieren Sie das System ordnungsgemäß.

Der Linux VDA unterstützt eine Liste von USB-Geräten, die erfolgreich vom Client umgeleitet werden.

Unterstützte USB-Geräte

> **Tipp:**
>
> Wir haben Unterstützung für USB 3.0-Ports hinzugefügt. Sie können USB 3.0-Geräte in USB 3.0-Ports eines Clientgeräts einstecken.

> Die folgenden Geräte wurden für die Unterstützung dieser Version des Linux VDA verifiziert. Andere Geräte können frei verwendet werden, jedoch mit unerwarteten Ergebnissen:

USB-MASSENSPEICHERGERÄT	VID:PID	DATEISYSTEM
`Netac Technology Co., Ltd`	0dd8:173c	FAT32, NTFS
`Kingston Datatraveler 101 II`	0951:1625	FAT32, NTFS
`Kingston Datatraveler GT101 G2`	1567:8902	FAT32, NTFS
`SanDisk SDCZ80 flash drive`	0781:5580	FAT32, NTFS
`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 unter Amazon Linux 2, CentOS, RHEL, Rocky Linux und SUSE zu verwenden, aktivieren Sie zuerst die NTFS-Unterstützung auf diesen 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

USB-WEBCAM	VID:PID
`Logitech composite USB device – WebCam, Audio`	0460:0825

USB-Geräteumleitung konfigurieren

(Nur für CentOS, RHEL und Rocky Linux) Installieren oder kompilieren Sie das USB/IP-Kernelmodul

Der Linux VDA verwendet USB/IP als virtuellen Hostcontroller für die USB-Geräteumleitung. Da das USB/IP-Kernelmodul in den meisten Fällen mit Linux-Kernelversion 3.17 und höher veröffentlicht wird, müssen Sie das Kernelmodul standardmäßig nicht erstellen. Das USB/IP-Kernelmodul ist jedoch für CentOS, RHEL und Rocky Linux nicht verfügbar. Um die USB-Geräteumleitung mit diesen Linux-Distributionen zu verwenden, müssen Sie das USB/IP-Kernelmodul installieren oder kompilieren. Laden Sie USB/IP von `<https://pkgs.org/download/kmod-usbip>` herunter und installieren Sie es basierend auf Ihrer Linux-Distribution.

Richtlinien für die USB-Geräteumleitung festlegen

Eine Citrix-Richtlinie steuert, ob die USB-Geräteumleitung aktiviert oder deaktiviert ist. Der Gerätetyp kann auch über eine Delivery Controller™-Richtlinie angegeben werden. Beim Konfigurieren der USB-Geräteumleitung für den Linux VDA konfigurieren Sie die folgenden Richtlinien und Regeln:

- Client-USB-Geräteumleitungsrichtlinie
- Client-USB-Geräteumleitungsregeln

USB-GERÄTEUMLEITUNG AKTIVIEREN

Aktivieren (oder deaktivieren) Sie in Citrix Studio die USB-Geräteumleitung vom Client aus (nur für Workstation-Hosts).

Im Dialogfeld **Einstellung bearbeiten**:

1. Wählen Sie **Zulässig**.
2. Klicken Sie auf **OK**.

USB-Geräteumleitung aktivieren(/en-us/linux-virtual-delivery-agent/2308/media/client-usb-redirection-policy.png)

REGELN FÜR DIE USB-GERÄTEUMLEITUNG FESTLEGEN

Nachdem Sie die USB-Umleitungsrichtlinie aktiviert haben, legen Sie die Umleitungsregeln mit Citrix Studio fest, indem Sie angeben, welche Geräte auf dem Linux VDA zugelassen (oder verweigert) werden.

Im Dialogfeld **Client-USB-Geräteumleitungsregeln**:

1. Klicken Sie auf **Neu**, um eine Umleitungsregel hinzuzufügen, oder auf **Bearbeiten**, um eine vorhandene Regel zu überprüfen.
2. Nachdem Sie eine Regel erstellt (oder bearbeitet) haben, klicken Sie auf **OK**.

Die Einstellung der Client-USB-Geräteumleitungsregel(/en-us/linux-virtual-delivery-agent/2308/media/client-usb-redirection-rule.png)

Beheben von Problemen mit der USB-Geräteumleitung

Verwenden Sie die Informationen in diesem Abschnitt, um verschiedene Probleme zu beheben, die bei der Verwendung des Linux VDA auftreten können.

Umgeleitete USB-Festplatte kann nicht ausgehängt werden

Der Linux VDA verwaltet alle von der Citrix Workspace-App umgeleiteten USB-Festplatten mit Administratorrechten, um sicherzustellen, dass nur der Besitzer auf das umgeleitete Gerät zugreifen kann. Daher können Sie das Gerät nur mit Administratorrechten aushängen.

Gerät kann nicht ausgehängt werden(/en-us/linux-virtual-delivery-agent/2308/media/unable-to-mount-disk.png)

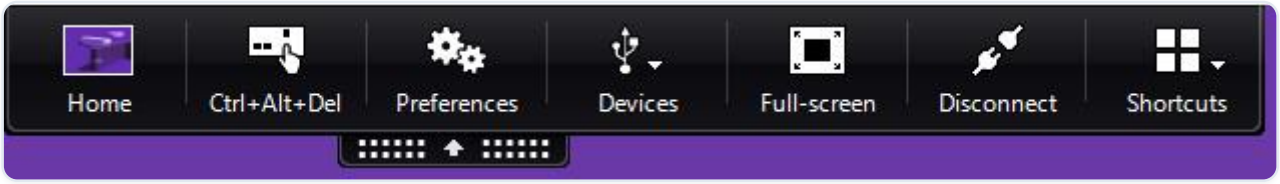
Datei geht verloren, wenn Sie die Umleitung einer USB-Festplatte beenden

Wenn Sie die Umleitung einer USB-Festplatte sofort über die Symbolleiste der Citrix Workspace-App beenden, können die auf der Festplatte geänderten oder erstellten Dateien verloren gehen. Dieses Problem tritt auf, weil das System beim Schreiben von Daten in ein Dateisystem den Speicher-Cache im Dateisystem einbindet. Die Daten werden nicht direkt auf die Festplatte geschrieben. Wenn Sie die Umleitung über die Symbolleiste der Citrix Workspace-App beenden, bleibt keine Zeit mehr, um die Daten auf die Festplatte zu schreiben, was zu Datenverlust führt.

Um dieses Problem zu beheben, verwenden Sie den Befehl **sync** in einem Terminal, um Daten auf die Festplatte zu schreiben, bevor Sie die USB-Umleitung beenden.

Keine Geräte in der Symbolleiste der Citrix Workspace-App

Manchmal werden in der Symbolleiste der Citrix Workspace-App keine Geräte angezeigt, was darauf hinweist, dass keine USB-Umleitung stattfindet.



Wenn dieses Problem auftritt, überprüfen Sie Folgendes:

- Die Richtlinie ist so konfiguriert, dass die USB-Geräteumleitung zugelassen wird.
- Das Citrix USB-Dienstmodul wird ausgeführt.

Wenn die Richtlinie nicht korrekt festgelegt ist, korrigieren Sie sie, indem Sie den Abschnitt USB-Geräteumleitungsrichtlinien festlegen in diesem Artikel heranziehen.

Wenn das Citrix USB-Dienstmodul 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
```

2. Wenn die Ausgabe wie folgt angezeigt wird, installieren oder kompilieren Sie das USB/IP-Kernelmodul basierend auf Ihrer Linux-Distribution:

```
modinfo: ERROR: Module usbip-core not found.
```

- Für Amazon Linux 2, CentOS, RHEL und Rocky Linux finden Sie weitere Informationen im Abschnitt USB/IP-Kernelmodul installieren oder kompilieren in diesem Artikel.
- Für SUSE laden Sie das USB/IP-Paket von `<https://software.opensuse.org/package/usbip>` herunter und installieren 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.

  Gehen Sie zum Linux-Kernel-Repository unter `<https://github.com/torvalds/linux/tree/master/drivers/usb/usbip>`, wählen Sie das Tag der Ziel-Linux-Kernelversion (v4.15 oder höher) aus und rufen Sie den Link wie `<https://github.com/torvalds/linux/tree/v4.15/drivers/usb/usbip>` ab.

  Gehen Sie zu DownGit und geben Sie den vorhergehenden 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
```

  c. Ändern Sie die Datei **Makefile** wie folgt:

```
# SPDX-License-Identifier: GPL-2.0



ccflags-$(CONFIG_USBIP_DEBUG) := -DDEBUG
```

```
obj-$(CONFIG_USBIP_CORE) += usbip-core.o

usbip-core-y := usbip_common.o usbip_event.o

obj-$(CONFIG_USBIP_VHCI_HCD) += vhci-hcd.o

vhci-hcd-y := vhci_sysfs.o vhci_tx.o vhci_rx.o vhci_hcd.o

#obj-$(CONFIG_USBIP_HOST) += usbip-host.o

#usbip-host-y := stub_dev.o stub_main.o stub_rx.o stub_tx.o

#obj-$(CONFIG_USBIP_VUDC) += usbip-vudc.o

#usbip-vudc-y := vudc_dev.o vudc_sysfs.o vudc_tx.o vudc_rx.o
vudc_transfer.o vudc_main.o
```

d. Kompilieren Sie den Quellcode:

```
apt-get install linux-headers-`uname -r`

make -C /lib/modules/`uname -r`/build M=$PWD
```

e. Installieren Sie das USB/IP-Kernelmodul:

```
cp usbip-core.ko vhci-hcd.ko /opt/Citrix/VDA/lib64/
```

f. Starten Sie den Dienst **ctxusbsd** neu, um das USB/IP-Kernelmodul zu laden:

```
service ctxusbsd restart
```

Umleitungsfehler, wenn USB-Geräte in der Symbolleiste der Citrix Workspace-App sichtbar sind, aber als „richtlinienbeschränkt“ gekennzeichnet sind

Wenn das Problem auftritt, gehen Sie wie folgt vor:

- Konfigurieren Sie die Linux VDA-Richtlinie, um die Umleitung zu aktivieren.
- Überprüfen Sie, ob zusätzliche Richtlinieneinschränkungen in der Registrierung der Citrix Workspace-App konfiguriert sind. Überprüfen Sie **DeviceRules** im Registrierungspfad, um sicherzustellen, dass der Zugriff auf das Gerät durch diese Einstellung nicht verweigert wird:

  HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Citrix\\ICA Client\\GenericUSB

Ein USB-Gerät wird erfolgreich umgeleitet, aber ich kann es in meiner Sitzung nicht verwenden

Typischerweise können nur unterstützte USB-Geräte umgeleitet werden. Andere Geräte können ebenfalls an eine aktive Linux VDA-Sitzung umgeleitet werden. Für jedes umgeleitete Gerät wird ein vom Benutzer besessener Knoten im Systempfad **/dev** erstellt. Es sind jedoch die Treiber und die Konfiguration, die bestimmen, ob der Benutzer das Gerät erfolgreich verwenden kann. Wenn Sie ein Gerät finden, das besessen (angeschlossen) aber unzugänglich ist, fügen Sie das Gerät einer uneingeschränkten Richtlinie hinzu.

> **Hinweis:**
>
> Bei USB-Laufwerken konfiguriert und mountet der Linux VDA die Festplatte. Der Benutzer (und nur der Besitzer, der sie installiert hat) kann ohne zusätzliche Konfiguration auf die Festplatte zugreifen. Dies trifft möglicherweise nicht auf Geräte zu, die nicht in der Liste der unterstützten Geräte aufgeführt sind.

Zwischenablageumleitung

Die Zwischenablageumleitung ermöglicht das Kopieren und Einfügen von Daten zwischen Anwendungen, die in der VDA-Sitzung ausgeführt werden, und Anwendungen, die auf dem Clientgerät ausgeführt werden.

Dieser Artikel beschreibt die verfügbaren Citrix®-Richtlinien, mit denen Sie die Zwischenablageumleitung realisieren können.

Citrix-Richtlinien für die Zwischenablageumleitung

Client-Zwischenablagenumleitung

Diese Einstellung erlaubt oder verhindert, dass die Zwischenablage auf dem Clientgerät der Zwischenablage auf dem VDA zugeordnet wird.

Standardmäßig ist die Zwischenablageumleitung auf **Zugelassen** festgelegt.

Um die Übertragung von Daten per Kopieren und Einfügen zwischen einer Sitzung und der lokalen Zwischenablage zu verhindern, wählen Sie **Verboten**. Benutzer können weiterhin Daten zwischen Anwendungen kopieren und einfügen, die in Sitzungen ausgeführt werden.

Bandbreitenbegrenzung für Zwischenablagenumleitung

Diese Einstellung gibt die maximal zulässige Bandbreite (in Kbit/s) für die Datenübertragung zwischen der Sitzung und den lokalen Zwischenablagen an.

Bandbreitenbegrenzung für Zwischenablage-Umleitung in Prozent

Diese Einstellung gibt die maximal zulässige Bandbreite für die Datenübertragung zwischen der Sitzung und den lokalen Zwischenablagen als Prozentsatz der gesamten Sitzungsbandbreite an.

Größe der Zwischenablageübertragung vom Client zur Sitzung begrenzen

Diese Einstellung gibt die maximale Größe der Zwischenablagedaten an, die ein einzelner Kopiervorgang von einem Clientgerät in eine virtuelle Sitzung übertragen kann.

Um die Größe der Zwischenablageübertragung zu begrenzen, aktivieren Sie die Einstellung **Größe der Zwischenablageübertragung vom Client zur Sitzung begrenzen**. 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.

Standardmäßig ist diese Einstellung deaktiviert.

Größe der Zwischenablageübertragung von Sitzung zu Client begrenzen

Diese Einstellung gibt die maximale Größe der Zwischenablagedaten an, die ein einzelner Kopiervorgang von einer virtuellen Sitzung auf ein Clientgerät übertragen kann.

Um die Größe der Zwischenablageübertragung zu begrenzen, aktivieren Sie die Einstellung **Größe der Zwischenablageübertragung von der Sitzung zum Client begrenzen**. 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.

Standardmäßig ist diese Einstellung deaktiviert.

Schreiben in die Clientzwischenablage einschränken UND Zulässige Formate für das Schreiben in die Clientzwischenablage

Durch Aktivieren der beiden Einstellungen können Sie zulassen, dass bestimmte Datenformate von der Sitzung zum Client kopiert und eingefügt werden (Schreiben in den Client).

Die folgenden Zwischenablageformate sind systemdefiniert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_UNICODETEXT
- CF_LOCALE
- CF_DIBV5
- CF_HDROP

Schreiben in die Sitzungs-Zwischenablage einschränken UND Zulässige Formate für das Schreiben in die Sitzungs-Zwischenablage

Durch Aktivieren der beiden Einstellungen können Sie bestimmte Datenformate zulassen, die vom Client in die Sitzung kopiert und eingefügt werden sollen (Schreiben in die Sitzung).

Die folgenden Zwischenablageformate sind systemdefiniert:

- CF_TEXT

- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_UNICODETEXT
- CF_LOCALE
- CF_DIBV5
- CF_HDROP

Tastatur

Dieser Abschnitt enthält die folgenden Themen:

- Client-IME
- Client-IME-Benutzeroberflächensynchronisierung
- Dynamische Tastaturlayout-Synchronisierung
- Bildschirmtastatur
- Unterstützung für mehrere Spracheingaben

Client-Eingabemethoden-Editor (IME)

Übersicht

Doppelbyte-Zeichen wie chinesische, japanische und koreanische Zeichen müssen über einen IME eingegeben werden. Geben Sie solche Zeichen mit jedem IME ein, der mit der Citrix Workspace™-App auf Clientseite kompatibel ist, z. B. dem nativen Windows CJK IME.

Installation

Diese Funktion wird automatisch installiert, wenn Sie den Linux VDA installieren.

Verwendung

Öffnen Sie eine Citrix Virtual Apps- oder Citrix Virtual Desktops™-Sitzung wie gewohnt.

Ändern Sie Ihre Eingabemethode nach Bedarf auf Clientseite, um die Client-IME-Funktion zu nutzen.

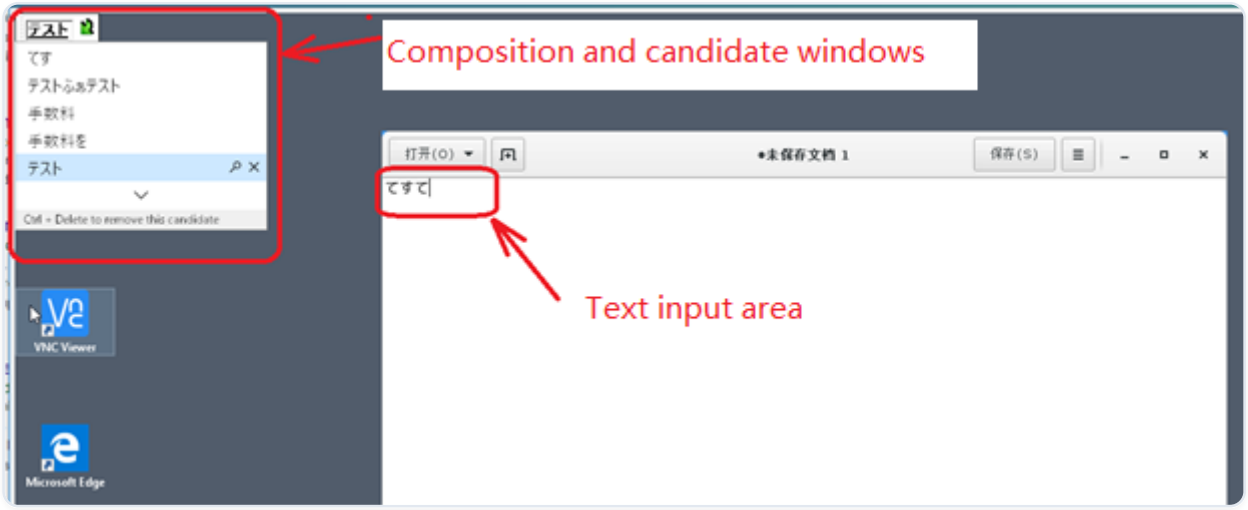
Bekannte Probleme

- Ein Doppelklick auf eine Zelle in einer Google-Tabelle ist zwingend erforderlich, bevor Sie die Client-IME-Funktion verwenden können, um Zeichen in die Zelle einzugeben.
- Die Client-IME-Funktion wird in Kennwortfeldern nicht automatisch deaktiviert.
- Die IME-Benutzeroberfläche folgt dem Cursor im Eingabebereich nicht.

Client-IME-Benutzeroberflächensynchronisierung

Übersicht

Bislang befand sich die Client-IME-Benutzeroberfläche (einschließlich des Kompositionsfensters und des Kandidatenfensters) in der oberen linken Ecke des Bildschirms. Sie folgte dem Cursor nicht und befand sich manchmal weit entfernt vom Cursor im Texteingabebereich:



Citrix® verbessert die Benutzerfreundlichkeit und das Benutzererlebnis mit dem Client-IME wie folgt:



Voraussetzungen für die Verwendung der Funktion

1. Aktivieren Sie Intelligent Input Bus (`IBus`) auf Ihrem Linux VDA. Informationen zum Aktivieren von `IBus` unter einem Linux-Betriebssystem finden Sie in der Dokumentation des Betriebssystemanbieters. Zum Beispiel:
   - Ubuntu: `<https://help.ubuntu.com/community/ibus>`
   - CentOS, RHEL: `<https://access.redhat.com/documentation/de-de/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. Die Funktion wird automatisch installiert, muss aber vor der Verwendung aktiviert werden.

Funktion aktivieren und deaktivieren

Die Synchronisierungsfunktion der Client-IME-Benutzeroberfläche ist standardmäßig deaktiviert. Um die Funktion zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client Keyboard Layout Sync and IME Improvement** fest oder bearbeiten Sie die Registrierung über das Dienstprogramm `ctxreg`.

> **Hinweis:**

> Die Richtlinie **Client Keyboard Layout Sync and IME Improvement** hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Computerobjekte oder alle Objekte in Ihrer Site angewendet werden. Registrierungseinstellungen auf einem bestimmten Linux VDA gelten für alle Sitzungen auf diesem VDA.

- Legen Sie die Richtlinie **Client Keyboard Layout Sync and IME Improvement** fest, um die Client-IME-Benutzeroberflächensynchronisierungsfunktion zu aktivieren oder zu deaktivieren:

  a. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.

  b. Suchen Sie nach der Richtlinie **Client Keyboard Layout Sync and IME Improvement**.

     Abbildung der Richtlinie Client Keyboard Layout Sync and IME Improvement(/en-us/linux-virtual-delivery-agent/2308/media/client-keyboard-and-ime-policy.png)

  c. Klicken Sie neben dem Richtliniennamen auf **Auswählen**.

  d. Legen Sie die Richtlinie fest.

     Abbildung der Einstellung der Richtlinie Client Keyboard Layout Sync and IME Improvement(/en-us/linux-virtual-delivery-agent/2308/media/setting-client-keyboard-and-ime-policy.png)

     Es stehen drei Optionen zur Verfügung:

     - **Deaktiviert**: deaktiviert die dynamische Tastaturlayoutsynchronisierung und die Client-IME-Benutzeroberflächensynchronisierung.
     - **Unterstützung der dynamischen Client-Tastaturlayoutsynchronisierung**: aktiviert die dynamische Tastaturlayoutsynchronisierung, unabhängig vom DWORD-Wert des Registrierungsschlüssels **SyncKeyboardLayout** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
     - **Unterstützung der dynamischen Client-Tastaturlayoutsynchronisierung und IME-Verbesserung**: aktiviert sowohl die dynamische Tastaturlayoutsynchronisierung als auch die Client-IME-Benutzeroberflächensynchronisierung, unabhängig von den DWORD-Werten der Registrierungsschlüssel **SyncKeyboardLayout** und **SyncClientIME** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.

- Bearbeiten Sie die Registrierung über das Dienstprogramm `ctxreg`, um die Client-IME-Benutzeroberflächensynchronisierungsfunktion zu aktivieren oder zu deaktivieren:

  Um die Funktion zu aktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v  "SyncClientIME" -d "0x00000001"
  ```

  Um die Funktion zu deaktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncClientIME" -d "0x00000000"
  ```

Dynamische Tastaturlayout-Synchronisierung

Bisher mussten die Tastaturlayouts auf dem Linux-VDA und auf dem Clientgerät identisch sein. Es konnten Probleme bei der Tastenbelegung auftreten, wenn sich beispielsweise das Tastaturlayout auf dem Clientgerät von Englisch zu Französisch änderte, aber nicht auf dem VDA.

Citrix® behebt das Problem, indem es das Tastaturlayout des VDA automatisch mit dem Tastaturlayout des Clientgeräts synchronisiert. Jedes Mal, wenn sich das Tastaturlayout auf dem Clientgerät ändert, passt sich das Layout auf dem VDA entsprechend an.

> **Hinweis:**

> Die Citrix Workspace™-App für HTML5 unterstützt die Funktion zur dynamischen Tastaturlayoutsynchronisierung nicht.

Konfiguration

Die Funktion zur dynamischen Tastaturlayoutsynchronisierung ist standardmäßig deaktiviert. Um die Funktion zu aktivieren oder zu deaktivieren, legen Sie die Richtlinie **Client Keyboard Layout Sync and IME Improvement** fest oder bearbeiten Sie die Registrierung über das Dienstprogramm `ctxreg`.

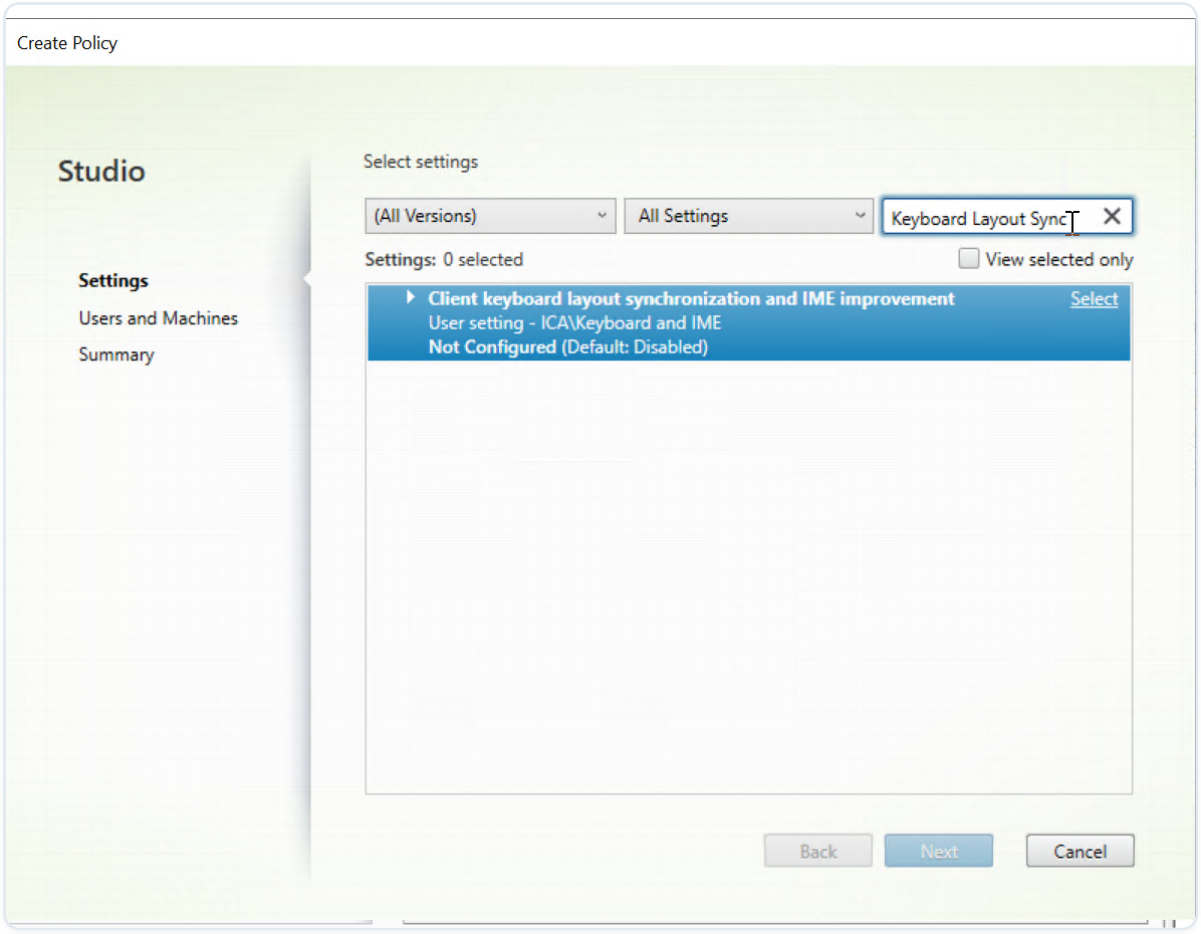
> **Hinweis:**

> Die Richtlinie **Client Keyboard Layout Sync and IME Improvement** hat Vorrang vor Registrierungseinstellungen und kann auf von Ihnen angegebene Benutzer- und Maschinenobjekte oder alle Objekte in Ihrer Site angewendet werden. Registrierungseinstellungen auf einem bestimmten Linux-VDA gelten für alle Sitzungen auf diesem VDA.

- Legen Sie die Richtlinie **Client Keyboard Layout Sync and IME Improvement** fest, um die Funktion zur dynamischen Tastaturlayoutsynchronisierung zu aktivieren oder zu deaktivieren:

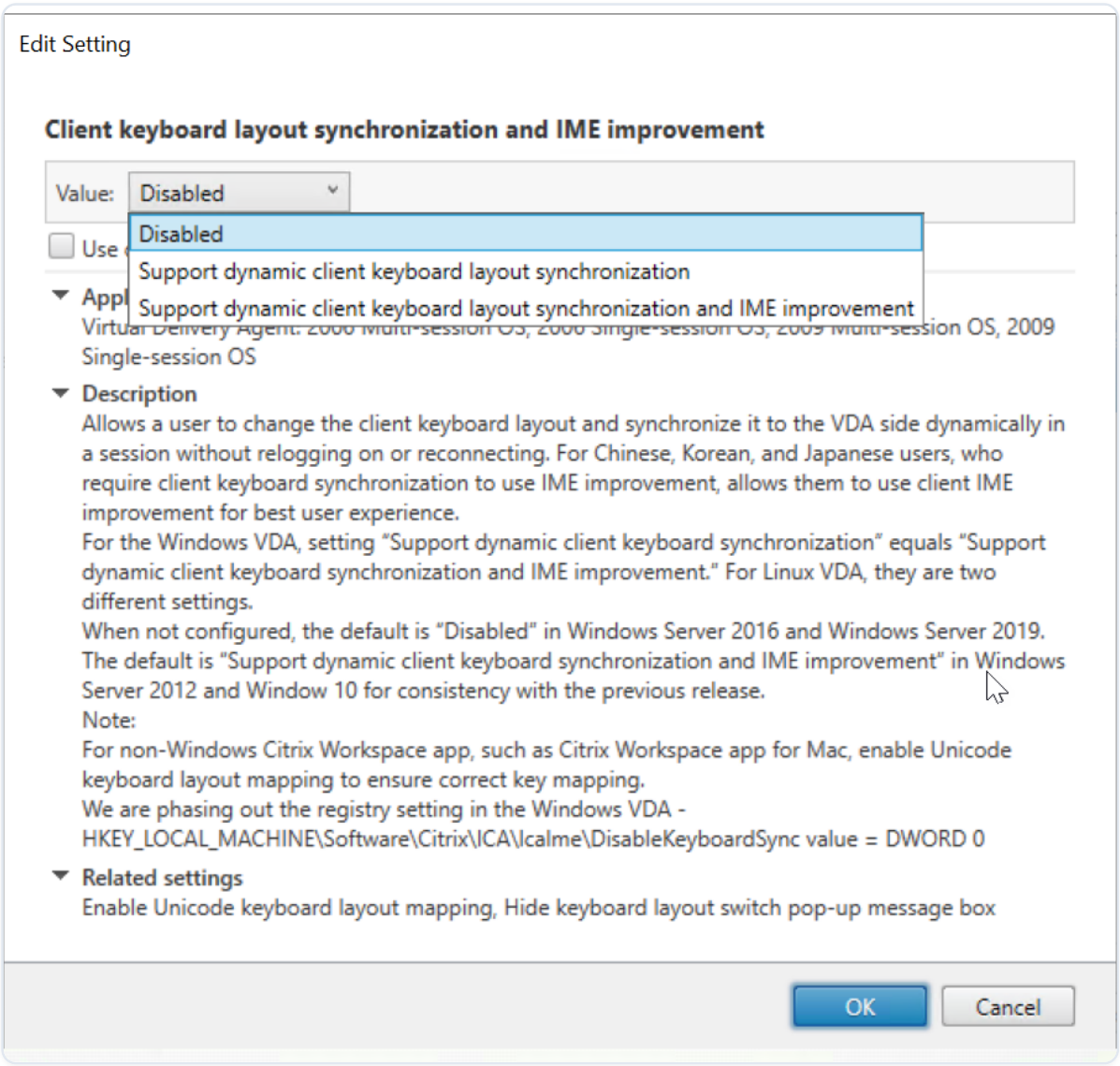
  a. Klicken Sie in Studio mit der rechten Maustaste auf **Richtlinien** und wählen Sie **Richtlinie erstellen**.

  b. Suchen Sie nach der Richtlinie **Client Keyboard Layout Sync and IME Improvement**.



  c. Klicken Sie neben dem Richtliniennamen auf **Auswählen**.

  d. Legen Sie die Richtlinie fest.



Es sind drei Optionen verfügbar:

- **Deaktiviert**: Deaktiviert die dynamische Tastaturlayoutsynchronisierung und die Synchronisierung der Client-IME-Benutzeroberfläche.
- **Dynamische Client-Tastaturlayoutsynchronisierung unterstützen**: Aktiviert die dynamische Tastaturlayoutsynchronisierung unabhängig vom DWORD-Wert des Registrierungsschlüssels **SyncKeyboardLayout** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.
- **Unterstützung der dynamischen Synchronisierung des Client-Tastaturlayouts und der IME-Verbesserung**: ermöglicht sowohl die dynamische Synchronisierung des Tastaturlayouts als auch die Synchronisierung der Client-IME-Benutzeroberfläche, unabhängig von den DWORD-Werten der Registrierungsschlüssel **SyncKeyboardLayout** und **SyncClientIME** unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar`.

- Bearbeiten Sie die Registrierung mit dem Dienstprogramm `ctxreg`, um die Funktion zur dynamischen Synchronisierung des Tastaturlayouts zu aktivieren oder zu deaktivieren:

  Um diese Funktion zu aktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncKeyboardLayout" -d "0x00000001"
  ```

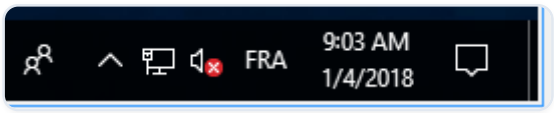
  Um diese Funktion zu deaktivieren, führen Sie den Befehl aus:

  ```
  /opt/Citrix/VDA/bin/ctxreg update -k
  "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar
  " -v "SyncKeyboardLayout" -d "0x00000000"
  ```

Verwendung

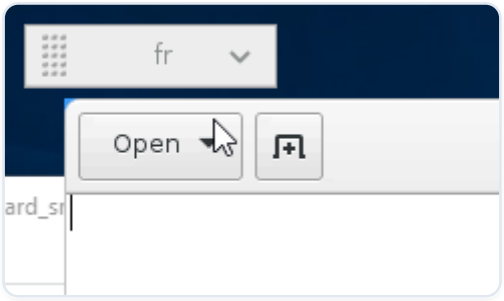
Wenn diese Funktion aktiviert ist und sich das Tastaturlayout auf dem Clientgerät während einer Sitzung ändert, ändert sich das Tastaturlayout der Sitzung entsprechend.

Wenn Sie beispielsweise das Tastaturlayout auf einem Clientgerät auf Französisch (FR) ändern:

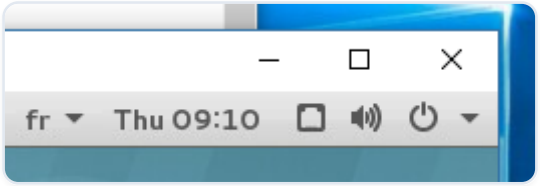


Dann ändert sich das Tastaturlayout der Linux VDA-Sitzung ebenfalls zu „fr.“

In einer Anwendungssitzung können Sie diese automatische Änderung sehen, wenn Sie die Sprachleiste aktiviert haben:

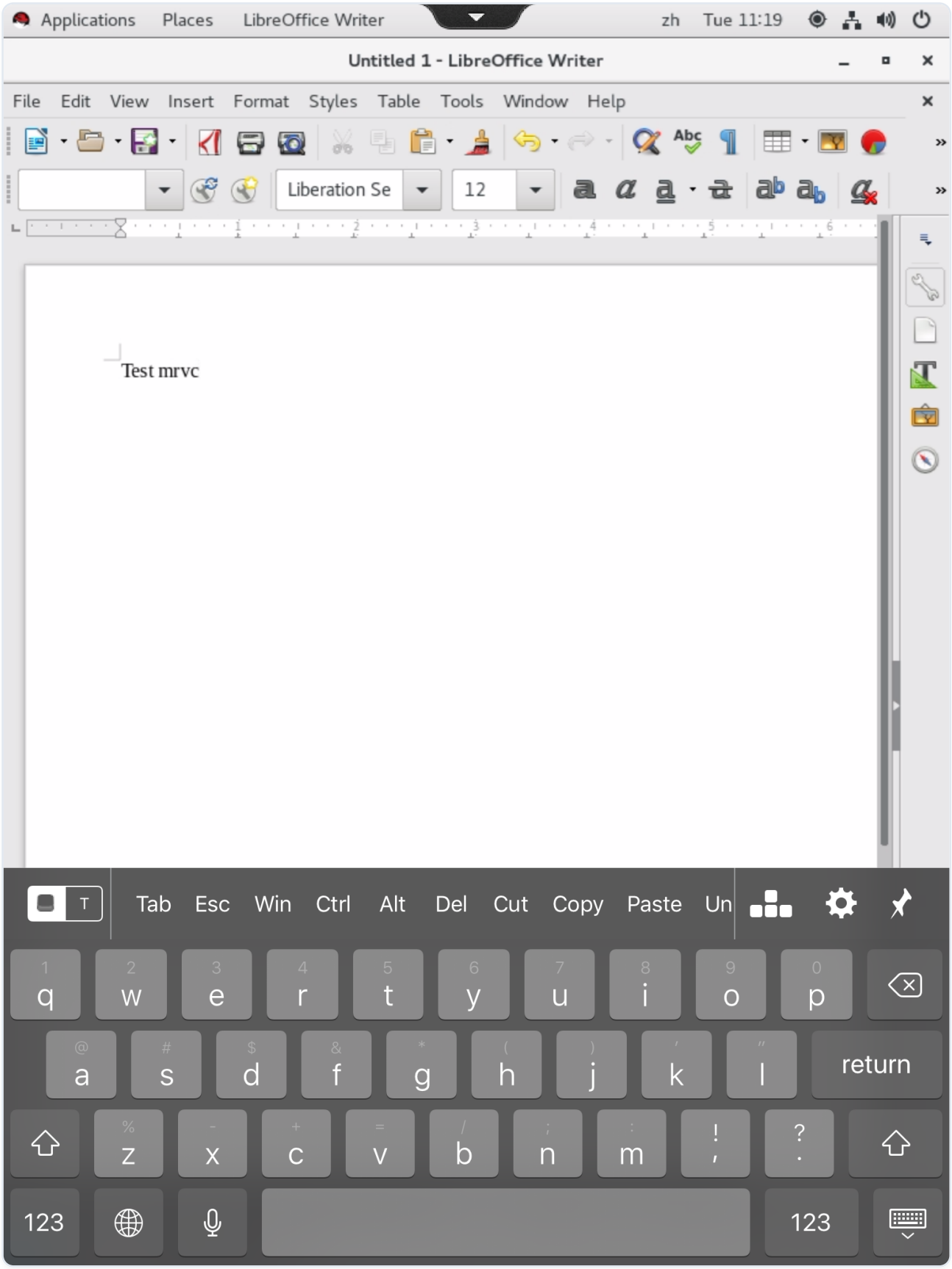


In einer Desktopsitzung können Sie diese automatische Änderung in der Taskleiste sehen:



Bildschirmtastatur

Die Bildschirmtastaturfunktion ist in einer virtuellen Linux-Desktop- oder Anwendungssitzung verfügbar. Die Bildschirmtastatur wird automatisch ein- oder ausgeblendet, wenn Sie ein Eingabefeld betreten oder verlassen.


Applications
Places
LibreOffice Writer
zh
Tue 11:19
Untitled 1 - LibreOffice Writer
File
Edit
View
Insert
Format
Styles
Table
Tools
Window
Help
Liberation Se
12
Test mrvc
Tab
Esc
Win
Ctrl
Alt
Del
Cut
Copy
Paste
Un
return
123
123

Hinweis:

> Die Funktion wird von der Citrix Workspace™-App für iOS und Android unterstützt.

Funktion aktivieren und deaktivieren

Die Funktion ist standardmäßig deaktiviert. Verwenden Sie das Dienstprogramm **ctxreg**, um die Funktion zu aktivieren oder zu deaktivieren. Die Funktionskonfiguration auf einem bestimmten Linux-VDA gilt für alle Sitzungen auf diesem VDA.

So aktivieren Sie die Funktion:

1. Führen Sie den Befehl aus:

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k
   "HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
   "Enabled" -d "0x00000001"
   ```

2. Legen Sie in Citrix Studio die Richtlinie **Automatische Tastaturanzeige** auf **Zulässig** fest.
3. (Optional) Führen Sie für RHEL 7 und CentOS 7 den folgenden Befehl aus, um den Intelligent Input Bus (`IBus`) als Standard-IM-Dienst zu konfigurieren:

   ```
   echo "GTK_IM_MODULE=ibus" >>/etc/bashrc
   ```

Um die Funktion zu deaktivieren, führen Sie den Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKLM\System\CurrentControlSet\Control\Citrix\VirtualChannels\MrVc"  -v
"Enabled" -d "0x00000000"
```

> **Hinweis:**

> Die vorstehenden Einstellungen werden wirksam, wenn Sie sich bei einer neuen Sitzung anmelden oder sich von der aktuellen Sitzung abmelden und wieder anmelden.

Einschränkungen

- Die Funktion funktioniert möglicherweise nicht wie erwartet mit Google Chrome, LibreOffice und anderen Apps.

- Um die Bildschirmtastatur nach dem manuellen Ausblenden wieder anzuzeigen, klicken Sie auf ein Nicht-Eingabefeld und dann erneut auf das aktuelle Eingabefeld.
- Die Bildschirmtastatur wird möglicherweise nicht angezeigt, wenn Sie in einem Webbrowser von einem Eingabefeld zu einem anderen klicken. Um dieses Problem zu umgehen, klicken Sie auf ein Nicht-Eingabefeld und dann auf das Ziel-Eingabefeld.
- Die Funktion unterstützt keine Unicode-Zeichen und Doppelbyte-Zeichen (wie z. B. chinesische, japanische und koreanische Zeichen).
- Die Bildschirmtastatur ist für Passworteingabefelder nicht verfügbar.
- Die Bildschirmtastatur kann das aktuelle Eingabefeld überlappen. Verschieben Sie in diesem Fall das App-Fenster oder scrollen Sie Ihren Bildschirm nach oben, um das Eingabefeld an eine zugängliche Position zu verschieben.
- Aufgrund von Kompatibilitätsproblemen zwischen der Citrix Workspace-App und Huawei-Tablets erscheint die Bildschirmtastatur auf Huawei-Tablets, selbst wenn eine physische Tastatur angeschlossen ist.

Unterstützung für mehrere Spracheingaben

Ab Linux VDA Version 1.4 hat Citrix die Unterstützung für veröffentlichte Anwendungen hinzugefügt. Benutzer können auf eine gewünschte Linux-Anwendung ohne die Linux-Desktopumgebung zugreifen.

Die native Sprachleiste auf dem Linux VDA war jedoch für die veröffentlichte Anwendung nicht verfügbar, da die Sprachleiste stark in die Linux-Desktopumgebung integriert ist. Infolgedessen konnten Benutzer keinen Text in einer Sprache eingeben, die IME erfordert, wie z. B. Chinesisch, Japanisch oder Koreanisch. Es war auch nicht möglich, während einer Anwendungssitzung zwischen Tastaturlayouts zu wechseln.

Um diese Probleme zu beheben, bietet diese Funktion eine Sprachleiste für veröffentlichte Anwendungen, die Texteingaben akzeptieren. Die Sprachleiste ermöglicht es Benutzern, eine serverseitige IME auszuwählen und während einer Anwendungssitzung zwischen Tastaturlayouts zu wechseln.

Konfiguration

Sie können das Dienstprogramm **ctxreg** verwenden, um diese Funktion zu aktivieren oder zu deaktivieren (standardmäßig deaktiviert). Die Funktionskonfiguration auf einem bestimmten Linux VDA-Server gilt für alle auf diesem VDA veröffentlichten Anwendungen.

Der Konfigurationsschlüssel ist „HKEY_LOCAL_MACHINE \\SYSTEM\\CurrentControlSet\\Control\\Citrix\\LanguageBar“ und der Typ ist DWORD.

Um diese Funktion zu aktivieren, führen Sie den Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar"
-v "Enabled" -d "0x00000001"
```

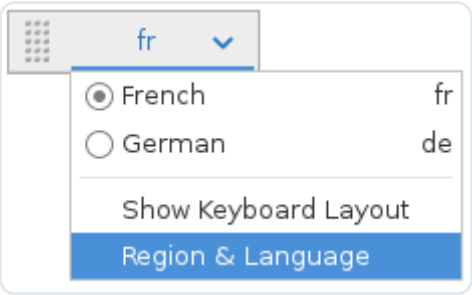
Um diese Funktion zu deaktivieren, führen Sie den Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\LanguageBar"
-v "Enabled" -d "0x00000000"
```

Verwendung

Die Verwendung ist unkompliziert.

1. Aktivieren Sie die Funktion.
2. Greifen Sie auf eine veröffentlichte Anwendung zu, die Texteingaben akzeptieren kann. Eine Sprachleiste wird in der Sitzung neben der Anwendung angezeigt.
3. Wählen Sie im Dropdown-Menü **Region & Sprache** aus, um die gewünschte Sprache (Eingabequelle) hinzuzufügen.



4. Wählen Sie die IME oder das Tastaturlayout aus dem Dropdown-Menü aus.
5. Geben Sie eine Sprache mit der ausgewählten IME oder dem Tastaturlayout ein.

> **Hinweis:**

- Wenn Sie ein Tastaturlayout in der Sprachleiste auf der VDA-Seite ändern, stellen Sie sicher, dass dasselbe Tastaturlayout auf der Clientseite (auf der die Citrix Workspace™-App ausgeführt wird) verwendet wird.
- Das Paket **accountsservice** muss auf Version 0.6.37 oder höher aktualisiert werden, bevor Sie Einstellungen im Dialogfeld **Region & Sprache** vornehmen können.

Abbildung der Auswahl von IME oder Tastaturlayout(/en-us/linux-virtual-delivery-agent/2308/media/region-language-dialog-box.png)

Multimedia

Dieser Abschnitt enthält die folgenden Themen:

- Audiofunktionen
- Browserinhaltsumleitung
- HDX-Webcam-Videokomprimierung

Audiofunktionen

Adaptives Audio

Adaptives Audio ist standardmäßig aktiviert. Es unterstützt die folgenden Citrix Workspace™-App-Clients:

- Citrix Workspace-App für Windows – 2109 und spätere Versionen
- Citrix Workspace-App für Linux – 2109 und spätere Versionen
- Citrix Workspace-App für Mac – 2109 und spätere Versionen

Adaptives Audio greift auf Legacy-Audio zurück, wenn Sie einen Client verwenden, der nicht auf der Liste steht.

Mit adaptivem Audio müssen Sie die Audiocenterichtlinien auf dem VDA nicht manuell konfigurieren. Adaptives Audio passt die Audio-Sampling-Bitraten dynamisch an die Netzwerkbedingungen an, um ein erstklassiges Audioerlebnis zu bieten.

Die folgende Tabelle zeigt einen Vergleich zwischen adaptivem Audio und Legacy-Audio:

ADAPTIVES AUDIO	LEGACY-AUDIO
Max. Audio-Samplerate: 48 kHz	Max. Audio-Samplerate: 8 kHz
Stereokanal	Monokanal

> **Tipp:**
>
> Verwenden Sie PulseAudio 13.99 oder höher unter RHEL 8.x und Rocky Linux 8.x.

Browserinhaltsumleitung

Übersicht

Die Browserinhaltsumleitung ermöglicht das Rendern von Webseiten in der Zulassungsliste auf Clientseite. Diese Funktion verwendet die Citrix Workspace™-App, um eine entsprechende Rendering-Engine auf Clientseite zu instanziieren, die die HTTP- und HTTPS-Inhalte von der URL abruft.

> **Hinweis:**
>
> Der Linux VDA unterstützt die Browserinhaltsumleitung in Google Chrome.

> Diese Overlay-Web-Layout-Engine läuft auf dem Client statt auf dem VDA und nutzt die CPU, GPU, den RAM und das Netzwerk des Clients.

Nur der Browser-Viewport wird umgeleitet. Der Viewport ist der rechteckige Bereich in Ihrem Browser, in dem Inhalte angezeigt werden. Der Viewport umfasst keine Elemente wie die Adressleiste, die Favoritenleiste und die Statusleiste. Diese Elemente werden weiterhin im Browser auf dem VDA ausgeführt.

Bild des Viewports(/en-us/linux-virtual-delivery-agent/2308/media/viewport.png)

Konfigurieren Sie eine Studio-Richtlinie, die eine Zugriffssteuerungsliste mit den URLs in der Zulassungsliste für die Umleitung angibt. Konfigurieren Sie eine Sperrliste, die die Umleitung für bestimmte URLs deaktiviert.

Wenn eine Übereinstimmung mit einer URL in einer Zulassungsliste, aber nicht in einer Sperrliste gefunden wird, weist ein virtueller Kanal (CTXCSB) die Citrix Workspace-App an, dass eine Umleitung erforderlich ist, und leitet die URL weiter. Die Citrix Workspace-App instanziiert dann eine lokale Rendering-Engine und zeigt die Website an.

Die Citrix Workspace-App fügt die Website dann nahtlos wieder in den Inhaltsbereich des virtuellen Desktop-Browsers ein.

Viewport und Client(/en-us/linux-virtual-delivery-agent/2308/media/viewport-desktop-viewer.png)

1. Symbol der Citrix® Browserinhaltsumleitungs-Erweiterung

   Die Farbe des Erweiterungssymbols gibt den Status der Chrome-Erweiterung an. Es ist eine der drei Farben:

   - Grün: Aktiv und verbunden
   - Grau: Nicht aktiv/inaktiv auf der aktuellen Registerkarte
   - Rot: Defekt/Funktioniert nicht

2. Viewport auf dem Client gerendert oder in den virtuellen Desktop zurückgemischt
3. Linux VDA
4. Windows-Client

Hier sind Szenarien, wie die Citrix Workspace-App Inhalte abruft:

Umleitungsszenarien(/en-us/linux-virtual-delivery-agent/2308/media/browser-viewport-redirection-scenarios.png)

- **Server-Abruf und Server-Rendering:** Es erfolgt keine Umleitung, da Sie die Site nicht zur Zulassungsliste hinzugefügt haben oder die Umleitung fehlgeschlagen ist. Wir greifen auf das Rendern der Webseite auf dem VDA zurück und verwenden Thinwire, um die Grafiken remote bereitzustellen. Verwenden Sie Richtlinien, um das Fallback-Verhalten zu steuern. Dieses Szenario führt zu einem hohen CPU-, RAM- und Bandbreitenverbrauch auf dem VDA.
- **Server-Abruf und Client-Rendering**: Die Citrix Workspace-App kontaktiert den Webserver und ruft Inhalte über den VDA über einen virtuellen Kanal (CTXPFWD) ab. Diese Option ist nützlich, wenn der Client keinen Zugriff auf den Webserver hat (z. B. Thin Clients). Sie senkt den CPU- und RAM-Verbrauch auf dem VDA, aber Bandbreite wird auf dem virtuellen ICA®-Kanal verbraucht.

Für dieses Szenario gibt es drei Betriebsmodi. CTXPFWD leitet Daten an ein Proxy-Gerät weiter, auf das der VDA zugreift, um Zugriff auf den Webserver zu erhalten.

Welche Richtlinienoption ist zu wählen:

- Expliziter Proxy – Wenn Sie einen einzelnen expliziten Proxy in Ihrem Rechenzentrum haben.
- Direkt oder Transparent – Wenn Sie keine Proxys haben oder transparente Proxys verwenden.
- PAC-Dateien – Wenn Sie auf PAC-Dateien angewiesen sind, damit Browser im VDA automatisch den geeigneten Proxyserver zum Abrufen einer bestimmten URL auswählen können.

Weitere Informationen finden Sie unter der Einstellung **Browser Content Redirection Proxy Configuration** später in diesem Artikel.

Umleitungs-Proxy-Einstellungen(/en-us/linux-virtual-delivery-agent/2308/media/browser-content-redirection-proxy-settings.png)

- **Client-Abruf und Client-Rendering:** Da die Citrix Workspace-App den Webserver direkt kontaktiert, ist Internetzugang erforderlich. Dieses Szenario entlastet Ihre Citrix Virtual Apps and Desktops™-Site von der gesamten Netzwerk-, CPU- und RAM-Nutzung.

  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 installierter Citrix Browser Content Redirection-Erweiterung

Browser Content Redirection konfigurieren

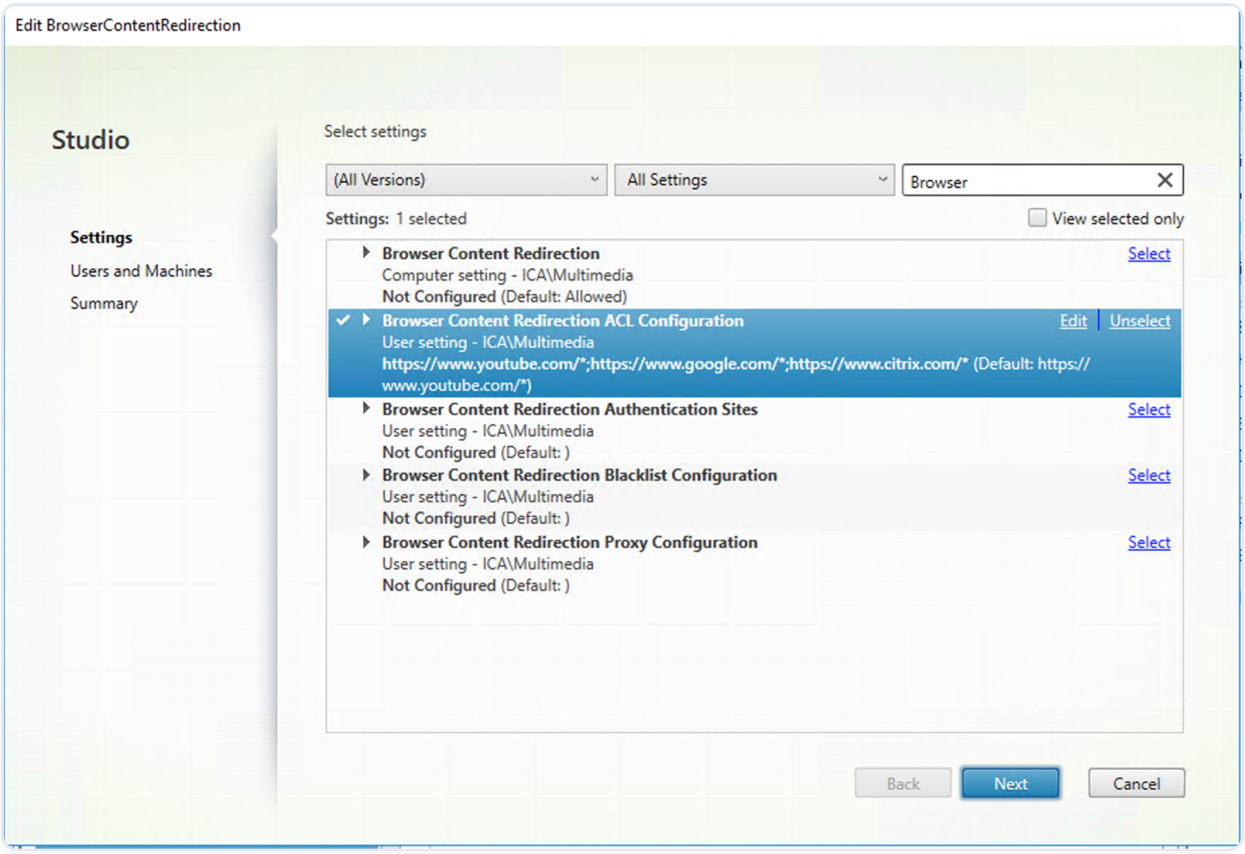
Um Browser Content Redirection zu verwenden, konfigurieren Sie die entsprechenden Richtlinien und installieren Sie die Browser Content Redirection-Erweiterung in Google Chrome. Gehen Sie dazu wie folgt vor:

1. Legen Sie in Citrix Studio **Browser Content Redirection** auf **Zulässig** fest, um Browser Content Redirection zu aktivieren.

   Browser Content Redirection auf Zulässig festgelegt(/en-us/linux-virtual-delivery-agent/2308/media/bcr-allowed-by-default.png)

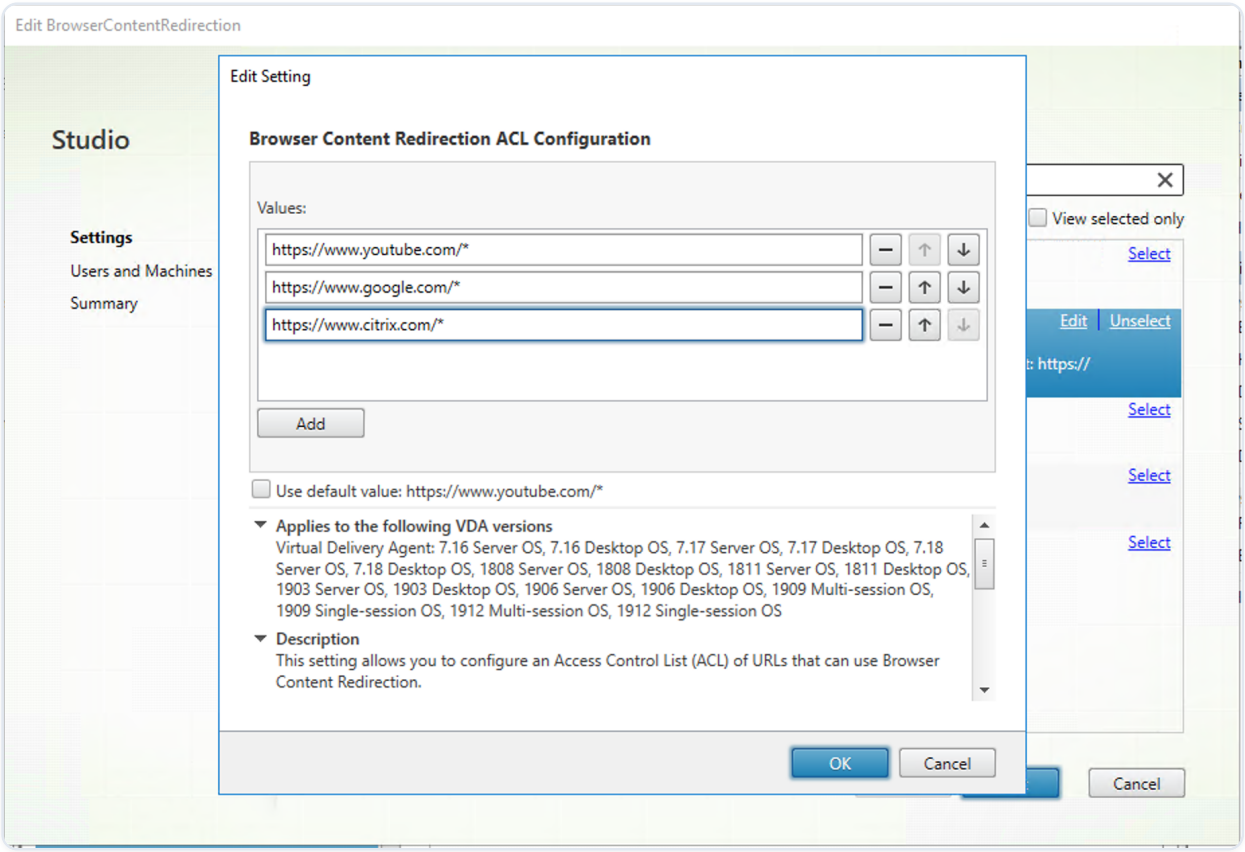
2. Geben Sie eine Zulassungsliste von URLs an, deren Inhalt an den Client umgeleitet werden kann, und eine Sperrliste, die die Umleitung für bestimmte URLs deaktiviert. Das Konfigurieren einer Sperrliste ist optional.

   Die Einstellung **Browser Content Redirection ACL Configuration** gibt eine Positivliste von URLs an, deren Inhalt auf den Client umgeleitet werden kann. Beim Angeben von URLs können Sie den Platzhalter `*` verwenden, um alle URL-Komponenten außer dem Protokoll darzustellen.

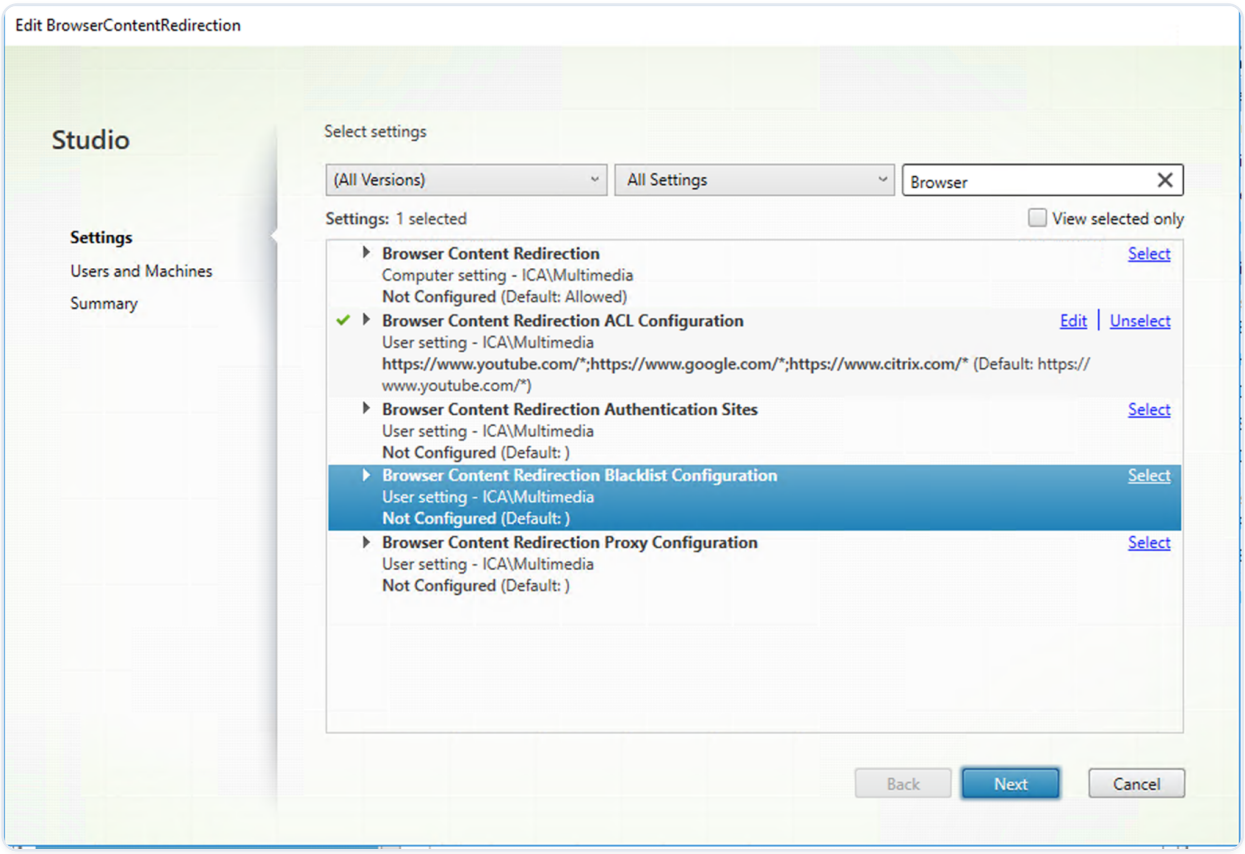


Im Folgenden sind zulässige Beispiele aufgeführt:

- `http://www.xyz.com/index.html` (Sie können eine bessere Granularität erreichen, 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 **Browser Content Redirection Blacklist Configuration** gibt eine Sperrliste an, die die Umleitung für bestimmte URLs deaktiviert.



3. Um das Abrufen vom Server und das Rendern auf dem Client zu aktivieren, konfigurieren Sie die Einstellung **Browser Content Redirection Proxy Configuration**.

   Diese Einstellung bietet Konfigurationsoptionen für Proxyeinstellungen auf dem VDA für die Browserinhaltsumleitung. Wenn sie mit einer gültigen Proxyadresse und Portnummer, einer PAC/WPAD-URL oder einer direkten/transparenten Einstellung aktiviert ist, versucht die Citrix Workspace-App immer zuerst das Abrufen vom Server und das Rendern auf dem Client. Weitere Informationen finden Sie unter Fallback-Mechanismus.

   Wenn die Citrix Workspace-App deaktiviert oder nicht konfiguriert ist und einen Standardwert verwendet, versucht sie das Abrufen vom Client und das Rendern auf dem Client.

   Standardmäßig ist diese Einstellung **Verboten**.

   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:

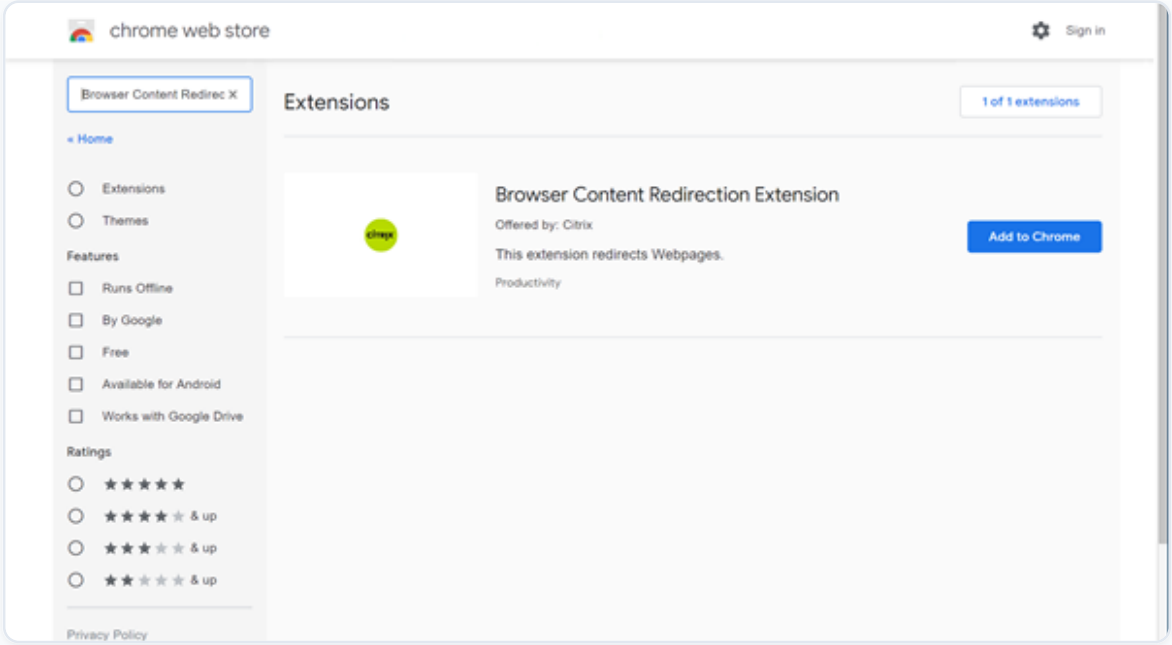
Geben Sie das Wort **DIRECT** in das Richtlinien-Textfeld ein.

> **Hinweis:**
>
> Sie können einen Proxy auch festlegen, indem Sie den Registrierungswert `HKLM\Software\Citrix\HdxMediastream\WebBrowserRedirectionProxyAddress.` bearbeiten. Außerdem können Sie mit dem Registrierungswert `HKLM\Software\Citrix\HdxMediastream\AllowNonTlsPacUri` festlegen, ob PAC-Dateidownloads über HTTP zugelassen werden sollen. Der Standardwert ist 0, was bedeutet, dass HTTP nicht zugelassen ist.
>
> Registrierungen überschreiben Optionen für Richtlinieneinstellungen. Eine Liste der relevanten Registrierungsschlüssel finden Sie unter Browser Content Redirection-Registrierungsschlüssel-Überschreibungen.

4. Klicken Sie auf dem VDA auf **Add to Chrome**, um die Citrix Browser Content Redirection-Erweiterung aus dem Chrome Web Store hinzuzufügen. Dadurch kann der Browser auf dem VDA erkennen, ob eine (angesteuerte) 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. Eine Aktualisierung eines Golden Image zum Hinzufügen oder Entfernen einer Erweiterung ist nicht erforderlich.



Fallback-Mechanismus

Wenn Sie die Richtlinie **Browser Content Redirection Proxy Configuration** aktivieren, versucht die Citrix Workspace-App, den Serverabruf und das Client-Rendering durchzuführen. Wenn der Serverabruf und das Client-Rendering fehlschlagen, wird auf Clientabruf und Client-Rendering zurückgegriffen. Wenn der Clientcomputer keinen Zugriff auf den Webserver hat, kann der Browser auf dem VDA die Seite dann neu laden und auf dem Server rendern (Serverabruf und Server-Rendering).

Browserinhaltsumleitung: Überschreibungen von Registrierungsschlüsseln

> **Warnung:**

> Eine falsche Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen, die eine Neuinstallation des Betriebssystems erforderlich machen können. Citrix kann nicht garantieren, dass Probleme, die aus der falschen Verwendung des Registrierungs-Editors resultieren, behoben werden können. Verwenden Sie den Registrierungs-Editor auf eigenes Risiko. Sichern Sie die Registrierung, bevor Sie sie bearbeiten.

> `HKLM\Software\Citrix\HdxMediastream`

NAME	TYP	WERT
WebBrowserRedirection	DWORD	1=Zulässig, 0=Verboten
WebBrowserRedirectionAcl	REG_MULTI_SZ	/
WebBrowserRedirectionProxyAddress	REG_SZ	Wenn Sie ihn auf einen der folgenden Modi einstellen, wird der Serverabruf und das Client-Rendering aktiviert: **Expliziter Proxy** – Wenn Sie einen einzelnen expliziten Proxy in Ihrem Datencenter haben. **Direkt oder Transparent** – Wenn Sie keine Proxys haben oder transparente Proxys verwenden. **PAC-Dateien** – Wenn Sie sich auf PAC-Dateien verlassen, damit Browser im VDA automatisch den geeigneten Proxyserver für den Abruf einer bestimmten URL auswählen können.
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	/
AllowNonTlsPacUri	DWORD	Legt fest, ob PAC-Dateidownloads über HTTP zugelassen werden sollen. Der Standardwert ist 0, was bedeutet, dass HTTP nicht zugelassen ist. Wenn Sie ihn auf 1 setzen, kann **HDXWebProxy.exe** PAC-Dateien über HTTP herunterladen (nicht ausschließlich über HTTPS).

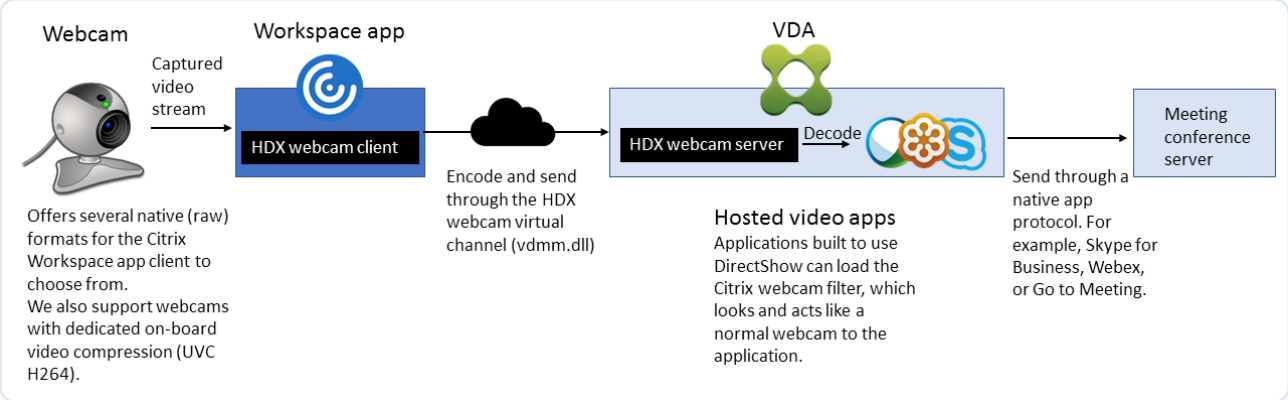
HDX™ Webcam-Videokompression

Übersicht

Benutzer von Videokonferenzanwendungen, die in Linux VDA-Sitzungen ausgeführt werden, können ihre Webcams jetzt mit HDX-Webcam-Videokompression verwenden. Die Funktion ist standardmäßig aktiviert. Wir empfehlen, nach Möglichkeit immer die HDX-Webcam-Videokompression zu verwenden.

Die HDX-Webcam-Videokompression wird auch als **optimierter** Webcam-Modus bezeichnet. Diese Art der Webcam-Videokompression sendet das H.264-Video direkt an die Videokonferenzanwendung, die in der virtuellen Sitzung ausgeführt wird. Die HDX-Webcam-Videokompression nutzt die Multimedia-Framework-Technologie, die Teil des Clientbetriebssystems ist, um Videos von Erfassungsgeräten abzufangen, zu transkodieren und zu komprimieren. Hersteller von Erfassungsgeräten liefern die Treiber, die in die Kernel-Streaming-Architektur des Betriebssystems integriert werden.

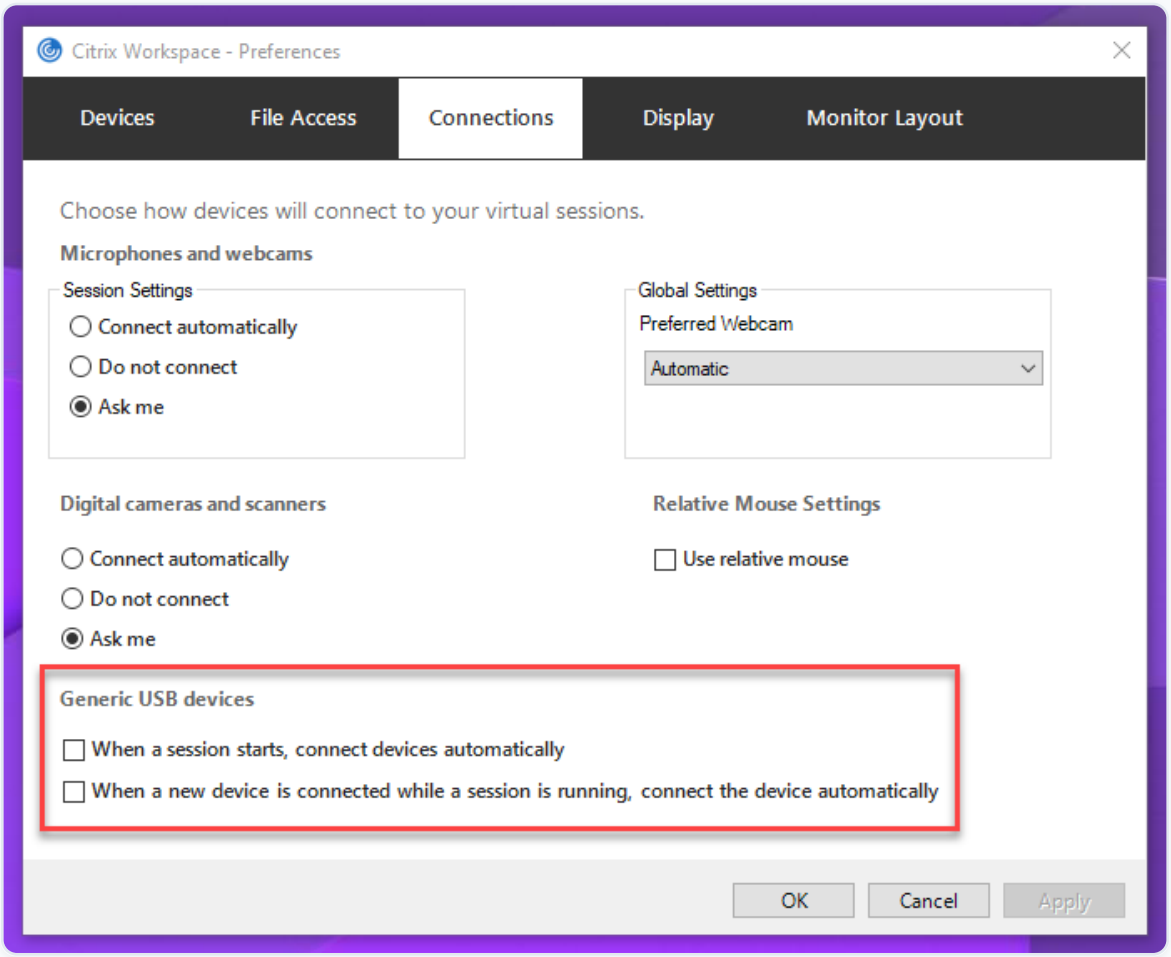
Der Client übernimmt die Kommunikation mit der Webcam. Der Client sendet das Video dann nur an den Server, der es korrekt anzeigen kann. Der Server kommuniziert nicht direkt mit der Webcam, aber seine Integration bietet Ihnen dieselbe Erfahrung auf Ihrem Desktop. Die Workspace-App komprimiert das Video, um Bandbreite zu sparen und eine bessere Ausfallsicherheit in WAN-Szenarien zu gewährleisten.



Hinweis:

- Die Funktion ist für Azure-Maschinen nicht verfügbar, da das Kernelmodul **videodev**, von dem die Funktion abhängt, auf Azure-Maschinen fehlt.
- Die Funktion unterstützt nur H.264-Videos von Ihrem Citrix Workspace-App-Client.
- Die unterstützte Webcam-Auflösung liegt zwischen 48x32 und 1920x1080.

- Wählen Sie nicht **Generische USB-Geräte** aus der Symbolleiste Ihrer Citrix Workspace™-App, wenn Sie eine Webcam verwenden. Andernfalls können unerwartete Probleme auftreten.



Unterstützte 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-Anwendungen unter XenApp und XenDesktop 7.17 und höher. Bei früheren Versionen unterstützt die Citrix Workspace-App für Windows nur 32-Bit-Anwendungen.

PLATTFORM	PROZESSOR
Citrix Workspace-App für Chrome	Da einige ARM-Chromebooks die H.264-Codierung nicht unterstützen, können nur 32-Bit-Apps die optimierte HDX-Webcam-Videokomprimierung verwenden.

Vollständig getestete Webcams

Verschiedene Webcams bieten unterschiedliche Bildraten und haben unterschiedliche Helligkeits- und Kontrastwerte. Citrix® verwendet die folgenden Webcams für die erste Funktionsvalidierung:

- Logitech HD Webcam C270
- Logitech Webcam C930e
- Microsoft-LifeCam-HD3000

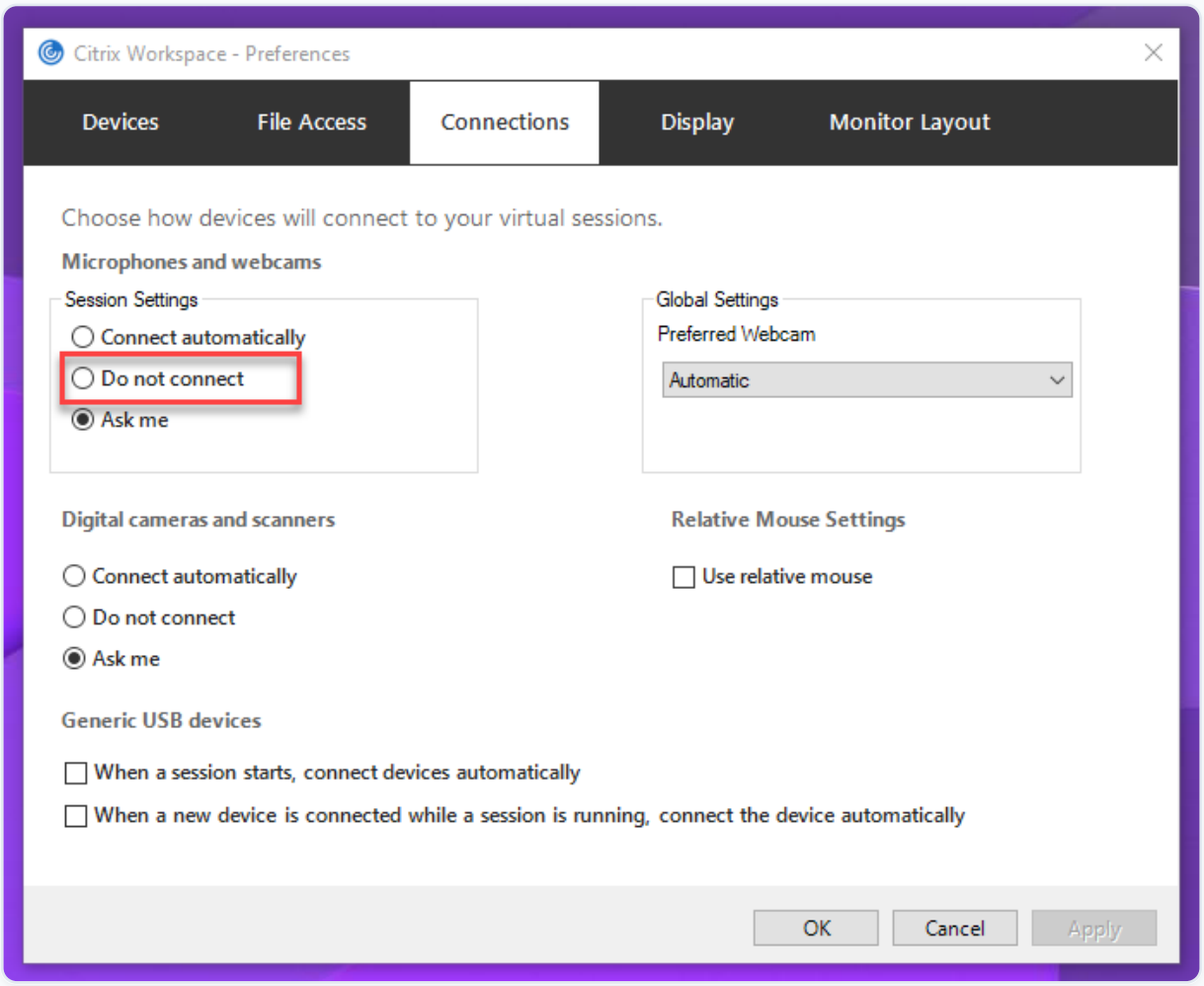
Konfiguration

Diese Funktion ist standardmäßig aktiviert. Um sie zu verwenden, führen Sie die folgende Überprüfung und Konfiguration durch:

> **Tipp:**

> Benutzer der Citrix Workspace-App können die Standardeinstellung überschreiben, indem sie für die Einstellung **Mikrofone und Webcams** des Desktop Viewer die Option **Nicht**

verbinden wählen.



1. Überprüfen Sie nach Abschluss der VDA-Installation, ob sich Ihr VDA beim Delivery Controller™ registrieren kann und die veröffentlichten Linux-Desktopsitzungen erfolgreich mit Windows-Anmeldeinformationen gestartet werden können.
2. Stellen Sie sicher, dass Ihr VDA Internetzugang hat, und führen Sie dann den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um die Webcam-Konfigurationen abzuschließen. Wenn Ihr VDA keinen Internetzugang hat, fahren Sie mit Schritt 3 fort.

> **Hinweis:**
>
> Es kann zu einer Kernel-Inkompatibilität zwischen `uname -r` und Kernel-Headern kommen. Die Inkompatibilität führt dazu, dass das Skript ctxwcamcfg.sh fehlschlägt. Um die HDX-Webcam-Videokomprimierung ordnungsgemäß zu verwenden, führen Sie **sudo apt-get dist-upgrade** aus, starten Sie den VDA neu und führen Sie dann das Skript ctxwcamcfg.sh erneut aus.

> Wenn Ihr VDA unter Debian bereitgestellt wird, stellen Sie sicher, dass er auf der neuesten Kernel-Version läuft. Andernfalls führen Sie die folgenden Befehle aus, um auf die neueste Kernel-Version zu aktualisieren:

```
sudo apt-get update

sudo apt-get dist-upgrade

sudo reboot
```

Wenn Ihr VDA unter SUSE 15.3, SUSE 15.2 oder SUSE 12.5 bereitgestellt wird, führen Sie die folgenden Befehle aus, um auf die neueste Kernel-Version zu aktualisieren und neu zu starten:

```
zypper up kernel-default

reboot
```

Das Skript ctxwcamcfg.sh hilft dabei:

a. Die Programme `kernel-devel` und Dynamic Kernel Module Support (DKMS) auf Ihrem VDA zu installieren.

   - `kernel-devel` wird verwendet, um ein virtuelles Webcam-Kernelmodul der entsprechenden Version zu erstellen.
   - DKMS wird verwendet, um das virtuelle Webcam-Kernelmodul dynamisch zu verwalten.

   > **Hinweis:**

   > Bei der Installation der oben genannten Programme auf RHEL, Rocky Linux und CentOS installiert und aktiviert das Skript `ctxwcamcfg.sh` die folgenden Repositorys auf Ihrem VDA:

   > - Zusätzliche Pakete für Enterprise Linux (EPEL)
   > - RPM Fusion

b. Laden Sie den Open-Source-Code `v4l2loopback` von `<https://github.com/umlaeute/v4l2loopback>` herunter und verwenden Sie DKMS zur Verwaltung von `v4l2loopback`.

   `v4l2loopback` ist ein Kernelmodul, mit dem Sie V4L2-Loopback-Geräte erstellen können.

c. Führen Sie den Befehl `sudo service ctxwcamsd restart` aus. Der Webcam-Dienst des Linux VDA – `ctxwcamsd` – wird neu gestartet und lädt das Kernelmodul `v4l2loopback` für die HDX-Webcam-Videokomprimierungsfunktion.

3. Wenn Ihr VDA keinen Internetzugang hat, erstellen Sie das v4l2loopback-Kernelmodul auf einem anderen Computer und kopieren Sie es dann auf Ihren VDA.

   a. Bereiten Sie einen Computer vor, der Internetzugang hat und dieselbe Kernel-Version wie Ihr VDA besitzt. Der Befehl `uname -r` hilft, Kernel-Versionen zu finden.

   b. Führen Sie auf dem Computer den Befehl `sudo mkdir -p /var/xdl` aus.

   c. Kopieren Sie `/var/xdl/configure_*` von Ihrem VDA auf den Computer unter `/var/xdl/`.

   d. Führen Sie auf dem Computer den Befehl `sudo /opt/Citrix/VDA/sbin/ctxwcamcfg.sh` aus, um das Kernelmodul zu erstellen. Wenn der Befehl erfolgreich ausgeführt wird, erstellt er eine Datei v4l2loopback.ko unter dem Pfad `/var/lib/dkms/v4l2loopback/1.81b8df79107d1fbf392fdcbaa051bd227a9c94c1/$(uname -r)/x86_64/module/`. Ignorieren Sie Fehler, die beim Ausführen des Skripts ctxwcamcfg.sh auftreten können.

   e. Kopieren Sie v4l2loopback.ko vom Computer auf Ihren VDA und legen Sie es unter `/opt/Citrix/VDA/lib64/` ab.

   f. Führen Sie auf Ihrem VDA den Befehl `sudo service ctxwcamsd restart` aus, um den Webcam-Dienst neu zu starten und das v4l2loopback-Kernelmodul zu laden.

Domänenunabhängige Linux-VDAs

Übersicht

Domänenunabhängige VDAs machen es überflüssig, VDAs für die VDA- und Benutzerauthentifizierung Active Directory-Domänen beizutreten. Beim Erstellen eines domänenunabhängigen VDAs generieren Sie ein Public-Private-Schlüsselpaar, um den VDA bei der Cloud-Steuerungsebene zu registrieren. Somit ist der Beitritt zu einer Active Directory-Domäne

nicht mehr erforderlich. Wenn ein Benutzer eine Sitzung vom domänenunabhängigen VDA startet, erstellt der VDA ein lokales Zuordnungskonto unter Verwendung des Benutzernamens, den der Benutzer für die Anmeldung bei der Citrix Workspace-App verwendet. Der VDA weist ein zufälliges Kennwort zu, das das lokale Zuordnungskonto für SSO und die Sitzungswiederverbindung verwendet. Wenn Sie das zufällige Kennwort ändern, schlagen SSO und die Sitzungswiederverbindung fehl. Um SSO zu deaktivieren, siehe Nicht-SSO-Authentifizierung.

Wichtig:

- Domänenunabhängige VDAs werden für Citrix DaaS unterstützt.
  - Ihre Steuerungsebene muss über Citrix DaaS bereitgestellt werden.
  - Sie können domänenunabhängige VDAs in einer Public Cloud oder einem lokalen Rechenzentrum bereitstellen. Die Steuerungsebene in Citrix DaaS verwaltet domänenunabhängige VDAs.
  - Sie können Rendezvous V2 konfigurieren, um Citrix Cloud Connectors zu umgehen. Andernfalls müssen Sie Cloud Connectors installieren, um VDAs mit Ihrer Steuerungsebene zu verbinden.
- Um domänenunabhängige VDAs zu erstellen, müssen Sie Machine Creation Services™ (MCS) verwenden.
  - MCS unterstützt keine Bare-Metal-Server.

Verfügbare Funktionen für domänenunabhängige Linux-VDAs

Lokale Benutzer mit angegebenen Attributen auf domänenunabhängigen VDAs erstellen

Wenn Sie eine Sitzung öffnen, die auf einem domänenunabhängigen VDA gehostet wird, erstellt der VDA automatisch einen lokalen Benutzer mit Standardattributen. Der VDA erstellt den lokalen Benutzer basierend auf dem Benutzernamen, den Sie für die Anmeldung bei der Citrix Workspace™-App verwendet haben. Sie können auch Benutzerattribute angeben, einschließlich der **Benutzer-ID (UID)**, **Gruppen-ID (GID)**, des **Home-Verzeichnisses** und der **Anmelde-Shell** des Benutzers. Um diese Funktion zu verwenden, führen Sie die folgenden Schritte aus:

1. Führen Sie den folgenden Befehl aus, um die Funktion zu aktivieren:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent\LocalMappedAccount" -t
"REG_DWORD" -v "CreateWithUidGid" -d "0x00000001" --force
```

2. Geben Sie die folgenden Attribute im `/var/xdl/getuidgid.sh`-Skript unter dem Installationspfad des VDAs an:

ATTRIBUT	ERFORDERLICH ODER OPTIONAL	BESCHREIBUNG
`uid`	Erforderlich	Eine Benutzerkennung (UID) ist eine von Linux jedem Benutzer im System zugewiesene Nummer. Sie bestimmt, auf welche Systemressourcen der Benutzer zugreifen kann.
`gid`	Erforderlich	Eine Gruppenkennung (GID) ist eine Nummer, die eine bestimmte Gruppe darstellt.
`homedir`	Optional	Das Linux-Home-Verzeichnis ist ein Verzeichnis für einen bestimmten Benutzer.
`shell`	Optional	Eine Anmelde-Shell ist eine Shell, die einem Benutzer **bei der Anmeldung** an seinem Benutzerkonto zugewiesen wird.

Das Folgende ist ein Beispiel für das `getuidgid.sh`-Skript:

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
```

Authentifizierung ohne SSO

Standardmäßig ist bei Linux VDA Single Sign-On (SSO) aktiviert. Benutzer melden sich mit einem Satz von Anmeldeinformationen bei der Citrix Workspace-App und bei VDA-Sitzungen an. Um Benutzern die Anmeldung bei VDA-Sitzungen mit einem anderen Satz von Anmeldeinformationen zu ermöglichen, deaktivieren Sie SSO auf dem Linux VDA. Weitere Informationen finden Sie unter Authentifizierung ohne SSO.

Authentifizierung mit Azure Active Directory

Die nicht in die Domäne eingebundenen VDAs, die Sie in Azure bereitstellen, werden in den AAD-Identitätsdienst integriert, um die Benutzerauthentifizierung bereitzustellen. Weitere Informationen finden Sie unter Authentifizierung mit Azure Active Directory.

Rendezvous V2

Nicht in die Domäne eingebundene VDAs werden für die Verwendung von Rendezvous V2 unterstützt, um Citrix Cloud Connectors zu umgehen. Weitere Informationen finden Sie unter Rendezvous V2.

Nicht in die Domäne eingebundene Linux-VDAs erstellen

Verwenden Sie MCS, um nicht in die Domäne eingebundene Linux-VDAs in Citrix DaaS zu erstellen. Weitere Informationen finden Sie unter Erstellen nicht in die Domäne eingebundener Linux-VDAs.

Liste der unterstützten Richtlinien

Liste der unterstützten Richtlinien für Linux VDA

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Lokale Clientzeit verwenden	UseLocalTimeOfClient	Benutzer	ICA\Time Zone Control	Server-Zeitzone verwenden
ICA-Roundtrip-Berechnung	IcaRoundTripCheckEnabled	Computer	ICA\End User Monitoring	Aktiviert (1)

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
ICA-Roundtrip-Berechnungsintervall	IcaRoundTripCheckPeriod	Computer	ICA\End User Monitoring	15
ICA-Roundtrip-Berechnungen für inaktive Verbindungen	IcaRoundTripCheckWhenIdle	Computer	ICA\End User Monitoring	Deaktiviert (0)
Gesamte Sitzungsbandbreitenbegrenzung	LimitOverallBw	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Audio-Umleitung	LimitAudioBw	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für Audio-Umleitung (Prozentsatz)	LimitAudioBwPercent	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für die Umleitung von Client-USB-Geräten	LimitUSBBw	Benutzer	ICA\Bandwidth	0
Bandbreitenprozentsatz für die Client-USB-Geräteumleitung	LimitUSBBwPercent	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für	LimitCdmBw	Benutzer	ICA\Bandwidth	0

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
die Dateiumleitung				
Bandbreitenbegrenzungsprozentsatz für die Dateiumleitung	LimitCdmBwPercent	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzung für die Druckerumleitung	LimitPrinterBw	Benutzer	ICA\Bandwidth	0
Bandbreitenbegrenzungsprozentsatz für die Druckerumleitung	LimitPrinterBwPercent	Benutzer	ICA\Bandwidth	0
WebSockets-Verbindungen	AcceptWebSocketsConnections	Computer	ICA\WebSockets	Verboten
WebSockets-Portnummer	WebSocketsPort	Computer	ICA\WebSockets	8008
Liste der vertrauenswürdigen WebSockets-Ursprungsserver	WSTrustedOriginServerList	Computer	ICA\WebSockets	*
ICA®-Keep-Alives	SendICAKeepAlives	Computer	**ICA-Keep-Alive**	Keine ICA-Keep-Alive-Nachrichten senden (0)

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
ICA Keep-Alive-Timeout	ICAKeepAliveTimeout	Computer	**ICA Keep-Alive**	60 Sekunden
ICA-Listener-Portnummer	IcaListenerPortNumber	Computer	ICA	1494
HDX™ adaptiver Transport	HDXoverUDP	Computer	ICA	Bevorzugt(2)
Sitzungszuverlässigkeitsverbindungen	AcceptSessionReliabilityConnections	Computer	ICA\Session Reliability	Zulässig(1)
Transparenzstufe der Wiederverbindungs-UI	ReconnectionUiTransparencyLevel	Computer	ICA\Automatischer Client-Reconnect	80 %
Portnummer für Sitzungszuverlässigkeit	SessionReliabilityPort	Computer	ICA\Sitzungszuverlässigkeit	2598
Zeitüberschreitung für Sitzungszuverlässigkeit	SessionReliabilityTimeout	Computer	ICA\Sitzungszuverlässigkeit	180 s
Automatischer Client-Reconnect	AllowAutoClientReconnect	Benutzer	ICA\Automatischer Client-Reconnect	Zulässig (1)
Client-Audio-Umleitung	AllowAudioRedirection	Benutzer	Audio	Zulässig (1)
Clientdruckerumleitung	AllowPrinterRedir	Benutzer	Drucken	Zulässig (1)

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
PDF-Universaldrucker automatisch erstellen	AutoCreatePDFPrinter	Benutzer	Drucken	Deaktiviert (0)
Druckertreiberzuordnung und -kompatibilität	DriverMappingList	Benutzer	Drucken	`"Microsoft XPS Document Writer *, Deny;Send to Microsoft OneNote *, Deny"`
Client-Zwischenablageumleitung	AllowClipboardRedir	Benutzer	Zwischenablage	Zulässig (1)
Größe der Zwischenablageübertragung vom Client zur Sitzung begrenzen	LimitClipboardTransferC2H	Benutzer	ICA	Deaktiviert (0)
Sitzungs-Zwischenablage auf Client-Übertragungsgröße beschränken	LimitClipboardTransferH2C	Benutzer	ICA	Deaktiviert (0)
Bandbreitenbegrenzung für die Zwischenablagenumleitung	LimitClipbdBW	Benutzer	ICA\Bandwidth	0
Prozentsatz der	LimitClipbdBWPercent	Benutzer	ICA\Bandwidth	0

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Bandbreitenbegrenzung für die Zwischenablagenumleitung				
Schreibzugriff der Client-Zwischenablage einschränken	RestrictClientClipboardWrite	Benutzer	Zwischenablage	Deaktiviert (0)
Zulässige Formate für den Schreibzugriff der Client-Zwischenablage	ClientClipboardWriteAllowedFormats	Benutzer	Zwischenablage	N/A
Schreiben der Sitzungszwischenablage einschränken	RestrictSessionClipboardWrite	Benutzer	Zwischenablage	Deaktiviert (0)
Zulässige Formate für das Schreiben der Sitzungszwischenablage	SessionClipboardWriteAllowedFormats	Benutzer	Zwischenablage	N/A
Client-USB-Geräteumleitung	AllowUSBRedir	Benutzer	USB	Verboten (0)
Regeln für die Client-USB-Geräteumleitung	USBDeviceRules	Benutzer	USB	"\0"

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Bewegtbildkomprimierung	MovingImageCompressionConfiguration	Benutzer	Thinwire	Aktiviert (1)
Zusätzliche Farbkomprimierung	ExtraColorCompression	Benutzer	Thinwire	Deaktiviert (0)
Ziel-Mindestbildrate	TargetedMinimumFramesPerSecond	Benutzer	Thinwire	10 Bilder pro Sekunde
Zielbildrate	FramesPerSecond	Benutzer	Thinwire	30 Bilder pro Sekunde
Visuelle Qualität	VisualQuality	Benutzer	Thinwire	Mittel (3)
Videocodec für Komprimierung verwenden	VideoCodec	Benutzer	Thinwire	Verwenden, wenn bevorzugt (3)
Hardware-Kodierung für Videocodec verwenden	UseHardwareEncodingForVideoCodec	Benutzer	Thinwire	Aktiviert (1)
Visuell verlustfreie Komprimierung zulassen	AllowVisuallyLosslessCompression	Benutzer	Thinwire	Deaktiviert (0)
Für 3D-Grafik-Workload optimieren	OptimizeFor3dWorkload	Benutzer	Thinwire	Deaktiviert (0)
Bevorzugte Farbtiefe für	PreferredColorDepth	Benutzer	Thinwire	24 Bit pro Pixel (1)

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
einfache Grafiken				
Audioqualität	SoundQuality	Benutzer	Audio	Hoch – High-Definition-Audio (2)
Client-Mikrofonumleitung	AllowMicrophoneRedir	Benutzer	Audio	Zulässig (1)
Maximale Anzahl von Sitzungen	MaximumNumberOfSessions	Computer	Lastverwaltung	250
Toleranz für gleichzeitige Anmeldungen	ConcurrentLogonsTolerance	Computer	Lastverwaltung	2
Automatische Aktualisierung der Controller aktivieren	EnableAutoUpdateOfControllers	Computer	Einstellungen für Virtual Delivery Agent	Zulässig (1)
Aktualisierungsmodus für die Zwischenablageauswahl	ClipboardSelectionUpdateMode	Benutzer	Zwischenablage	3
Aktualisierungsmodus für die primäre Auswahl	PrimarySelectionUpdateMode	Benutzer	Zwischenablage	3
Maximale Speex-Qualität	MaxSpeexQuality	Benutzer	Audio	5
Automatische Verbindung von	AutoConnectDrives	Benutzer	Dateiumleitung\CDM	Aktiviert (1)

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Clientlaufwerken				
Client-optische Laufwerke	AllowCdromDrives	Benutzer	Dateiumleitung\CDM	Zugelassen (1)
Client-Festplattenlaufwerke	AllowFixedDrives	Benutzer	Dateiumleitung\CDM	Zugelassen (1)
Client-Diskettenlaufwerke	AllowFloppyDrives	Benutzer	Dateiumleitung\CDM	Zugelassen (1)
Client-Netzwerklaufwerke	AllowNetworkDrives	Benutzer	Dateiumleitung\CDM	Zulässig (1)
Clientlaufwerksumleitung	AllowDriveRedir	Benutzer	Dateiumleitung\CDM	Zulässig (1)
Schreibgeschützter Client-Laufwerkszugriff	ReadOnlyMappedDrive	Benutzer	Dateiumleitung\CDM	Deaktiviert (0)
Automatische Tastaturanzeige	AllowAutoKeyboardPopUp	Benutzer	MRVC	Deaktiviert (0)
Dateitransfer zwischen Desktop und Client zulassen	AllowFileTransfer	Benutzer	Dateiübertragung	Zulässig
Datei vom Desktop herunterladen	AllowFileDownload	Benutzer	Dateiübertragung	Zulässig

STUDIO-RICHTLINIE	SCHLÜSSELNAME	TYP	MODUL	STANDARDWERT
Datei auf den Desktop hochladen	AllowFileUpload	Benutzer	Dateiübertragung	Zulässig
Sitzungs-Inaktivitäts-Timer	EnableSessionIdleTimer	Benutzer	Sitzungs-Timer	Aktiviert (1)
Intervall des Sitzungs-Inaktivitäts-Timers	SessionIdleTimerInterval	Benutzer	Sitzungs-Timer	1440 Minuten
Timer für getrennte Sitzung	EnableSessionDisconnectTimer	Benutzer	Sitzungs-Timer	Deaktiviert (0)
Intervall des Timers für getrennte Sitzung	SessionDisconnectTimerPeriod	Benutzer	Sitzungstimer	1440 Minuten
Browserinhaltsumleitung	WebBrowserRedirection	Computer	ICA\Multimedia	Zulässig
Browserinhaltsumleitung ACL-Konfiguration	WebBrowserRedirectionAcl	Benutzer	ICA\Multimedia	`https://www.youtube.com/*`
Browserinhaltsumleitung Blacklist-Konfiguration	WebBrowserRedirectionBlacklist	Benutzer	ICA\Multimedia	Null
Browserinhaltsumleitung Proxy-Konfiguration	WebBrowserRedirectionProxy	Benutzer	ICA\Multimedia	Null

> **Hinweis:**

> Nur der Windows Virtual Delivery Agent (VDA) unterstützt Audio über das User Datagram Protocol (UDP). Der Linux VDA unterstützt dies nicht. Weitere Informationen finden Sie unter Audio über User Datagram Protocol (UDP) Real-time Transport.

> Sie können die folgenden Citrix-Richtlinieneinstellungen verwenden, um Sitzungsverbindungstimer in Citrix Studio zu konfigurieren:

- **Sitzungs-Inaktivitätstimer**: Legt fest, ob eine Zeitbegrenzung für inaktive Sitzungen erzwungen werden soll.
- **Sitzungs-Inaktivitätstimer-Intervall**: Legt ein Zeitlimit für inaktive Sitzungen fest. Wenn der **Sitzungs-Inaktivitätstimer** auf **Aktiviert** steht und eine aktive Sitzung während der festgelegten Zeit keine Benutzereingaben erhalten hat, wird die Sitzung getrennt.
- **Timer für getrennte Sitzungen**: Legt fest, ob ein Zeitlimit für getrennte Sitzungen erzwungen werden soll.
- **Intervall für Timer für getrennte Sitzungen**: Legt ein Intervall fest, bevor eine getrennte Sitzung abgemeldet wird.

Wenn Sie eine der Richtlinieneinstellungen aktualisieren, stellen Sie sicher, dass diese in Ihrer gesamten Bereitstellung konsistent sind.

Eine Warnmeldung wird angezeigt, wenn Ihr Zeitlimit für inaktive Sitzungen abläuft. Ein Beispiel finden Sie in der folgenden Bildschirmaufnahme. Durch Klicken auf **OK** wird die Warnmeldung geschlossen, aber Ihre Sitzung kann dadurch nicht aktiv gehalten werden. Um Ihre Sitzung aktiv zu halten, geben Sie Benutzereingaben ein, um den Inaktivitätstimer zurückzusetzen.

Warnmeldung(/en-us/linux-virtual-delivery-agent/2308/media/warning-message-idle-session-timeout.png)

Die folgenden Richtlinien können in Citrix Studio Version 7.12 und höher konfiguriert werden.

- MaxSpeexQuality

  Wert (Ganzzahl):

  Standardwert: 5

  Details:

Die Audioumleitung kodiert Audiodaten mit dem Speex-Codec, wenn die Audioqualität mittel oder niedrig ist (siehe die Richtlinie Audioqualität). Speex ist ein verlustbehafteter Codec, was bedeutet, dass er Komprimierung auf Kosten der Wiedergabetreue des eingehenden Sprachsignals erreicht. Im Gegensatz zu einigen anderen Sprach-Codecs ist es möglich, den Kompromiss zwischen Qualität und Bitrate zu steuern. Der Speex-Kodierungsprozess wird meistens durch einen Qualitätsparameter gesteuert, der von 0 bis 10 reicht. Je höher die Qualität, desto höher die Bitrate.

Die maximale Speex-Qualität wählt die beste Speex-Qualität, um Audiodaten entsprechend der Audioqualität und der Bandbreitenbegrenzung zu kodieren (siehe die Richtlinie Bandbreitenbegrenzung für Audioumleitung). Wenn die Audioqualität mittel ist, befindet sich der Encoder im Breitbandmodus, was eine höhere Abtastrate bedeutet. Wenn die Audioqualität niedrig ist, befindet sich der Encoder im Schmalbandmodus, was eine niedrigere Abtastrate bedeutet. Dieselbe Speex-Qualität hat in verschiedenen Modi unterschiedliche Bitraten. Die beste Speex-Qualität ist erreicht, wenn der größte Wert die folgenden Bedingungen erfüllt:

- Er ist gleich oder kleiner als die maximale Speex-Qualität.
- Seine Bitrate ist gleich oder kleiner als die Bandbreitenbegrenzung.

Verwandte Einstellungen: Audioqualität, Bandbreitenbegrenzung für Audio-Umleitung

- PrimarySelectionUpdateMode

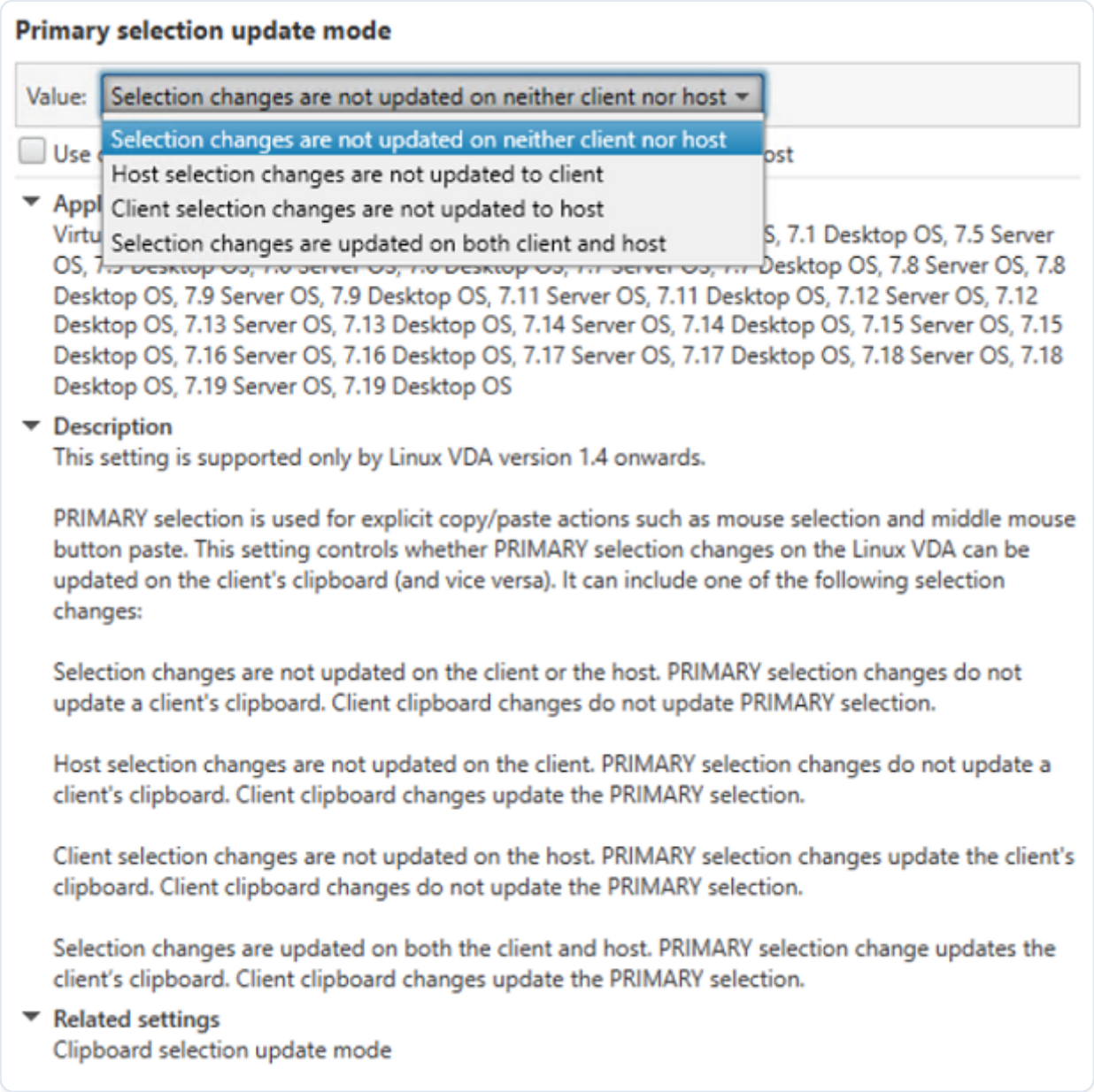
  Wert (Enum):

  Standardwert: 3

  Details:

  Die primäre Auswahl wird verwendet, wenn Sie Daten auswählen und diese durch Drücken der mittleren Maustaste einfügen.

  Diese Richtlinie steuert, ob Änderungen der primären Auswahl auf dem Linux VDA und dem Client die Zwischenablage gegenseitig aktualisieren können. Es gibt vier Wertoptionen:



- **Auswahländerungen werden weder auf dem Client noch auf dem Host aktualisiert**

  Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Host-Auswahländerungen werden nicht auf den Client aktualisiert**

  Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA.

- **Client-Auswahländerungen werden nicht auf den Host aktualisiert**

Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Auswahländerungen werden sowohl auf dem Client als auch auf dem Host aktualisiert**

  Änderungen der primären Auswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der primären Auswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA. Diese Option ist der Standardwert.

Verwandte Einstellung: Aktualisierungsmodus für die Zwischenablagen-Auswahl

- ClipboardSelectionUpdateMode

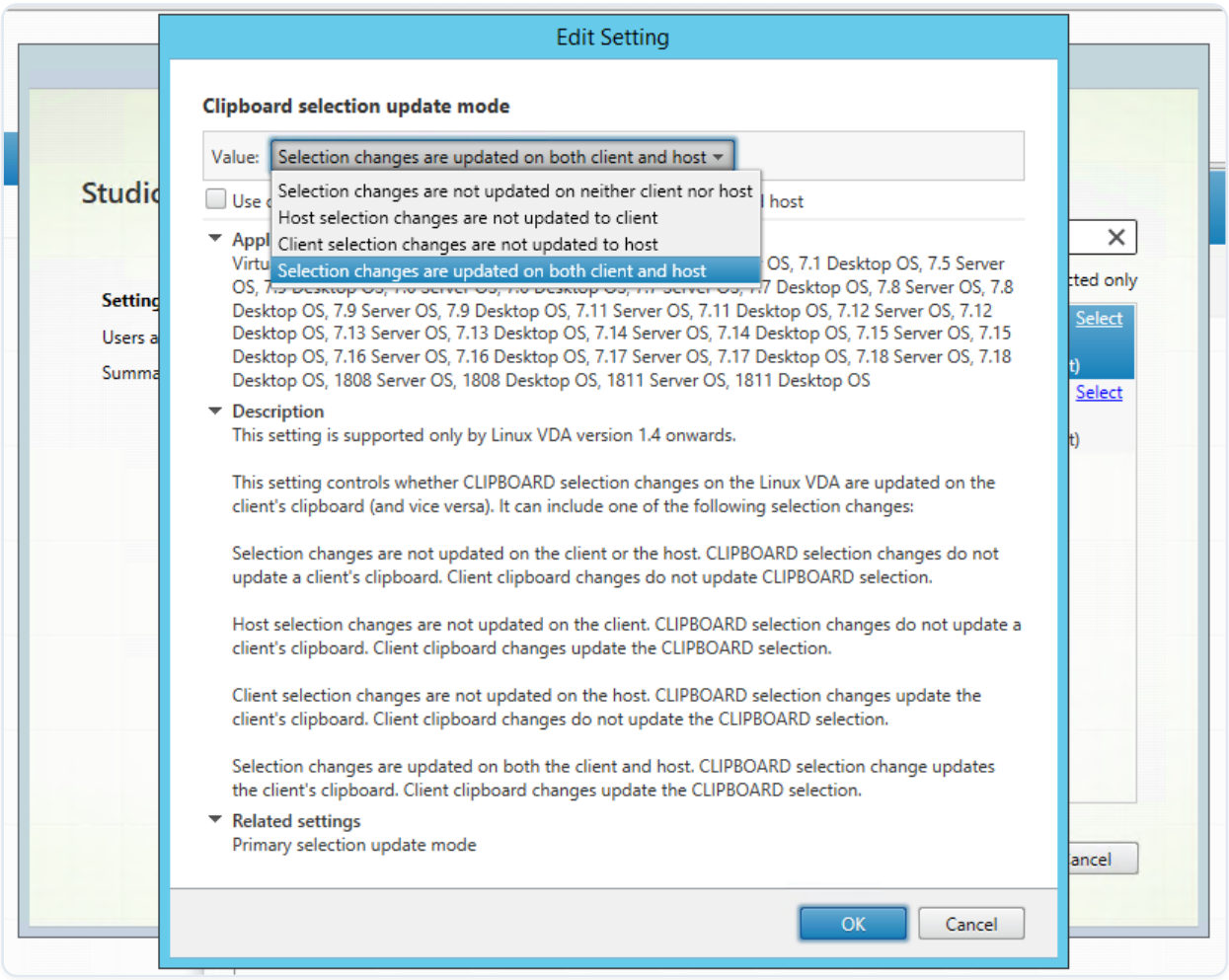
  Wert (Enum):

  Standardwert: 3

  Details:

  Die Zwischenablageauswahl wird verwendet, wenn Sie Daten auswählen und explizit anfordern, dass diese in die Zwischenablage „kopiert“ werden, z. B. durch Auswahl von „Kopieren“ aus dem Kontextmenü. Die Zwischenablageauswahl wird hauptsächlich in Verbindung mit Microsoft Windows-Zwischenablagevorgängen verwendet, während die primäre Auswahl einzigartig für Linux ist.

  Diese Richtlinie steuert, ob Änderungen der Zwischenablageauswahl auf dem Linux VDA und dem Client die Zwischenablage des jeweils anderen aktualisieren können. Es gibt vier Wertoptionen:



- **Auswahländerungen werden weder auf dem Client noch auf dem Host aktualisiert**

  Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Host-Auswahländerungen werden nicht auf den Client aktualisiert**

  Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client nicht. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA.

- **Client-Auswahländerungen werden nicht auf den Host aktualisiert**

  Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA nicht.

- **Auswahländerungen werden sowohl auf dem Client als auch auf dem Host aktualisiert**

Änderungen der Zwischenablageauswahl auf dem Linux VDA aktualisieren die Zwischenablage auf dem Client. Änderungen der Zwischenablageauswahl auf dem Client aktualisieren die Zwischenablage auf dem Linux VDA. Diese Option ist der Standardwert.

Zugehörige Einstellung: Aktualisierungsmodus für primäre Auswahl

Hinweis:

Der Linux VDA unterstützt sowohl die Zwischenablageauswahl als auch die primäre Auswahl. Um das Kopier- und Einfügeverhalten zwischen dem Linux VDA und dem Client zu steuern, empfehlen wir, sowohl den Aktualisierungsmodus für die Zwischenablageauswahl als auch den Aktualisierungsmodus für die primäre Auswahl auf denselben Wert einzustellen.

Drucken

Dieser Abschnitt enthält die folgenden Themen:

- Bewährte Methoden für den Druck
- PDF-Druck

Bewährte Methoden für den Druck

Dieser Artikel enthält Informationen zu bewährten Methoden für den Druck.

Installation

Der Linux-VDA erfordert sowohl **cups**- als auch **foomatic**-Filter. Die Filter werden bei der Installation des VDA installiert. Sie können die Filter auch manuell je nach Distribution installieren. Beispiel:

Unter RHEL 7:

```
sudo yum –y install cups



sudo yum -y install foomatic-filters
```

Druckrichtlinieneinstellungen

Client-Druckerumleitung

Diese Einstellung steuert, ob Clientdrucker einer VDA-Sitzung zugeordnet werden. Standardmäßig ist die Clientdruckerzuordnung zulässig.

Clientdrucker automatisch erstellen

Diese Einstellung gibt Clientdrucker an, die VDA-Sitzungen zugeordnet werden können. Standardmäßig ist sie auf **Alle Clientdrucker automatisch erstellen** festgelegt, was bedeutet, dass alle Clientdrucker VDA-Sitzungen zugeordnet werden. Weitere Informationen zu dieser Einstellung finden Sie unter Clientdrucker automatisch erstellen in der Citrix Virtual Apps and Desktops-Dokumentation.

PDF-Universaldrucker automatisch erstellen

Um die Funktion PDF-Druck zu verwenden, setzen Sie diese Richtlinie auf **Aktiviert**.

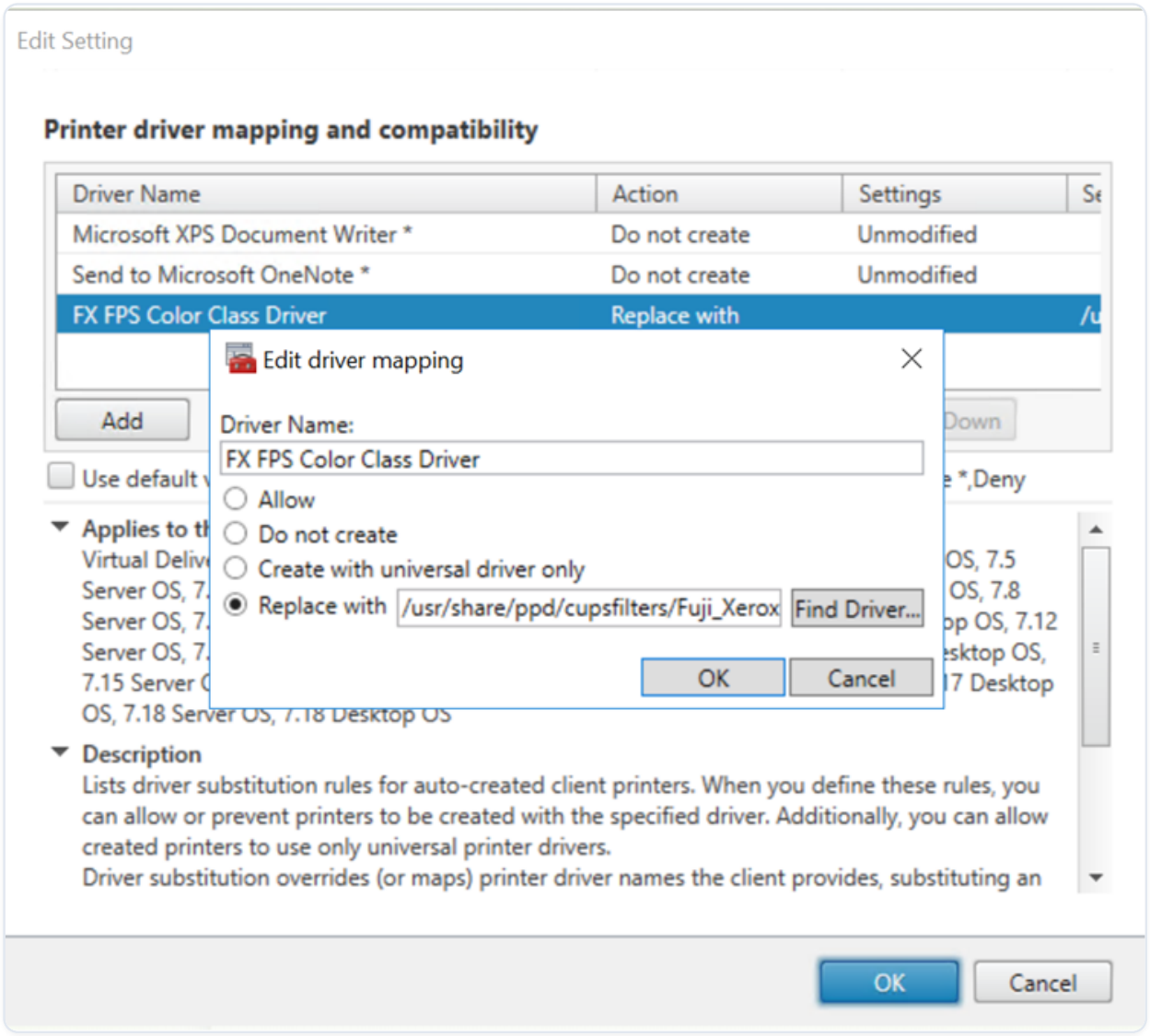
Druckertreiberzuordnung und -kompatibilität

Citrix bietet drei Arten von Universaldruckertreibern (PostScript, PCL5 und PCL6). Der Universaldruckertreiber ist jedoch möglicherweise nicht mit Ihrem Clientdrucker kompatibel. In früheren Releases bestand die einzige Möglichkeit darin, die Konfigurationsdatei ~/.CtxlpProfile$CLIENT_NAME zu bearbeiten. Ab Version 1906 können Sie stattdessen die Richtlinie **Druckertreiberzuordnung und -kompatibilität** in Citrix Studio konfigurieren.

So konfigurieren Sie die Richtlinie **Druckertreiberzuordnung und -kompatibilität** in Citrix Studio:

1. Wählen Sie die Richtlinie **Druckertreiberzuordnung und -kompatibilität** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie unter **Treibername** den Treibernamen des Clientdruckers ein. Wenn Sie die Citrix Workspace™-App für Linux verwenden, geben Sie stattdessen den Druckernamen ein.

   4\. Wählen Sie **Ersetzen durch** und geben Sie den absoluten Pfad der Treiberdatei auf dem VDA ein.



Hinweis:

- Es werden nur PPD-Treiberdateien unterstützt.
- Andere Optionen der Richtlinie **Druckertreiberzuordnung und -kompatibilität** werden nicht unterstützt. Nur **Ersetzen durch** wird wirksam.

Verwendung

Sie können sowohl von veröffentlichten Desktops als auch von veröffentlichten Anwendungen drucken. Alle Clientdrucker können einer VDA-Sitzung zugeordnet werden. Die Druckernamen sind für Desktops und Anwendungen unterschiedlich:

- Für veröffentlichte Desktops:

`<client printer name>:$CLIENT_NAME:dsk$SESSION_ID`

- Für veröffentlichte Anwendungen:

`<client printer name>:$CLIENT_NAME:app$SESSION_ID`

> **Hinweis:**
>
> Wenn derselbe Benutzer sowohl einen veröffentlichten Desktop als auch eine veröffentlichte Anwendung öffnet, stehen beide Drucker der Sitzung zur Verfügung. Das Drucken auf einem Desktopdrucker in einer veröffentlichten Anwendungssitzung oder das Drucken auf einem Anwendungsdrucker in einem veröffentlichten Desktop schlägt fehl.

Problembehandlung

Drucken nicht möglich

Wenn der Druck nicht ordnungsgemäß funktioniert, überprüfen Sie den Druck-Daemon **ctxlpmngt** und das **CUPS-Framework**.

Der Druck-Daemon **ctxlpmngt** ist ein pro Sitzung ausgeführter Prozess und muss für die Dauer der Sitzung ausgeführt werden. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Druck-Daemon ausgeführt wird. Wenn **ctxlpmngt** nicht ausgeführt wird, starten Sie **ctxlpmngt** manuell über eine Befehlszeile.

```
ps –ef | grep ctxlpmngt
```

Wenn der Druck immer noch nicht funktioniert, überprüfen Sie das **CUPS**-Framework. Der Dienst **ctxcups** wird für die Druckerverwaltung verwendet und kommuniziert mit dem Linux-CUPS-Framework. Es handelt sich um einen einzelnen Prozess pro Maschine, der mit dem folgenden Befehl überprüft werden kann:

```
service ctxcups status
```

Zusätzliche Schritte zum Sammeln von CUPS-Protokollen

Um CUPS-Protokolle zu sammeln, führen Sie die folgenden Befehle aus, um die CUPS-Dienstdatei zu konfigurieren. Andernfalls können CUPS-Protokolle nicht in **hdx.log** aufgezeichnet werden:

```
sudo service cups stop


sudo vi /etc/systemd/system/printer.target.wants/cups.service


PrivateTmp=false


sudo service cups start


sudo systemctl daemon-reload
```

Hinweis:

Diese Konfiguration dient nur zum Sammeln des vollständigen Druckprotokolls, wenn ein Problem auftritt. Unter normalen Umständen wird diese Konfiguration nicht empfohlen, da sie die CUPS-Sicherheit beeinträchtigt.

Druckausgabe ist fehlerhaft

Ein inkompatibler Druckertreiber kann zu einer fehlerhaften Ausgabe führen. Eine treiberspezifische Konfiguration pro Benutzer ist verfügbar und kann durch Bearbeiten der Konfigurationsdatei **~/.CtxlpProfile$CLIENT_NAME** konfiguriert werden:

```
[DEFAULT_PRINTER]


printername=


model=
```

```
ppdpath=


drivertype=
```

Wichtig:

Das Feld **printername** enthält den Namen des aktuellen clientseitigen Standarddruckers. Es ist ein schreibgeschützter Wert. Bearbeiten Sie ihn nicht.

Die Felder **ppdpath**, **model** und **drivertype** können nicht gleichzeitig festgelegt werden, da nur eines für den **mapped printer** wirksam wird.

- Wenn der universelle Druckertreiber nicht mit dem Clientdrucker kompatibel ist, konfigurieren Sie das Modell des nativen Druckertreibers mithilfe der Option **model**=. Sie können den aktuellen Modellnamen des Druckers mit dem Befehl **lpinfo** ermitteln:

  ```
  lpinfo –m


  …


  xerox/ph3115.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0


  xerox/ph3115fr.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0

  xerox/ph3115pt.ppd.gz Xerox Phaser 3115, SpliX V. 2.0.0
  ```

  Sie können das Modell dann so einstellen, dass es dem Drucker entspricht:

```
model=xerox/ph3115.ppd.gz
```

- Wenn der universelle Druckertreiber nicht mit dem Clientdrucker kompatibel ist, konfigurieren Sie den PPD-Dateipfad des nativen Druckertreibers. Der Wert von **ppdpath** ist der absolute Pfad der nativen Druckertreiberdatei.

  Beispiel: Es gibt einen **ppd driver** unter /home/tester/NATIVE_PRINTER_DRIVER.ppd:

  ```
  ppdpath=/home/tester/NATIVE_PRINTER_DRIVER.ppd
  ```

- Es gibt drei Arten von universellen Druckertreibern, die von Citrix bereitgestellt werden (Postscript, PCL5 und PCL6). Sie können den Treibertyp basierend auf Ihren Druckereigenschaften konfigurieren.

  Wenn beispielsweise der Standard-Druckertreibertyp des Clients PCL5 ist, setzen Sie **drivertype** auf:

  ```
  drivertype=pcl5
  ```

Ausgabegröße ist null

Probieren Sie verschiedene Druckertypen aus. Und versuchen Sie es mit einem virtuellen Drucker wie CutePDF und PDFCreator, um herauszufinden, ob dieses Problem mit dem Druckertreiber zusammenhängt.

Der Druckauftrag hängt vom Druckertreiber des Standard-Clientdruckers 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 wählt, kann ein Problem auftreten.

Wenn der Druckertreibertyp korrekt ist, können Sie das Problem identifizieren, indem Sie die folgenden Schritte ausführen:

1. Melden Sie sich bei einer veröffentlichten Desktopsitzung an.
2. Führen Sie den Befehl **vi ~/.CtxlpProfile$CLIENT_NAME** aus.
3. Fügen Sie das folgende Feld hinzu, um die Spool-Datei auf dem Linux VDA zu speichern:

   ```
   deletespoolfile=no
   ```

4. Melden Sie sich ab und wieder an, um die Konfigurationsänderungen zu laden.

5. Drucken Sie das Dokument, um das Problem zu reproduzieren. Nach dem Drucken wird eine Spool-Datei unter `/var/spool/cups-ctx/$logon_user/$spool_file` gespeichert.
6. Überprüfen Sie, ob der Spool leer ist. Wenn die Spool-Datei null ist, deutet dies auf ein Problem hin. Wenden Sie sich an den Citrix Support (und stellen Sie das Druckprotokoll bereit), um weitere Unterstützung zu erhalten.
7. Wenn die Spool-Größe nicht null ist, kopieren Sie die Datei auf den Client. Der Inhalt der Spool-Datei hängt vom Druckertreibertyp des Standarddruckers des Clients ab. Wenn der Treiber des **zugeordneten Druckers** (nativ) PostScript ist, kann die Spool-Datei direkt im Linux-Betriebssystem geöffnet werden. Überprüfen Sie, ob der Inhalt korrekt ist.

   Wenn die Spool-Datei PCL ist oder wenn das Client-Betriebssystem Windows ist, kopieren Sie die Spool-Datei auf den Client und drucken Sie sie auf dem clientseitigen Drucker mit einem anderen Druckertreiber.
8. Ändern Sie den **zugeordneten Drucker**, um einen anderen Druckertreiber zu verwenden. Das folgende Beispiel verwendet den PostScript-Clientdrucker als Beispiel:

   a. Melden Sie sich bei einer aktiven Sitzung an und öffnen Sie einen Browser auf dem Client-Desktop.

   b. Öffnen Sie das Druckverwaltungsportal:

   ```
   localhost:631
   ```

   c. Wählen Sie den **zugeordneten Drucker** `CitrixUniversalPrinter:$ClientName:app/dsk$SESSION_ID` und **Drucker ändern**. Dieser Vorgang erfordert Administratorrechte.

   d. Behalten Sie die **cups-ctx**-Verbindung bei und klicken Sie dann auf **Weiter**, um den Druckertreiber zu ändern.

   e. Wählen Sie in den Feldern **Hersteller** und **Modell** einen anderen Druckertreiber als den Citrix UPD-Treiber aus. Wenn beispielsweise der virtuelle CUPS-PDF-Drucker installiert ist, wählen Sie den generischen CUPS-PDF-Druckertreiber aus. Speichern Sie die Änderung.

   f. Wenn dieser Vorgang erfolgreich ist, konfigurieren Sie den PPD-Dateipfad des Treibers in `.CtxlpProf` damit der zugeordnete Drucker den neu ausgewählten Treiber verwenden kann.

Bekannte Probleme

Die folgenden Probleme wurden beim Drucken auf dem Linux VDA festgestellt:

CTXPS-Treiber ist nicht mit einigen PLC-Druckern kompatibel

Wenn Sie auf eine Beschädigung der Druckausgabe stoßen, stellen Sie den Druckertreiber auf den nativen Treiber des Herstellers ein.

Langsame Druckleistung bei großen Dokumenten

Wenn Sie ein großes Dokument auf einem lokalen Client-Drucker drucken, wird das Dokument über die Serververbindung übertragen. Bei langsamen Verbindungen kann die Übertragung lange dauern.

Drucker- und Druckauftragsbenachrichtigungen aus anderen Sitzungen

Linux hat nicht dasselbe Sitzungskonzept wie das Windows-Betriebssystem. Daher erhalten alle Benutzer systemweite Benachrichtigungen. Sie können diese Benachrichtigungen deaktivieren, indem Sie die CUPS-Konfigurationsdatei ändern: **/etc/cups/cupsd.conf**.

Suchen Sie den aktuellen Richtliniennamen, der in der Datei konfiguriert ist:

`DefaultPolicy default`

Wenn der Richtlinienname *default* lautet, fügen Sie die folgenden Zeilen zum Standard-Richtlinien-XML-Block hinzu:

```
<Policy default>

     # Job/subscription privacy...

     JobPrivateAccess default

     JobPrivateValues default

     SubscriptionPrivateAccess default

     SubscriptionPrivateValues default
```

```
    … …

    <Limit Create-Printer-Subscription>

        Require user @OWNER

        Order deny,allow

    </Limit>

    <Limit All>

        Order deny,allow

    </Limit>

</Policy>
```

PDF-Druck

Mit einer Version der Citrix Workspace™ App, die PDF-Druck unterstützt, können Sie PDFs drucken, die innerhalb der Linux VDA-Sitzungen konvertiert wurden. Sitzungsdruckaufträge werden an den lokalen Computer gesendet, auf dem die Citrix Workspace App installiert ist. Auf

dem lokalen Computer können Sie PDFs mit Ihrem bevorzugten PDF-Viewer öffnen und auf Ihrem bevorzugten Drucker ausdrucken.

Der Linux VDA unterstützt den PDF-Druck auf den folgenden Versionen der Citrix Workspace App:

- Citrix Receiver für HTML5 Versionen 2.4 bis 2.6.9, Citrix Workspace App 1808 für HTML5 und höher
- Citrix Receiver für Chrome Versionen 2.4 bis 2.6.9, Citrix Workspace App 1808 für Chrome und höher
- Citrix Workspace App 1905 für Windows und höher

Konfiguration

Neben der Verwendung einer Version der Citrix Workspace App, die PDF-Druck unterstützt, legen Sie die folgenden Richtlinien in Citrix Studio fest:

- Legen Sie **Clientdruckerumleitung** auf **Zulässig** fest (**Zulässig** ist Standard)
- Legen Sie **PDF-Universaldrucker automatisch erstellen** auf **Aktiviert** fest (**Deaktiviert** ist Standard)
- Legen Sie **Clientdrucker automatisch erstellen** auf **Alle Clientdrucker automatisch erstellen** fest.

Wenn diese Richtlinien aktiviert sind, wird auf dem lokalen Computer eine Druckvorschau angezeigt, damit Sie einen Drucker auswählen können, wenn Sie in Ihrer gestarteten Sitzung auf **Drucken** klicken. Informationen zum Festlegen von Standarddruckern finden Sie in der Citrix Workspace App-Dokumentation.

Remote PC Access

Übersicht

Remote PC Access ist eine Erweiterung von Citrix Virtual Apps and Desktops. Es ermöglicht Unternehmen, Mitarbeitern den einfachen und sicheren Fernzugriff auf ihre physischen Büro-PCs zu ermöglichen. Wenn Benutzer auf ihre Büro-PCs zugreifen können, können sie auf alle Anwendungen, Daten und Ressourcen zugreifen, die sie für ihre Arbeit benötigen.

Remote PC Access verwendet dieselben Komponenten von Citrix Virtual Apps™ und Desktops, die virtuelle Desktops und Anwendungen bereitstellen. Die Anforderungen und der Prozess für die Bereitstellung und Konfiguration von Remote PC Access sind dieselben wie die Anforderungen und der Prozess für die Bereitstellung von Citrix Virtual Apps and Desktops. Diese Einheitlichkeit bietet

eine konsistente und einheitliche administrative Erfahrung. Benutzer erhalten die beste Benutzererfahrung, indem sie Citrix HDX verwenden, um ihre Remote-Büro-PC-Sitzungen bereitzustellen.

Weitere Informationen finden Sie unter Remote PC Access in der Dokumentation zu Citrix Virtual Apps and Desktops.

Überlegungen

Diese Überlegungen beziehen sich speziell auf den Linux VDA:

- Verwenden Sie auf physischen Maschinen den Linux VDA nur im Nicht-3D-Modus. Aufgrund von Einschränkungen des NVIDIA-Treibers kann der lokale Bildschirm des PCs nicht ausgeblendet werden, wenn der HDX™ 3D-Modus aktiviert ist. Das Anzeigen dieses Bildschirms stellt ein potenzielles Sicherheitsrisiko dar.
- Verwenden Sie Maschinenkataloge vom Typ Single-Session-OS für physische Linux-Maschinen.
- Die automatische Benutzerzuweisung ist für Linux-Maschinen nicht verfügbar. Bei der automatischen Benutzerzuweisung werden Benutzer ihren Maschinen automatisch zugewiesen, wenn sie sich lokal an den PCs anmelden. Diese Anmeldung erfolgt ohne Eingreifen des Administrators. Die Citrix Workspace™-App auf dem Client hilft Benutzern, innerhalb der Remote PC Access-Desktopsitzung auf die Anwendungen und Daten auf dem Büro-PC zuzugreifen.
- Wenn Benutzer bereits lokal an ihren PCs angemeldet sind, schlagen Versuche, die PCs von StoreFront™ aus zu starten, fehl.
- Energiesparoptionen sind für Linux-Maschinen nicht verfügbar.

Konfiguration

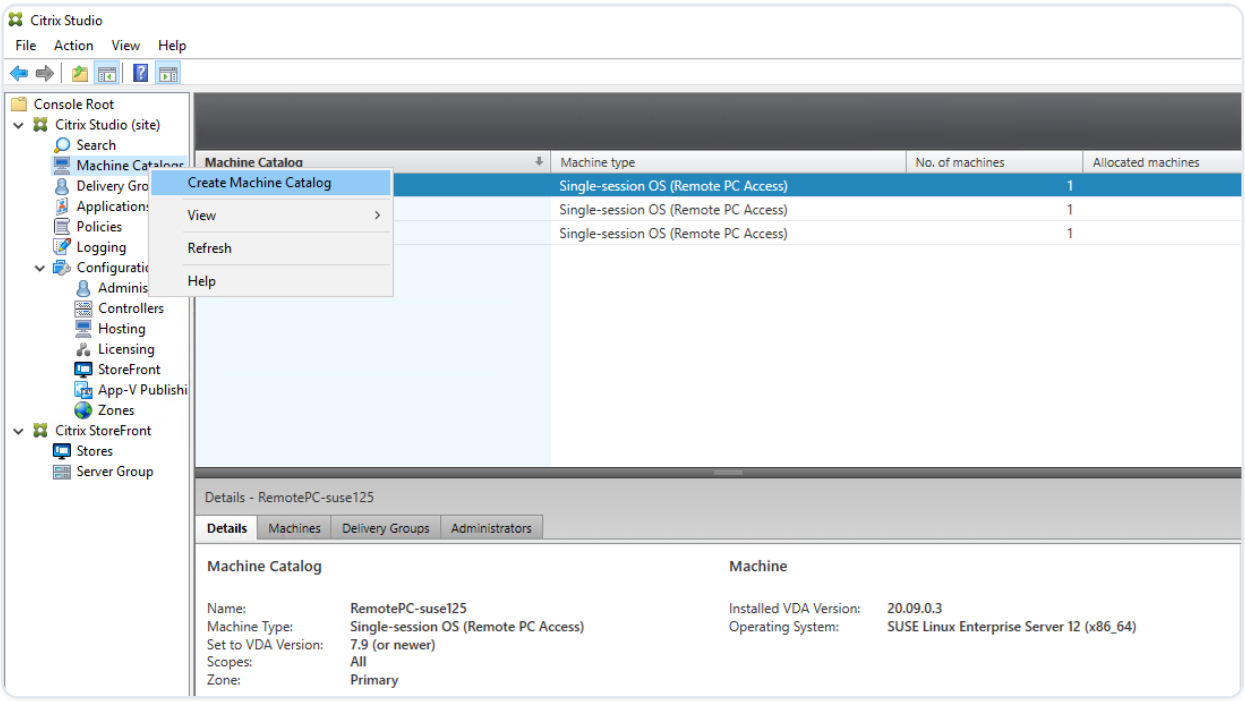
Um Linux-PC-Sitzungen bereitzustellen, installieren Sie den Linux VDA auf den Ziel-PCs, erstellen Sie einen Maschinenkatalog vom Typ **Remote PC Access** und erstellen Sie eine Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern. Der folgende Abschnitt beschreibt das Verfahren im Detail:

Schritt 1 – Installieren des Linux VDA auf den Ziel-PCs

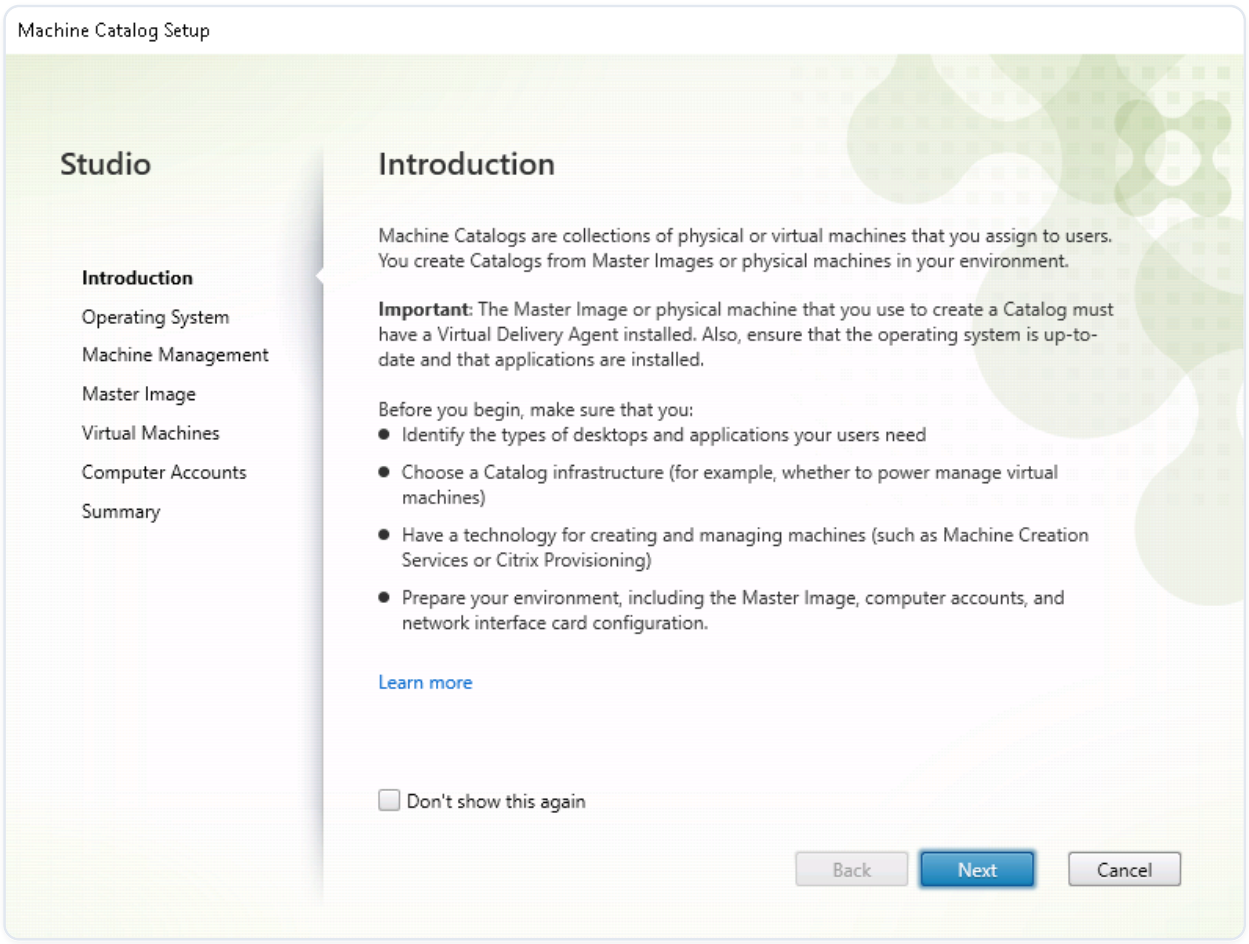
Wir empfehlen Ihnen, easy install zur Installation des Linux VDA zu verwenden. Legen Sie während der Installation den Wert der Variablen `CTX_XDL_VDI_MODE` auf `Y` fest.

Schritt 2 – Erstellen eines Maschinenkatalogs vom Typ Remote PC Access

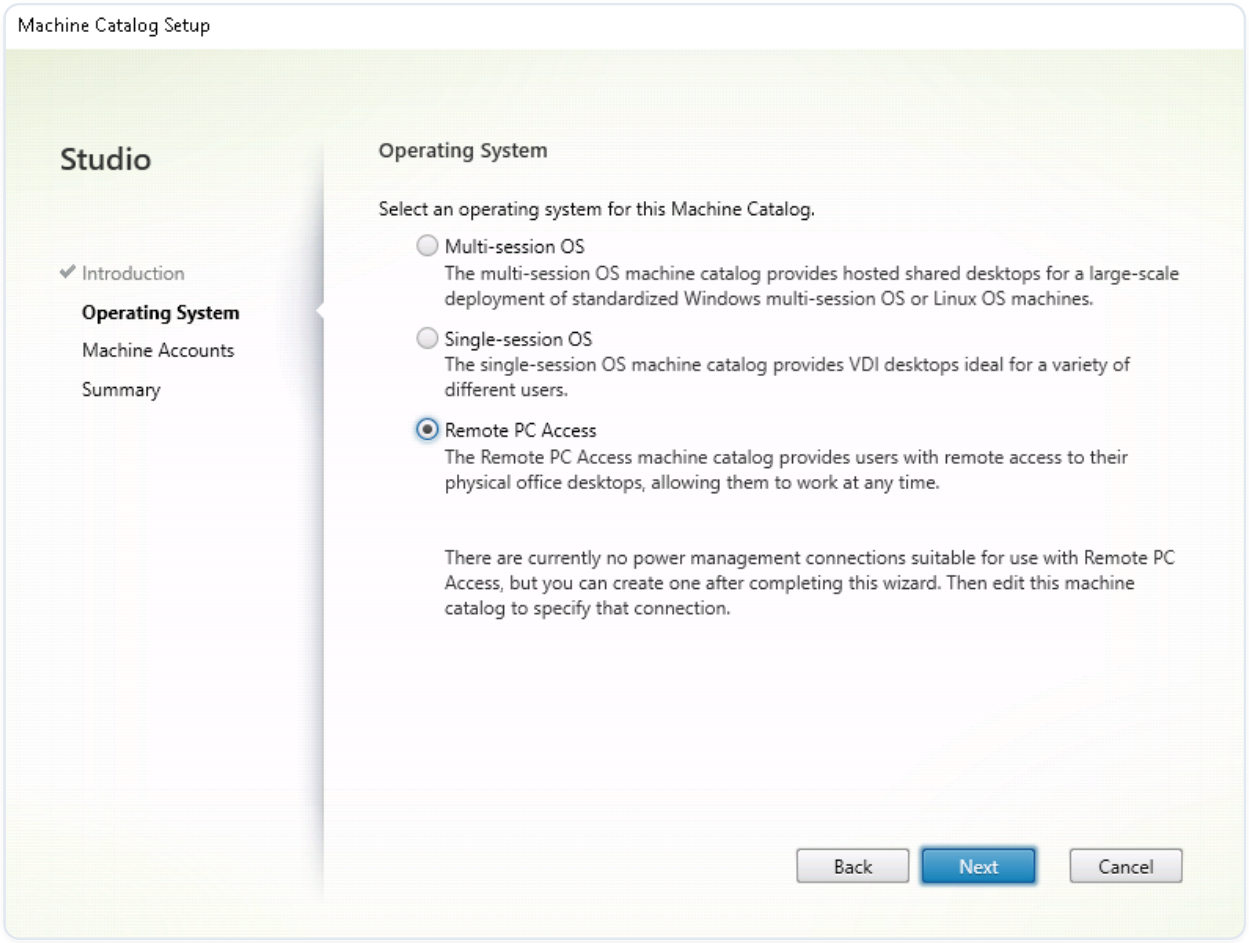
1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Maschinenkataloge** und wählen Sie im Kontextmenü **Maschinenkatalog erstellen**.



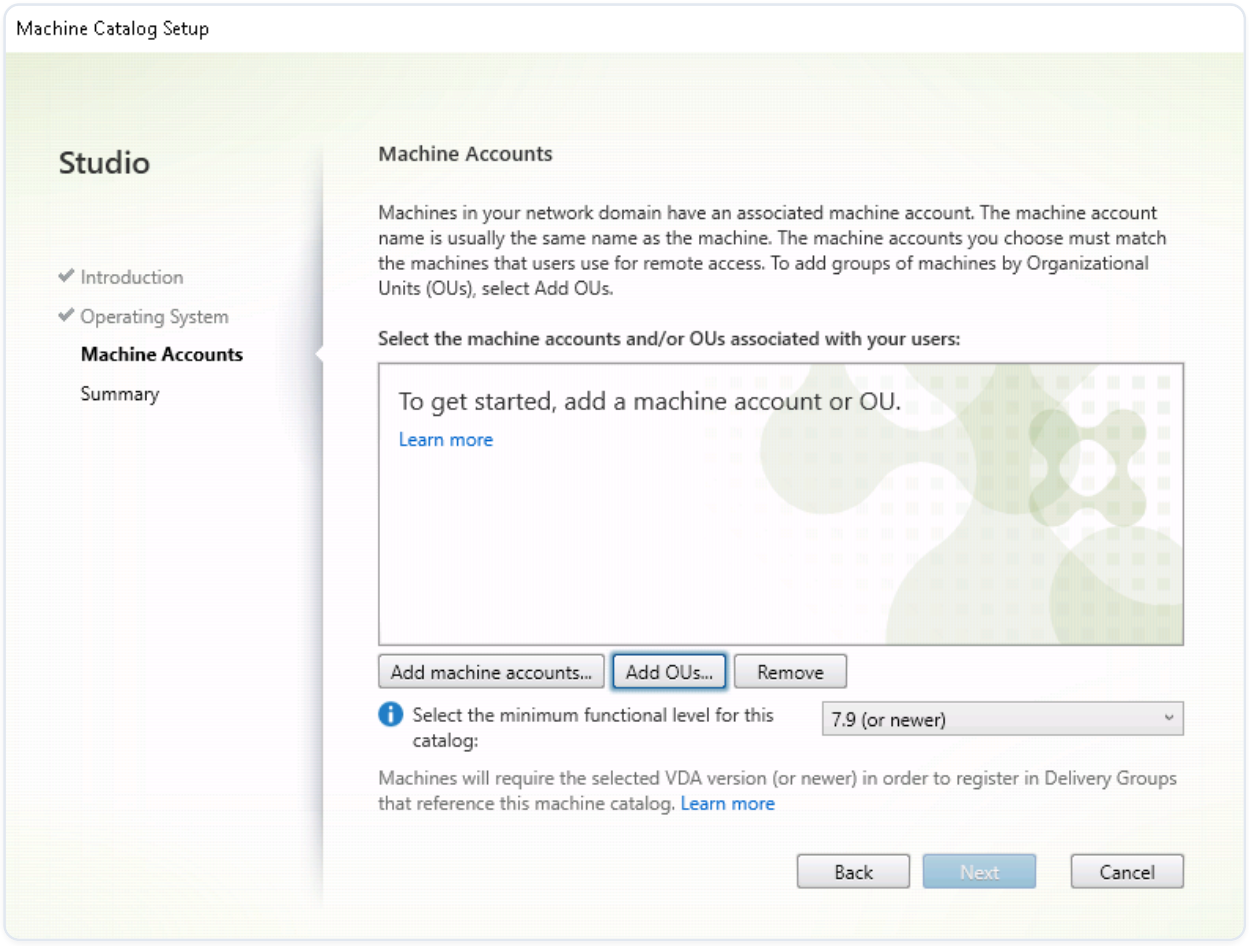
2. Klicken Sie auf der Seite **Einführung** auf **Weiter**.



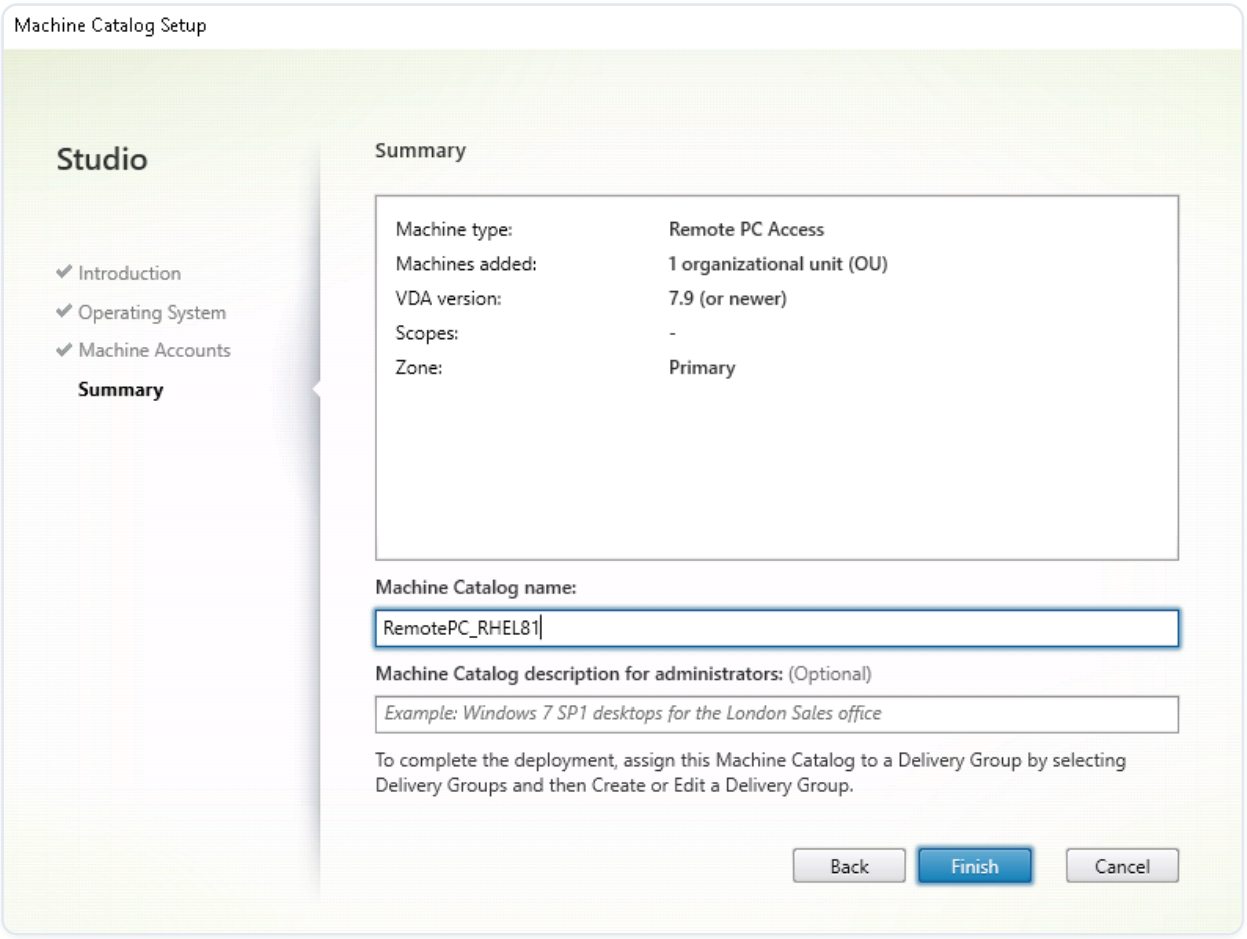
3. Wählen Sie auf der Seite **Betriebssystem** die Option **Remote PC Access**.



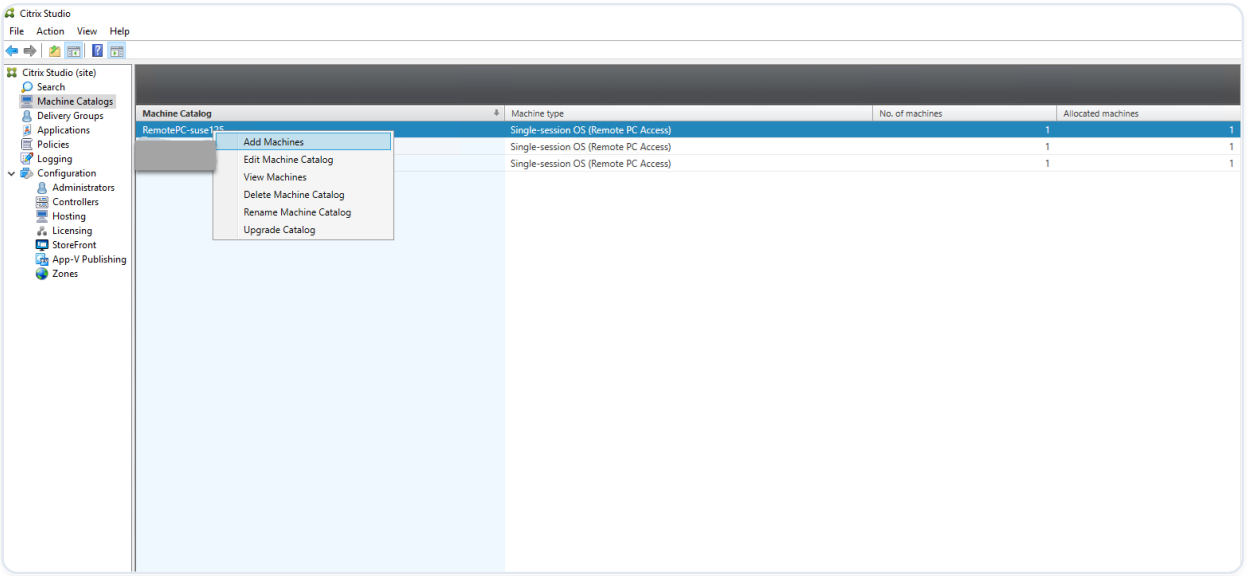
4. Klicken Sie auf **OUs hinzufügen**, um OUs auszuwählen, die die Ziel-PCs enthalten, oder klicken Sie auf **Maschinenkonten hinzufügen**, um einzelne Maschinen zum Maschinenkatalog hinzuzufügen.



5. Benennen Sie den Maschinenkatalog.

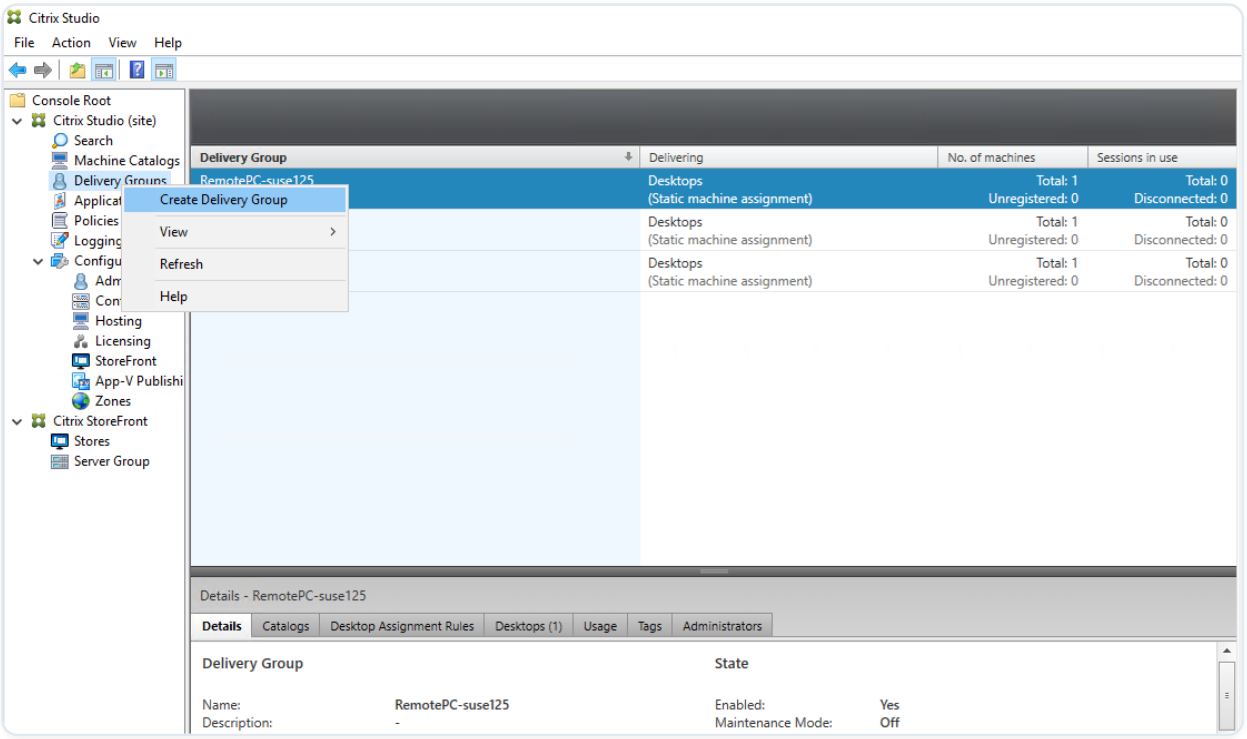


6. (Optional) Klicken Sie mit der rechten Maustaste auf den Maschinenkatalog, um relevante Vorgänge auszuführen.

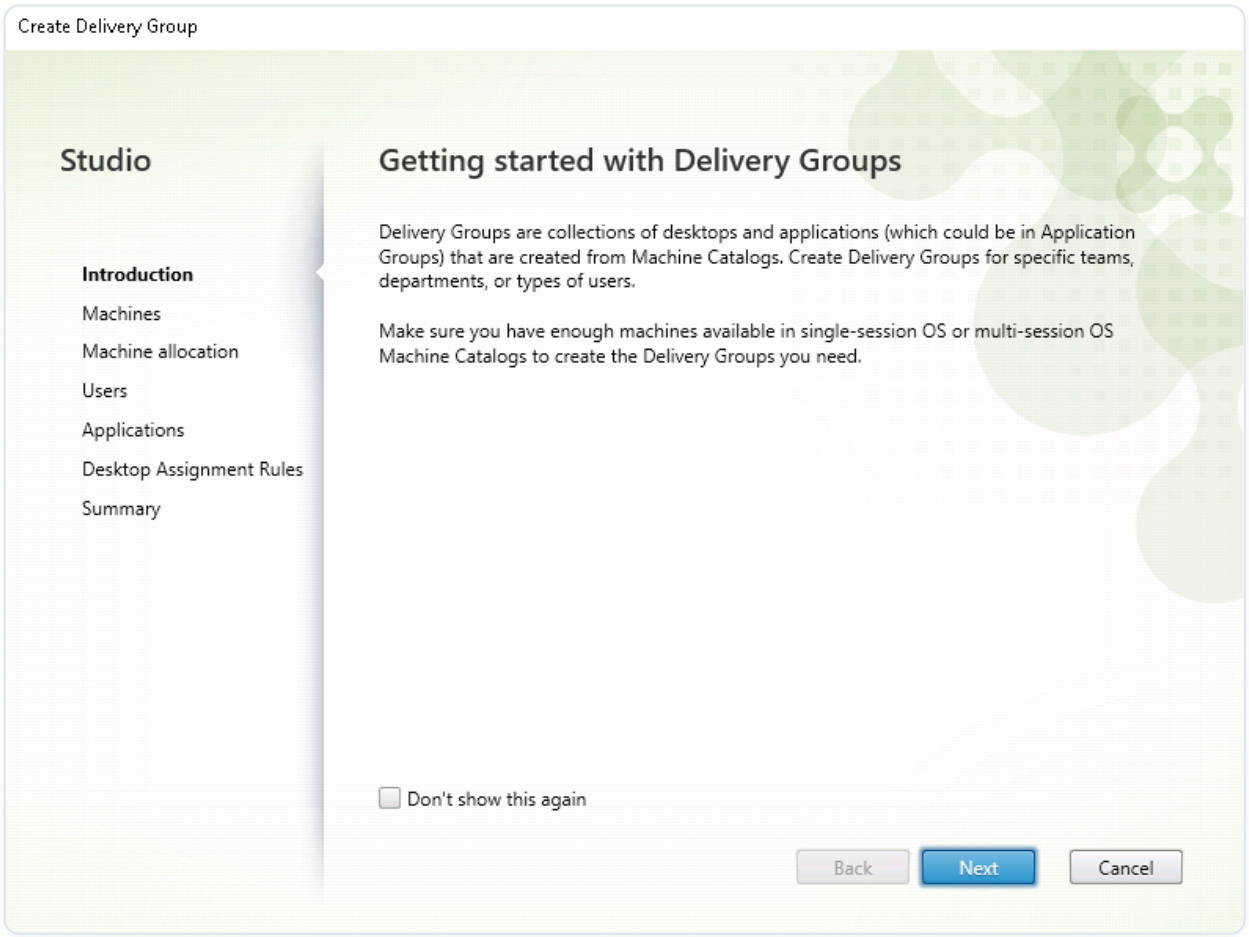


Schritt 3 – Erstellen einer Bereitstellungsgruppe, um die PCs im Maschinenkatalog für Benutzer verfügbar zu machen, die Zugriff anfordern

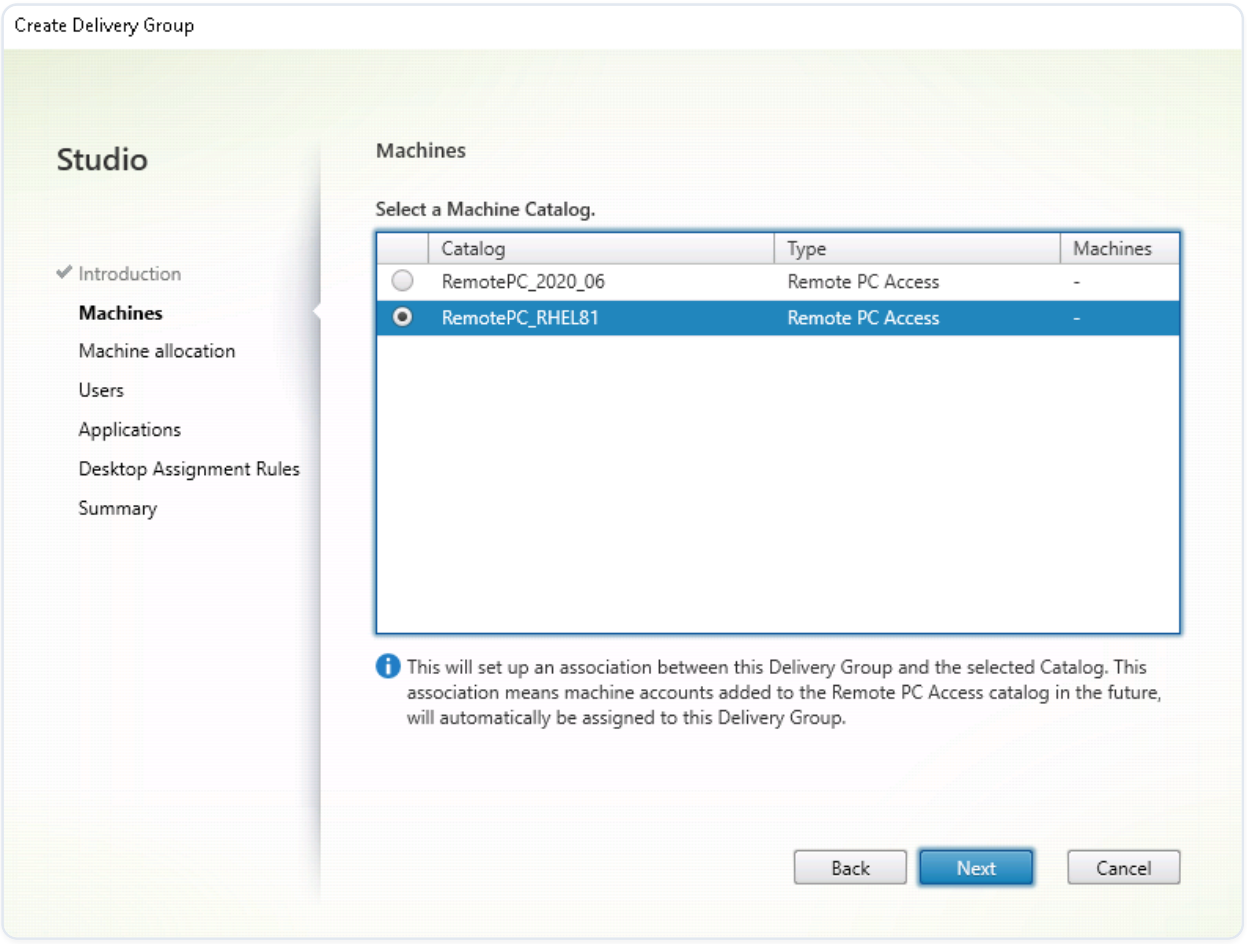
1. Klicken Sie in Citrix Studio mit der rechten Maustaste auf **Bereitstellungsgruppen**, und wählen Sie im Kontextmenü **Bereitstellungsgruppe erstellen**.



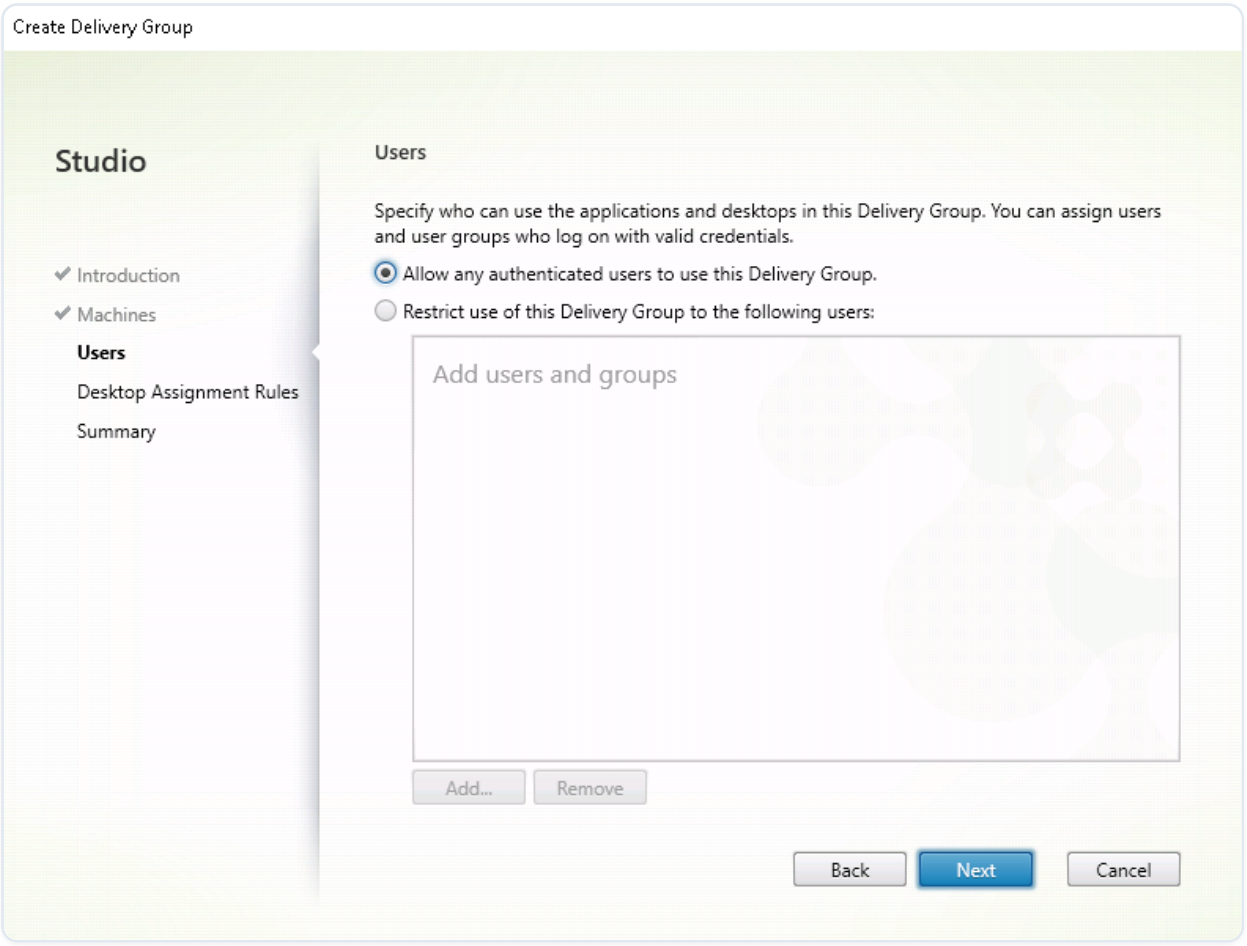
2. Klicken Sie auf der Seite **Erste Schritte mit Bereitstellungsgruppen** auf **Weiter**.



3. Wählen Sie den in Schritt 2 erstellten Maschinenkatalog aus, um ihn der Bereitstellungsgruppe zuzuordnen.



4. Fügen Sie Benutzer hinzu, die auf die PCs im Maschinenkatalog zugreifen können. Die hinzugefügten Benutzer können die Citrix Workspace-App auf einem Clientgerät verwenden, um remote auf die PCs zuzugreifen.



Wake on LAN

Remote PC Access unterstützt Wake on LAN, wodurch Benutzer physische PCs remote einschalten können. Diese Funktion ermöglicht es Benutzern, ihre Büro-PCs bei Nichtgebrauch ausgeschaltet zu lassen, um Energiekosten zu sparen. Sie ermöglicht auch den Fernzugriff, wenn ein Computer versehentlich ausgeschaltet wurde.

Mit der Wake-on-LAN-Funktion werden die Magic Pakete direkt vom auf dem PC ausgeführten VDA an das Subnetz gesendet, in dem sich der PC befindet, wenn dies vom Delivery Controller angewiesen wird. Dadurch kann die Funktion ohne Abhängigkeiten von zusätzlichen Infrastrukturkomponenten oder Drittanbieterlösungen für die Zustellung von Magic Paketen arbeiten.

Die Wake-on-LAN-Funktion unterscheidet sich von der älteren SCCM-basierten Wake-on-LAN-Funktion. Informationen zum SCCM-basierten Wake-on-LAN finden Sie unter Wake on LAN – SCCM-integriert.

Systemanforderungen

Die folgenden Systemanforderungen gelten für die Verwendung der Wake on LAN-Funktion:

- Steuerungsebene:
  - Citrix DaaS™ (ehemals Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops 2012 oder höher
- Physische PCs:
  - VDA-Version 2012 oder höher
  - Wake on LAN im BIOS und auf der NIC aktiviert

Wake-on-LAN konfigurieren

Derzeit wird die Konfiguration von integriertem Wake on LAN nur über PowerShell unterstützt.

So konfigurieren Sie Wake-on-LAN:

1. Erstellen Sie den Maschinenkatalog für Remote-PC-Zugriff, falls Sie noch keinen haben.
2. Erstellen Sie die Wake on LAN-Hostverbindung, falls Sie noch keine haben.

> **Hinweis:**
>
> Um die Wake on LAN-Funktion zu verwenden, erstellen Sie eine Hostverbindung, wenn Sie eine Hostverbindung vom Typ „Microsoft Configuration Manager Wake on LAN“ haben.

3. Rufen Sie den eindeutigen Bezeichner der Wake on LAN-Hostverbindung ab.
4. Ordnen Sie die Wake on LAN-Hostverbindung einem Maschinenkatalog zu.

   So erstellen Sie die Wake on LAN-Hostverbindung:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"
```

```
# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
             -Name $connectionName `
             -HypervisorAddress "N/A" `
             -UserName "woluser" `
             -Password "wolpwd" `
             -ConnectionType Custom `
             -PluginId VdaWOLMachineManagerFactory `
             -CustomProperties "<CustomProperties></CustomProperties>" `
             -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{
    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
}
```

Wenn die Hostverbindung bereit ist, führen Sie die folgenden Befehle aus, um den eindeutigen Bezeichner der Hostverbindung abzurufen:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

Nachdem Sie den eindeutigen Bezeichner der Verbindung abgerufen haben, führen Sie die folgenden Befehle aus, um die Verbindung dem Maschinenkatalog für Remote-PC-Zugriff zuzuordnen:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

5. Aktivieren Sie Wake on LAN im BIOS und auf der NIC jeder VM im Maschinenkatalog.

   Hinweis: Die Methode zum Aktivieren von Wake on LAN variiert je nach Maschinenkonfiguration.

   - So aktivieren Sie Wake on LAN im BIOS:

     a. Rufen Sie das BIOS auf und aktivieren Sie die Wake on LAN-Funktion.

        Die Methode für den Zugriff auf das BIOS hängt vom Hersteller Ihres Motherboards und dem vom Hersteller ausgewählten BIOS-Anbieter ab.

     b. Speichern Sie Ihre Einstellungen und starten Sie die Maschine neu.

   - So aktivieren Sie Wake on LAN auf der NIC:

     a. Führen Sie den Befehl `sudo ethtool <NIC>` aus, um zu überprüfen, ob Ihre NIC Magic Packets unterstützt.

        `<NIC>` ist der Gerätename Ihrer NIC, zum Beispiel `eth0`. Der Befehl `sudo ethtool <NIC>` liefert eine Ausgabe über die Funktionen Ihrer NIC:

        - Wenn die Ausgabe eine Zeile ähnlich `Supports Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` enthält, unterstützt Ihre NIC die Wake-on-LAN-Magic-Packet-Methode.
        - Wenn die Ausgabe eine Zeile ähnlich `Wake-on: <letters>` enthält, wobei `<letters>` den Buchstaben `g` enthält und nicht den Buchstaben `d` enthält, ist

die Wake-on-LAN-Magic-Packet-Methode aktiviert. Wenn `<letters>` jedoch den Buchstaben `d` enthält, weist dies darauf hin, dass die Wake-on-LAN-Funktion deaktiviert ist. Aktivieren Sie in diesem Fall Wake-on-LAN, indem Sie den Befehl `sudo ethtool -s <NIC> wol g` ausführen.

b. Bei den meisten Distributionen ist der Befehl `sudo ethtool -s <NIC> wol g` nach jedem Start erforderlich. Um diese Option dauerhaft festzulegen, führen Sie die folgenden Schritte basierend auf Ihren Distributionen aus:

Ubuntu:

Fügen Sie die Zeile `up ethtool -s <NIC> wol g` zur Schnittstellenkonfigurationsdatei `/etc/network/interfaces` hinzu. Zum Beispiel:

```
# ifupdown has been replaced by netplan(5) on this system. See

# /etc/netplan for current configuration.

# To re-enable ifupdown on this system, you can run:

# sudo apt install ifupdown

auto eth0

iface eth0 inet static

           address 10.0.0.1

           netmask 255.255.240.0

           gateway 10.0.0.1

           up ethtool -s eth0 wol g
```

RHEL/SUSE:

Fügen Sie den folgenden Parameter `ETHTOOL_OPTS` zur Schnittstellenkonfigurationsdatei `/etc/sysconfig/network-scripts/ifcfg-<NIC>` hinzu:

```
ETHTOOL_OPTS="-s ${DEVICE} wol g"
```

Designüberlegungen

Wenn Sie Wake on LAN mit Remote-PC-Zugriff verwenden möchten, beachten Sie Folgendes:

- Mehrere Maschinenkataloge können dieselbe Wake on LAN-Hostverbindung verwenden.
- Damit ein PC einen anderen PC aufwecken kann, müssen sich beide PCs im selben Subnetz befinden und dieselbe Wake on LAN-Hostverbindung verwenden. Es spielt keine Rolle, ob sich die PCs in denselben oder verschiedenen Maschinenkatalogen befinden.
- Hostverbindungen werden bestimmten Zonen zugewiesen. Wenn Ihre Bereitstellung mehr als eine Zone enthält, benötigen Sie in jeder Zone eine Wake on LAN-Hostverbindung. Dasselbe gilt für Maschinenkataloge.
- Magic Pakete werden über die globale Broadcast-Adresse 255.255.255.255 gesendet. Stellen Sie sicher, dass die Adresse nicht blockiert ist.
- Es muss mindestens ein PC im Subnetz eingeschaltet sein – für jede Wake-on-LAN-Verbindung –, um Maschinen in diesem Subnetz aufwecken zu können.

Betriebliche Überlegungen

Im Folgenden sind Überlegungen zur Verwendung der Wake-on-LAN-Funktion aufgeführt:

- Der VDA muss sich mindestens einmal registrieren, bevor der PC mithilfe der integrierten Wake-on-LAN-Funktion aufgeweckt werden kann.
- Wake on LAN kann nur zum Aufwecken von PCs verwendet werden. Es unterstützt keine anderen Energieaktionen, wie Neustart oder Herunterfahren.
- Nachdem die Wake-on-LAN-Verbindung erstellt wurde, ist sie in Studio sichtbar. Das Bearbeiten ihrer Eigenschaften innerhalb von Studio wird jedoch nicht unterstützt.
- Magic Pakete werden auf eine von zwei Arten gesendet:
  - Wenn ein Benutzer versucht, eine Sitzung auf seinem PC zu starten und der VDA nicht registriert ist
  - Wenn ein Administrator manuell einen Einschaltbefehl von Studio oder PowerShell aus sendet
- Da der Delivery Controller den Energiezustand eines PCs nicht kennt, zeigt Studio unter Energiezustand **Nicht unterstützt** an. Der Delivery Controller verwendet den VDA-Registrierungsstatus, um festzustellen, ob ein PC ein- oder ausgeschaltet ist.

Weitere Ressourcen

Im Folgenden finden Sie weitere Ressourcen für den Remote-PC-Zugriff:

- Leitfaden für das Lösungsdesign: Entscheidungen zum Design des Remote-PC-Zugriffs.
- Beispiele für Architekturen für den Remote-PC-Zugriff: Referenzarchitektur für die Citrix Remote-PC-Zugriffslösung.

Sitzung

Dieser Abschnitt enthält die folgenden Themen:

- Adaptiver Transport
- Anmeldung mit einem temporären Home-Verzeichnis
- Anwendungen veröffentlichen
- Sitzungszuverlässigkeit
- Rendezvous V1
- Rendezvous V2
- Benutzersitzungen mit TLS sichern
- Benutzersitzungen mit DTLS sichern

Adaptiver Transport

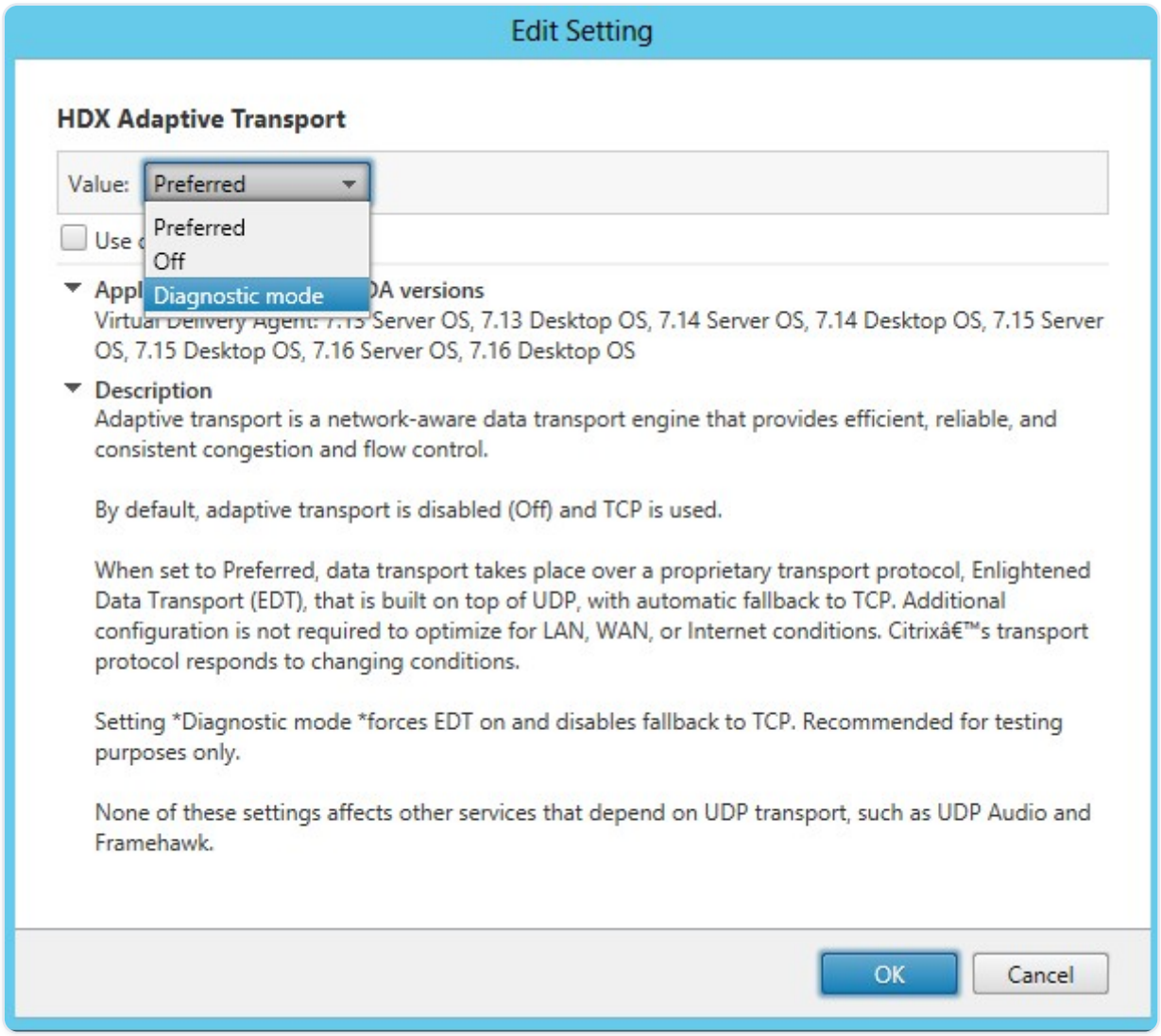
Der adaptive Transport ist ein Mechanismus in Citrix Virtual Apps and Desktops™, der Enlightened Data Transport (EDT) als Transportprotokoll für ICA-Verbindungen verwenden kann. Der adaptive Transport wechselt zu TCP, wenn EDT nicht verfügbar ist.

EDT ist ein Citrix-eigenes Transportprotokoll, das auf dem User Datagram Protocol (UDP) aufbaut. Es bietet eine überragende Benutzererfahrung bei anspruchsvollen Langstreckenverbindungen und bewahrt gleichzeitig die Skalierbarkeit des Servers. EDT verbessert den Datendurchsatz für alle ICA®-virtuellen Kanäle in unzuverlässigen Netzwerken und sorgt so für eine bessere und konsistentere Benutzererfahrung.

Weitere Informationen finden Sie unter Adaptiver Transport in der Citrix Virtual Apps and Desktops-Dokumentation.

Adaptiven Transport aktivieren oder deaktivieren

Der adaptive Transport ist standardmäßig aktiviert. Sie können die folgenden Optionen über die Richtlinieneinstellung **HDX™ Adaptive Transport** konfigurieren:



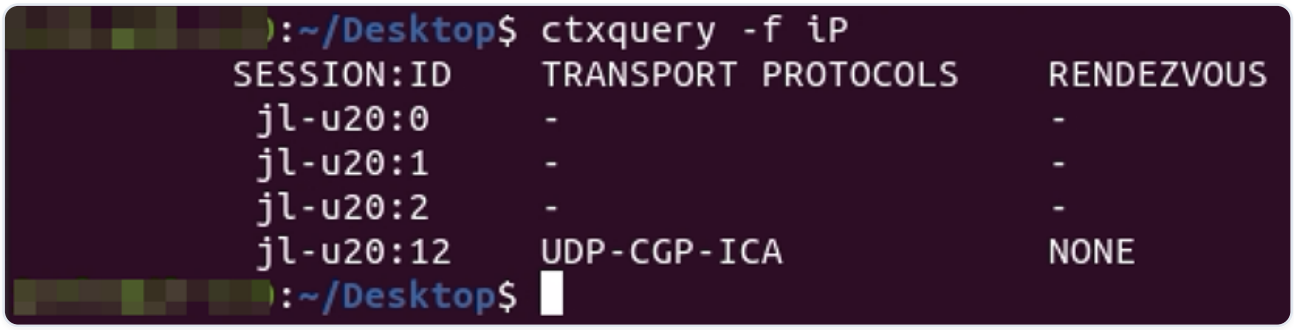
- **Bevorzugt**: Der adaptive Transport ist aktiviert und verwendet Enlightened Data Transport (EDT) als bevorzugtes Transportprotokoll, mit Fallback auf TCP.
- **Diagnosemodus**: Der adaptive Transport ist aktiviert und erzwingt die Verwendung von EDT. Das Fallback auf TCP ist deaktiviert. Diese Einstellung wird nur für Tests und die Fehlerbehebung empfohlen.
- **Aus**. Der adaptive Transport ist deaktiviert, und für den Transport wird nur TCP verwendet.

Prüfen, ob der adaptive Transport verwendet wird

Um zu prüfen, ob EDT als Transportprotokoll für die aktuelle Sitzung verwendet wird, führen Sie den folgenden Befehl aus.

```
/opt/Citrix/VDA/bin/ctxquery -f iP
```

Wenn EDT verwendet wird, umfassen die angezeigten Transportprotokolle UDP, zum Beispiel:



EDT-MTU-Ermittlung

Die MTU-Ermittlung ermöglicht es EDT, die maximale Übertragungseinheit (MTU) beim Aufbau einer Sitzung automatisch zu bestimmen. Dadurch wird eine EDT-Paketfragmentierung verhindert, die zu Leistungseinbußen oder zum Fehlschlagen des Sitzungsaufbaus führen könnte.

Systemanforderungen:

- Linux VDA Mindestversion 2012
- 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

Wenn Sie Clientplattformen oder -versionen verwenden, die diese Funktion nicht unterstützen, finden Sie unter CTX231821 Details zur Konfiguration einer benutzerdefinierten EDT-MTU, die für Ihre Umgebung geeignet ist.

EDT MTU-Erkennung auf dem VDA steuern

Die EDT MTU-Erkennung ist standardmäßig deaktiviert.

- Um die EDT MTU-Erkennung zu aktivieren, legen Sie den Registrierungsschlüssel `MtuDiscovery` mit dem folgenden Befehl fest, starten Sie den VDA neu und warten Sie, bis sich der VDA registriert hat:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\icawd" -t
"REG_DWORD" -v "MtuDiscovery" -d "0x00000001" --force
```

- Um die EDT MTU-Erkennung zu deaktivieren, löschen Sie den Registrierungswert `MtuDiscovery`.

> **Warnung:**
>
> Eine falsche Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen, die eine Neuinstallation des Betriebssystems erforderlich machen können. Citrix kann nicht garantieren, dass Probleme, die durch die falsche Verwendung des **Registrierungs-Editors** entstehen, behoben werden können. Verwenden Sie den **Registrierungs-Editor** auf eigenes Risiko. Sichern Sie die Registrierung unbedingt, bevor Sie sie bearbeiten.

EDT MTU-Erkennung auf dem Client steuern

Sie können die EDT MTU-Erkennung selektiv auf dem Client steuern, indem Sie den Parameter `MtuDiscovery` in der ICA-Datei hinzufügen. Um die Funktion zu deaktivieren, legen Sie Folgendes unter dem Abschnitt `Application` fest:

```
MtuDiscovery=Off
```

Um die Funktion wieder zu aktivieren, entfernen Sie den Parameter `MtuDiscovery` aus der ICA-Datei.

> **Wichtig:**
>
> Damit dieser ICA-Dateiparameter funktioniert, muss die EDT MTU-Erkennung auf dem VDA aktiviert sein. Wenn die EDT MTU-Erkennung auf dem VDA nicht aktiviert ist, hat der ICA-Dateiparameter keine Auswirkung.

Erweiterte EDT-Überlastungssteuerung

Ein Überlastkontrollalgorithmus wird eingeführt, um das EDT-Protokoll zu optimieren. Diese Implementierung ermöglicht es EDT, einen höheren Durchsatz zu erzielen und die Latenz für eine verbesserte Benutzererfahrung zu reduzieren. Diese Funktion ist standardmäßig deaktiviert. Um sie zu aktivieren, führen Sie den folgenden Befehl aus und starten Sie dann den `ctxhdx` Dienst neu:

```
/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
```

Benutzerdefinierte Hintergründe und Bannernachrichten auf Sitzungsanmeldebildschirmen

Benutzerdefinierten Hintergrund oder Bannernachricht zu Sitzungsanmeldebildschirmen hinzufügen

Tipp:

Um die Funktion unter SUSE 15.4 zu verwenden, installieren Sie `imlib2` von `<http://download.opensuse.org/distribution/leap/15.3/repo/oss/>`.

Sie können die folgenden Befehle verwenden, um einen benutzerdefinierten Hintergrund oder eine Bannernachricht zu Sitzungs**anmelde**bildschirmen hinzuzufügen. Um sowohl einen Hintergrund als auch eine Bannernachricht zu Sitzungs**anmelde**bildschirmen hinzuzufügen, können Sie die Bannernachricht in das Hintergrundbild einbetten. Nachdem Sie eine Sitzung geöffnet haben, wird zuerst die Bannernachrichtenseite angezeigt und dann erscheint der Authentifizierungsdialog.

Um den Titel einer benutzerdefinierten Bannernachricht festzulegen, führen Sie Folgendes aus:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
"LogonDisplayStringTitle" -d "<Banner message title>" --force
```

Die maximale Länge eines Bannernachrichtentitels beträgt 64 Byte.

Um den Haupttext einer benutzerdefinierten Bannernachricht festzulegen, führen Sie Folgendes aus:

```
/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
```

Die maximale Länge eines Bannernachrichtentextes beträgt 1.024 Byte.

Tipp:

Das Element `\n` erzeugt einen Zeilenumbruch. In diesem Beispiel sieht der Bannernachrichtenbildschirm wie folgt aus:

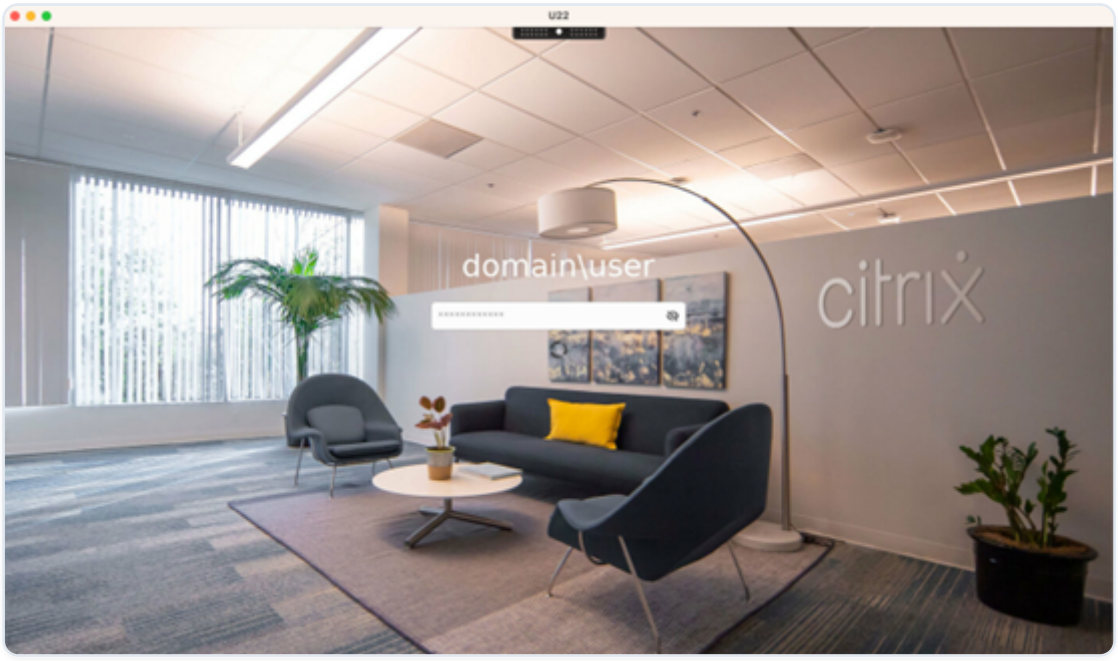


Um einen benutzerdefinierten Hintergrund zu Sitzungs**anmelde**bildschirmen hinzuzufügen, führen Sie Folgendes aus:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_SZ" -v
"BackgroundImagePath" -d "<path to the background image>" --force
```

Um den benutzerdefinierten Hintergrund zu sehen, müssen Sitzungsbenutzer Zugriff auf den Pfad des Hintergrundbilds haben.

Zum Beispiel:



Beispiel für Sitzungsanmeldebildschirme

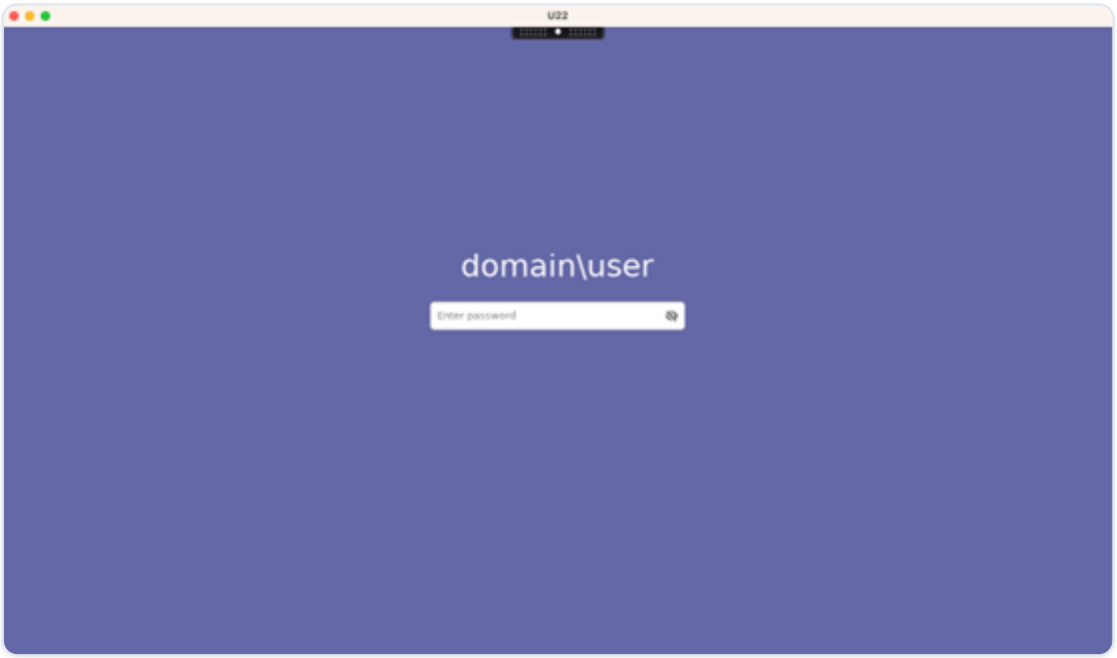
Im Folgenden finden Sie Beispiele für Sitzungsanmeldebildschirme in verschiedenen Szenarien:

- Sitzungs**anmeldung** in Single Sign-On (SSO)-Szenarien:

  Der **Anmelde**vorgang wird angezeigt.

- Sitzungs**anmeldung** in typischen Nicht-SSO-Szenarien:



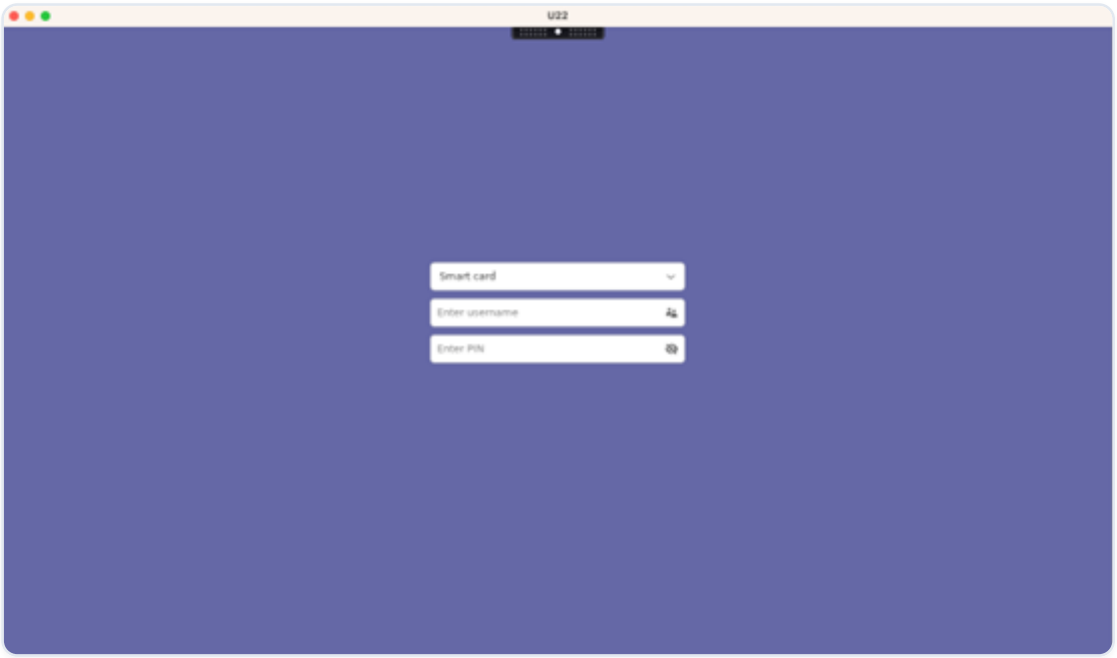
  - In Nicht-SSO-Szenarien ist ein Kennwort oder PIN-Code erforderlich.
  - Benutzer können die Sichtbarkeit von Kennwörtern und PIN-Codes umschalten, wodurch es für Benutzer einfacher wird, falsche Eingaben zu erkennen.

- Sitzungsanmeldung in Nicht-SSO-Szenarien, wenn sich Benutzer mit Anmeldeinformationen bei VDA-Sitzungen anmelden, die sich von den Anmeldeinformationen unterscheiden, die für die Anmeldung bei der Citrix Workspace™-App verwendet wurden:

  Benutzername und Kennwort für die Sitzungsanmeldung:



  Smartcard für die Sitzungsanmeldung:



Informationen zu den Kombinationen von Benutzerauthentifizierungsmethoden, die in Nicht-SSO-Szenarien unterstützt werden, finden Sie unter Nicht-SSO-Authentifizierung.

Benutzerdefinierte Desktop-Umgebungen für Sitzungsbenutzer

Sie können eine Desktop-Umgebung für Sitzungsbenutzer mithilfe der Variable **CTX_XDL_DESKTOP_ENVIRONMENT** angeben. Ab Version 2209 können Sitzungsbenutzer ihre eigenen Desktop-Umgebungen anpassen. Damit Sitzungsbenutzer diese Funktion nutzen können, müssen Sie Desktop-Umgebungen vorab auf dem VDA installieren.

Die folgende Tabelle zeigt eine Matrix der Linux-Distributionen und der Desktop-Umgebungen, die benutzerdefinierte Desktop-Umgebungen 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

Desktop-Wechselbefehle

> **Hinweis:**

> Sie können zwischen Desktop-Umgebungen sowohl über das Terminal als auch über die Systemleiste wechseln.

> Um im Terminal zu einer Ziel-Desktop-Umgebung zu wechseln, führen Sie den entsprechenden Befehl innerhalb der Sitzung aus:

WENN DIE ZIEL-DESKTOP-UMGEBUNG	FÜHREN SIE DEN 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 wird möglicherweise beim Start in KDE geladen. Als Workaround können Sie das Magnus-Paket entfernen, indem Sie `sudo apt remove magnus` ausführen.
- Um QT-Warnungen zu deaktivieren, die während des KDE-Starts auftreten, bearbeiten Sie `/usr/share/qt5/qtlogging.ini` als Root-Benutzer, indem Sie die folgenden Einträge hinzufügen:

```
qt.qpa.xcb.xcberror.error=false

qt.qpa.xcb.warning=false

qt.qpa.xcb.error=false
```

- Das Entsperren des Bildschirms kann bei KDE fehlschlagen. Als Workaround empfehlen wir Ihnen, die automatische Sperrfunktion Ihres Desktops zu deaktivieren.

Anmeldung mit einem temporären Home-Verzeichnis

Sie können ein temporäres Home-Verzeichnis für Fälle angeben, in denen der Bereitstellungspunkt auf dem Linux-VDA fehlschlägt. Wenn ein temporäres Home-Verzeichnis angegeben ist, wird bei der Sitzungsanmeldung eine Aufforderung angezeigt, wenn der Bereitstellungspunkt fehlschlägt. Benutzerdaten werden dann unter dem temporären Home-Verzeichnis gespeichert.

Die folgende Tabelle beschreibt Registrierungsschlüssel, die Ihnen bei den Einstellungen für Ihr Home-Verzeichnis helfen.

REGISTRIERUNGSSCHLÜSSEL	BESCHREIBUNG	BEFEHL
`LogNoHome`	Steuert, ob sich Benutzer ohne Home-Verzeichnis bei Sitzungen anmelden können. Der Standardwert ist 1, was „Ja“ bedeutet. Wenn der Wert auf 0 gesetzt ist, sind Sitzungsanmeldungen ohne Home-Verzeichnis deaktiviert.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "LogNoHome" -d "0x00000001" --force`
`HomeMountPoint`	Legt einen lokalen Bereitstellungspunkt auf dem Linux-VDA fest. Wenn beispielsweise `/mnt/home` der Bereitstellungspunkt ist, ist das Home-Verzeichnis eines Benutzers `/mnt/home/domain/<user_name>`. Stellen Sie sicher, dass der Bereitstellungspunkt mit dem Home-Verzeichnis des Benutzers in Ihrer Umgebung übereinstimmt. Diese Einstellung wird 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 Home-Verzeichnisse als Bereitstellungspunkt auf dem Linux-VDA festgelegt werden sollen. Wenn Sie benutzerspezifische Home-Verzeichnisse als Bereitstellungspunkt festlegen möchten, setzen Sie den Wert auf **1**. Der Standardwert ist **0**.	`ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "CheckUserHomeMountPoint" -d "0x00000001" --force`
`TempHomeDirectoryPath`	Legt ein temporäres Home-Verzeichnis auf dem Linux-VDA fest, falls der Bereitstellungspunkt fehlschlägt. Der Standardwert ist `/tmp`. Die Einstellung für das temporäre Home-Verzeichnis wird nur wirksam, wenn der durch `HomeMountPoint` und `CheckUserHomeMountPoint` bestimmte Bereitstellungspunkt nicht verfügbar ist. Ein temporäres Home-Verzeichnis 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 die Anzahl der Prüfungen fest, ob die Bereitstellung erfolgreich ist, und zwar einmal pro Sekunde. Der Standardwert ist 5.	`ctxreg create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "CheckMountPointRetryTime" -d "0x000000010" --force`

REGISTRIERUNGSSCHLÜSSEL	BESCHREIBUNG	BEFEHL
`RemoveHomeOnLogoff`	Steuert, ob temporäre Home-Verzeichnisse bei der Benutzerabmeldung entfernt werden sollen. 1 bedeutet Ja. 0 bedeutet Nein.	`create -k "HKLM\System\CurrentControlSet\Control\Citrix" -t "REG_DWORD" -v "RemoveHomeOnLogoff" -d "0x00000000" --force`

Anwendungen veröffentlichen

Mit Linux VDA Version 7.13 hat Citrix die Funktion für nahtlose Anwendungen zu allen unterstützten Linux-Plattformen hinzugefügt. Für die Verwendung dieser Funktion sind keine speziellen Installationsverfahren erforderlich.

> **Tipp:**

> Mit Linux VDA Version 1.4 hat Citrix die Unterstützung für nicht-nahtlose veröffentlichte Anwendungen und Sitzungsfreigabe hinzugefügt.

Anwendungen mit Citrix Studio veröffentlichen

Sie können auf einem Linux-VDA installierte Anwendungen veröffentlichen, wenn Sie eine Bereitstellungsgruppe erstellen oder Anwendungen zu einer vorhandenen Bereitstellungsgruppe hinzufügen. Der Prozess ähnelt dem Veröffentlichen von Anwendungen, die auf einem Windows-VDA installiert sind. Weitere Informationen finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation (basierend auf der verwendeten Version von Citrix Virtual Apps and Desktops).

> **Hinweis:**

> - Stellen Sie beim Konfigurieren von Bereitstellungsgruppen sicher, dass der Bereitstellungstyp auf **Desktops und Anwendungen** oder **Anwendungen** festgelegt ist.
> - Das Veröffentlichen von Anwendungen wird ab Linux VDA Version 1.4 unterstützt. Der Linux VDA unterstützt jedoch nicht die Bereitstellung von Desktops und Anwendungen auf derselben Maschine. Um dieses Problem zu beheben, empfehlen wir Ihnen, separate

Bereitstellungsgruppen für die Bereitstellung von Anwendungen und Desktops zu erstellen.

- Um nahtlose Anwendungen zu verwenden, deaktivieren Sie den nahtlosen Modus in StoreFront nicht. Der nahtlose Modus ist standardmäßig aktiviert. Wenn Sie ihn bereits durch Setzen von „TWIMode=Off“ deaktiviert haben, entfernen Sie diese Einstellung, anstatt sie in „TWIMode=On“ zu ändern. Andernfalls können Sie einen veröffentlichten Desktop möglicherweise nicht starten.

Einschränkung

Der Linux VDA unterstützt nicht den Start mehrerer gleichzeitiger Instanzen derselben Anwendung durch einen einzelnen Benutzer.

In einer App-Sitzung funktionieren nur anwendungsspezifische Verknüpfungen wie erwartet.

Bekannte Probleme

Die folgenden bekannten Probleme treten beim Veröffentlichen von Anwendungen auf:

- Nicht-rechteckige Fenster werden nicht unterstützt. Die Ecken eines Fensters zeigen möglicherweise den serverseitigen Hintergrund an.
- Die Vorschau des Fensterinhalts einer veröffentlichten Anwendung wird nicht unterstützt.
- Wenn Sie mehrere LibreOffice-Anwendungen ausführen, wird in Citrix Studio nur die zuerst gestartete angezeigt, da diese Anwendungen den Prozess gemeinsam nutzen.
- Veröffentlichte Qt5-basierte Anwendungen wie „Dolphin“ zeigen möglicherweise keine Symbole an. Informationen zur Behebung des Problems finden Sie im Artikel unter `<https://wiki.archlinux.org/title/Qt>`.

Rendezvous V1

When using the Citrix Gateway service, the Rendezvous protocol allows traffic to bypass the Citrix Cloud™ Connectors and connect directly and securely with the Citrix Cloud control plane.

There are two types of traffic to consider: 1) control traffic for VDA registration and session brokering; 2) HDX™ session traffic.

Rendezvous V1 ermöglicht es dem HDX-Sitzungsdatenverkehr, Cloud Connectors zu umgehen, erfordert aber weiterhin, dass Cloud Connectors den gesamten Steuerdatenverkehr für die VDA-Registrierung und Sitzungsbrokerung als Proxy weiterleiten.

Anforderungen

- Zugriff auf die Umgebung mit Citrix Workspace™ und dem Citrix Gateway-Dienst.
- Steuerungsebene: Citrix DaaS (ehemals Citrix Virtual Apps and Desktops™ Service).
- Linux VDA Version 2112 oder höher.
  - Version 2112 ist die Mindestanforderung für nicht-transparente HTTP-Proxys.
  - Version 2204 ist die Mindestanforderung für transparente und SOCKS5-Proxys.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix-Richtlinie. Weitere Informationen finden Sie unter Richtlinieneinstellung für das Rendezvous-Protokoll.
- Die VDAs müssen Zugriff auf `https://*.nssvc.net` haben, einschließlich aller Subdomains. Wenn Sie nicht alle Subdomains auf diese Weise auf die Whitelist setzen können, verwenden Sie stattdessen `https://*.c.nssvc.net` und `https://*.g.nssvc.net`. Weitere Informationen finden Sie im Abschnitt Anforderungen an die Internetkonnektivität der Citrix Cloud-Dokumentation (unter Virtual Apps and Desktop Service) und im Knowledge Center-Artikel CTX270584.
- Cloud Connectors müssen die FQDNs der VDAs beim Brokering einer Sitzung abrufen. Um dieses Ziel zu erreichen, aktivieren Sie die DNS-Auflösung für die Site: Führen Sie mit dem Citrix DaaS Remote PowerShell SDK den Befehl `Set-BrokerSite -DnsResolutionEnabled $true` aus. Weitere Informationen zum Citrix DaaS Remote PowerShell SDK finden Sie unter SDKs und APIs.

Proxykonfiguration

Der VDA unterstützt den Aufbau von Rendezvous-Verbindungen über HTTP- und SOCKS5-Proxys.

Proxy-Überlegungen

Beachten Sie bei der Verwendung von Proxys mit Rendezvous Folgendes:

- Nicht-transparente HTTP-Proxys und SOCKS5-Proxys werden unterstützt.
- Paketentschlüsselung und -inspektion werden nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der ICA®-Datenverkehr zwischen dem VDA und dem Gateway Service nicht abgefangen, entschlüsselt oder inspiziert wird. Andernfalls wird die Verbindung unterbrochen.
- HTTP-Proxys unterstützen die maschinenbasierte Authentifizierung mithilfe der Authentifizierungsprotokolle Negotiate und Kerberos. Wenn Sie eine Verbindung zum

Proxyserver herstellen, wählt das Negotiate-Authentifizierungsschema automatisch das Kerberos-Protokoll aus. Kerberos ist das einzige Schema, das der Linux VDA unterstützt.

> **Hinweis:**
>
> Um Kerberos zu verwenden, müssen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver erstellen und ihn dem Active Directory-Konto des Proxys zuordnen. Der VDA generiert den SPN im Format `HTTP/<proxyURL>` beim Herstellen einer Sitzung, wobei die Proxy-URL aus der Richtlinieneinstellung **Rendezvous-Proxy** abgerufen wird. Wenn Sie keinen SPN erstellen, schlägt die Authentifizierung fehl.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Wenn Sie einen SOCKS5-Proxy verwenden, müssen Sie eine Ausnahme konfigurieren, damit der für Gateway Service-Adressen (in den Anforderungen angegeben) bestimmte Datenverkehr die Authentifizierung umgehen kann.
- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Für einen HTTP-Proxy verwenden Sie TCP als Transportprotokoll für ICA.

Transparenter Proxy

Transparenter HTTP-Proxy wird für Rendezvous unterstützt. Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist keine zusätzliche Konfiguration auf dem VDA erforderlich.

Nicht-transparenter Proxy

Wenn Sie einen nicht-transparenten Proxy in Ihrem Netzwerk verwenden, konfigurieren Sie die Einstellung Rendezvous-Proxykonfiguration. Wenn die Einstellung aktiviert ist, geben Sie die HTTP- oder SOCKS5-Proxyadresse an, damit der VDA weiß, welchen Proxy er verwenden soll. Beispiel:

- Proxy-Adresse: `http://<URL or IP>:<port>` oder `socks5://<URL or IP>:<port>`

Rendezvous-Validierung

Wenn Sie alle Anforderungen erfüllen, führen Sie die folgenden Schritte aus, um zu überprüfen, ob Rendezvous verwendet wird:

1. Starten Sie ein Terminal auf dem VDA.
2. Führen Sie `/opt/Citrix/VDA/bin/ctxquery -f iP` aus.
3. Die TRANSPORT PROTOCOLS geben den Verbindungstyp an:

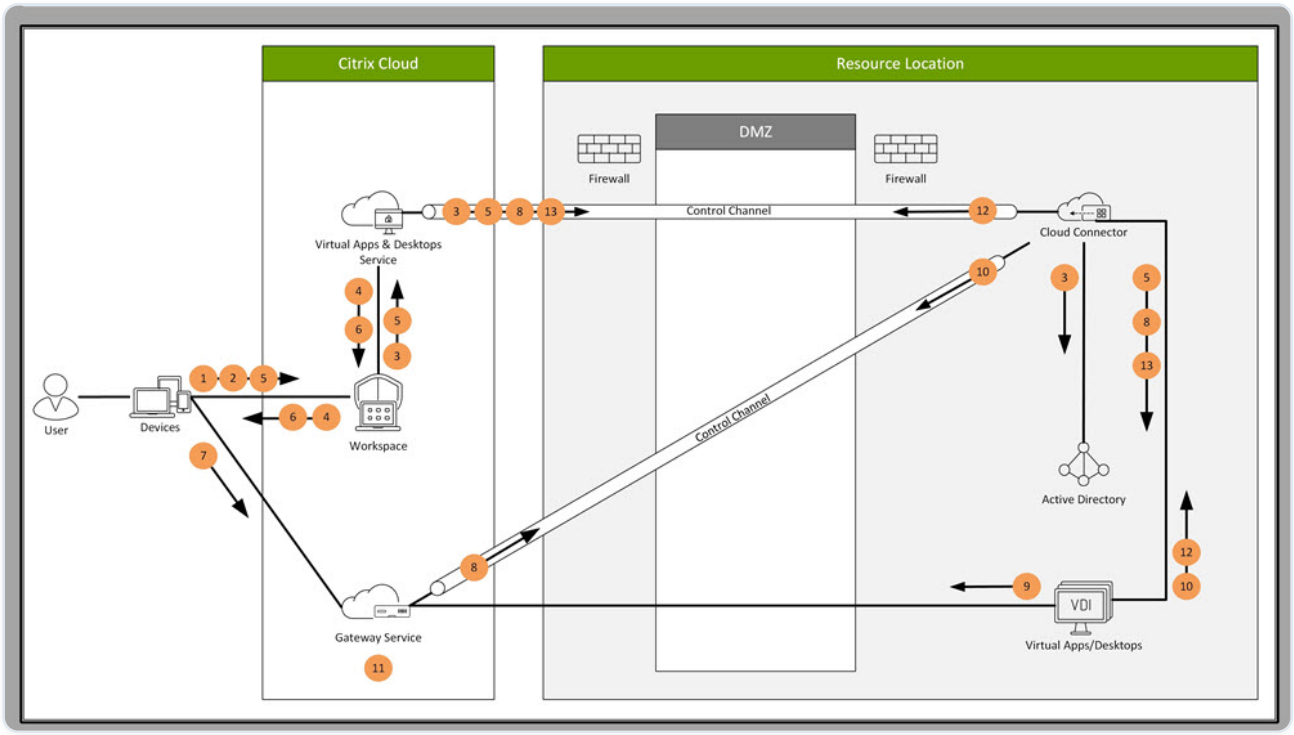
- TCP Rendezvous: TCP - TLS - CGP - ICA
- EDT Rendezvous: UDP - DTLS - CGP - ICA
- Proxy über Cloud Connector: TCP – PROXY – SSL – CGP – ICA oder UDP – PROXY – DTLS – CGP – ICA

Tipp:

Wenn der VDA den Citrix Gateway-Dienst bei aktiviertem Rendezvous nicht direkt erreichen kann, fällt der VDA auf die Proxy-Verbindung der HDX-Sitzung über den Cloud Connector zurück.

Funktionsweise von Rendezvous

Dieses Diagramm bietet einen Überblick über den Rendezvous-Verbindungsfluss.



Befolgen Sie die Schritte, um den Ablauf zu verstehen.

1. Navigieren Sie zu Citrix Workspace.
2. Geben Sie die Anmeldeinformationen in Citrix Workspace ein.
3. Bei Verwendung von lokalem Active Directory authentifiziert Citrix DaaS™ die Anmeldeinformationen mit Active Directory über den Cloud Connector-Kanal.
4. Citrix Workspace zeigt die aufgelisteten Ressourcen von Citrix DaaS an.

5. Wählen Sie Ressourcen aus Citrix Workspace aus. Citrix DaaS sendet eine Nachricht an den VDA, um sich auf eine eingehende Sitzung vorzubereiten.
6. Citrix Workspace sendet eine ICA-Datei an den Endpunkt, die ein von Citrix Cloud generiertes STA-Ticket enthält.
7. Der Endpunkt stellt eine Verbindung zum Citrix Gateway-Dienst her, stellt das Ticket zur Verbindung mit dem VDA bereit, und Citrix Cloud validiert das Ticket.
8. Der Citrix Gateway-Dienst sendet Verbindungsinformationen an den Cloud Connector. Der Cloud Connector ermittelt, ob es sich um eine Rendezvous-Verbindung handelt, und sendet die Informationen an den VDA.
9. Der VDA stellt eine direkte Verbindung zum Citrix Gateway-Dienst her.
10. Wenn eine direkte Verbindung zwischen dem VDA und dem Citrix Gateway Service nicht möglich ist, leitet der VDA seine Verbindung über den Cloud Connector weiter.
11. Der Citrix Gateway Service stellt eine Verbindung zwischen dem Endpunktgerät und dem 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

Bei Verwendung des Citrix Gateway service ermöglicht das Rendezvous-Protokoll dem Datenverkehr, die Citrix Cloud™ Connectors zu umgehen und sich direkt und sicher mit der Citrix Cloud-Steuerungsebene zu verbinden.

Es sind zwei Arten von Datenverkehr zu berücksichtigen: 1) Steuerdatenverkehr für die VDA-Registrierung und das Session Brokering; 2) HDX™-Sitzungsdatenverkehr.

Rendezvous V1 ermöglicht es dem HDX-Sitzungsdatenverkehr, Cloud Connectors zu umgehen, erfordert aber weiterhin, dass Cloud Connectors den gesamten Steuerdatenverkehr für die VDA-Registrierung und das Session Brokering proxen.

Standard-AD-domänenverbundene Maschinen und nicht-domänenverbundene Maschinen werden für die Verwendung von Rendezvous V2 mit Single-Session- und Multi-Session-Linux-VDAs unterstützt. Bei nicht-domänenverbundenen Maschinen ermöglicht Rendezvous V2, dass sowohl HDX-Datenverkehr als auch Steuerdatenverkehr die Cloud Connectors umgehen.

Anforderungen

Die Anforderungen für die Verwendung von Rendezvous V2 sind:

- Zugriff auf die Umgebung über Citrix Workspace™ und Citrix Gateway service.
- Steuerungsebene: Citrix DaaS (ehemals Citrix Virtual Apps and Desktops™ service).
- VDA-Version 2201 oder höher.
  - Version 2204 ist die Mindestanforderung für HTTP- und SOCKS5-Proxys.
- Aktivieren Sie das Rendezvous-Protokoll in der Citrix-Richtlinie. Weitere Informationen finden Sie unter Rendezvous-Protokoll-Richtlinieneinstellung.
- Die VDAs müssen Zugriff auf `https://*.nssvc.net` haben, einschließlich aller Subdomains. Wenn Sie nicht alle Subdomains auf diese Weise auf die Whitelist setzen können, verwenden Sie stattdessen `https://*.c.nssvc.net` und `https://*.g.nssvc.net`. Weitere Informationen finden Sie im Abschnitt Anforderungen an die Internetkonnektivität der Citrix Cloud-Dokumentation (unter Virtual Apps and Desktop service) und im Knowledge Center-Artikel CTX270584.
- Die VDAs müssen in der Lage sein, sich mit den zuvor genannten Adressen zu verbinden:
  - Auf TCP 443, für TCP Rendezvous.
  - Auf UDP 443, für EDT Rendezvous.

Proxykonfiguration

Der VDA unterstützt die Verbindung über Proxys sowohl für den Steuerungsdatenverkehr als auch für den HDX-Sitzungsdatenverkehr bei Verwendung von Rendezvous. Die Anforderungen und Überlegungen für beide Arten von Datenverkehr sind unterschiedlich, daher sollten Sie diese sorgfältig prüfen.

Überlegungen zum Proxy für Steuerungsdatenverkehr

- Es werden nur HTTP-Proxys unterstützt.
- Paketentschlüsselung und -inspektion werden nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der Steuerungsdatenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder inspiziert wird. Andernfalls schlägt die Verbindung fehl.
- Proxy-Authentifizierung wird nicht unterstützt.
- Um einen Proxy für den Steuerungsdatenverkehr zu konfigurieren, bearbeiten Sie die Registrierung wie folgt:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\Software\Citrix\VirtualDesktopAgent" -t "REG_SZ" -v
"ProxySettings" -d "http://<URL or IP>:<port>" --force
```

Überlegungen zum Proxy für 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, verwenden Sie die Richtlinieneinstellung Rendezvous-Proxykonfiguration.
- Paketentschlüsselung und -inspektion werden nicht unterstützt. Konfigurieren Sie eine Ausnahme, damit der HDX-Datenverkehr zwischen dem VDA und der Citrix Cloud-Steuerungsebene nicht abgefangen, entschlüsselt oder inspiziert wird. Andernfalls schlägt die Verbindung fehl.
- HTTP-Proxys unterstützen die maschinenbasierte Authentifizierung mithilfe der Authentifizierungsprotokolle Negotiate und Kerberos. Wenn Sie eine Verbindung zum Proxyserver herstellen, wählt das Negotiate-Authentifizierungsschema automatisch das Kerberos-Protokoll aus. Kerberos ist das einzige Schema, das der Linux VDA unterstützt.

  Hinweis:

  Um Kerberos zu verwenden, müssen Sie den Dienstprinzipalnamen (SPN) für den Proxyserver erstellen und ihn dem Active Directory-Konto des Proxys zuordnen. Der VDA generiert den SPN im Format `HTTP/<proxyURL>`, wenn eine Sitzung hergestellt wird, wobei die Proxy-URL aus der Richtlinieneinstellung **Rendezvous-Proxy** abgerufen wird. Wenn Sie keinen SPN erstellen, schlägt die Authentifizierung fehl.

- Die Authentifizierung mit einem SOCKS5-Proxy wird derzeit nicht unterstützt. Wenn Sie einen SOCKS5-Proxy verwenden, müssen Sie eine Ausnahme konfigurieren, damit der für Gateway-Dienstadressen (in den Anforderungen angegeben) bestimmte Datenverkehr die Authentifizierung umgehen kann.
- Nur SOCKS5-Proxys unterstützen den Datentransport über EDT. Für einen HTTP-Proxy verwenden Sie TCP als Transportprotokoll für ICA.

Transparenter Proxy

Transparenter HTTP-Proxy wird für Rendezvous unterstützt. Wenn Sie einen transparenten Proxy in Ihrem Netzwerk verwenden, ist keine zusätzliche Konfiguration auf dem VDA erforderlich.

So konfigurieren Sie Rendezvous V2

Im Folgenden sind die Schritte zur Konfiguration von Rendezvous in Ihrer Umgebung aufgeführt:

1. Stellen Sie sicher, dass alle Anforderungen erfüllt sind.
2. Nach der Installation des VDA 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 "0x00000001" --force
   ```

3. Starten Sie die VDA-Maschine neu.
4. Erstellen Sie eine Citrix-Richtlinie oder bearbeiten Sie eine vorhandene:
   - Setzen Sie die Einstellung für das Rendezvous-Protokoll auf **Zulässig**.
   - Stellen Sie sicher, dass die Citrix-Richtlinienfilter ordnungsgemäß eingestellt sind. Die Richtlinie gilt für die Maschinen, auf denen Rendezvous aktiviert werden muss.
   - Stellen Sie sicher, dass die Citrix-Richtlinie die richtige Priorität hat, damit sie keine andere überschreibt.

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 den Verbindungstyp 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

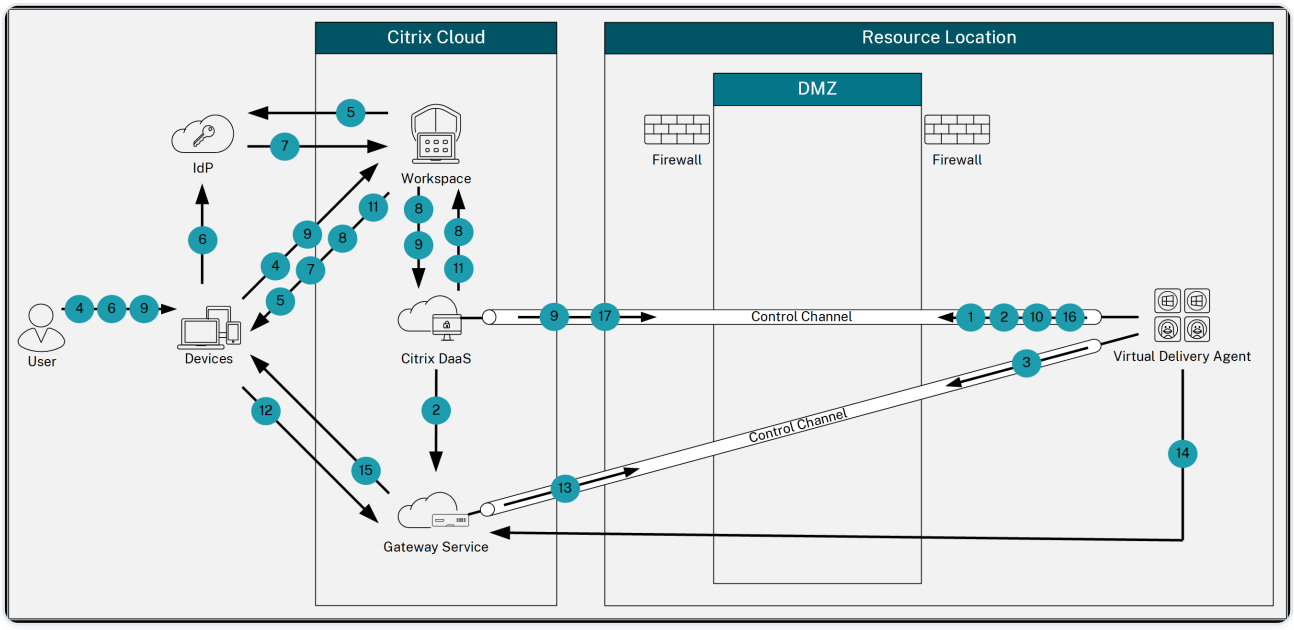
Wenn Rendezvous V2 verwendet wird, wird die Protokollversion 2.0 angezeigt.

> **Tipp:**

> Wenn der VDA den Citrix Gateway-Dienst bei aktiviertem Rendezvous nicht direkt erreichen kann, fällt der VDA auf die Proxy-Verbindung der HDX-Sitzung über den Cloud Connector zurück.

Rendezvous-Datenfluss

Das folgende Diagramm veranschaulicht die Abfolge der Schritte zum Rendezvous-Datenfluss.



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 ein dediziertes Token.
3. Der VDA stellt eine persistente Steuerverbindung mit dem 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 seine Anmeldeinformationen ein.
7. Nach erfolgreicher Validierung der Benutzeranmeldeinformationen wird der Benutzer zu Workspace weitergeleitet.
8. Workspace zählt die Ressourcen für den Benutzer und zeigt sie an.
9. Der Benutzer wählt einen Desktop oder eine Anwendung aus 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 antwortet 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 zum Gateway Service her und stellt das Startticket zur Authentifizierung und Identifizierung der zu verbindenden Ressource bereit.
13. Der Gateway Service sendet die Verbindungsinformationen an den VDA.
14. Der VDA stellt eine direkte Verbindung für die Sitzung mit dem Gateway Service her.
15. Der Gateway Service schließt die Verbindung zwischen dem Endpunkt und dem VDA ab.
16. Der VDA überprüft die Lizenzierung für die Sitzung.
17. Citrix DaaS sendet die anwendbaren Richtlinien an den VDA.

Benutzersitzungen mit DTLS sichern

Die DTLS-Verschlüsselung ist ab Release 7.18 eine vollständig unterstützte Funktion. Standardmäßig ist diese Funktion auf dem Linux VDA aktiviert. Weitere Informationen finden Sie unter Transport Layer Security.

DTLS-Verschlüsselung aktivieren

Überprüfen, ob adaptiver Transport aktiviert ist

Stellen Sie in Citrix Studio sicher, dass die Richtlinie **HDX™ Adaptive Transport** auf **Bevorzugt** oder **Diagnosemodus** eingestellt ist.

SSL-Verschlüsselung auf dem Linux VDA aktivieren

Verwenden Sie auf dem Linux VDA das Tool **enable_vdassl.sh** unter **/opt/Citrix/VDA/sbin**, um die SSL-Verschlüsselung zu aktivieren (oder zu deaktivieren). Informationen zu den im Tool verfügbaren Optionen erhalten Sie, indem Sie den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh –h` ausführen.

> **Hinweis:**
>
> Der Linux VDA unterstützt sowohl DTLS 1.0 als auch DTLS 1.2 und verwendet standardmäßig DTLS 1.2. Überprüfen Sie, welche DTLS-Version in Ihrer Citrix Workspace-App verwendet wird. Stellen Sie sicher, dass dieselbe DTLS-Version sowohl auf dem Linux VDA als auch in 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** mit dem Tool **enable_vdassl.sh**.

Sichere Benutzersitzungen mit TLS

Ab Version 7.16 unterstützt der Linux VDA die TLS-Verschlüsselung für sichere Benutzersitzungen. Die TLS-Verschlüsselung ist standardmäßig deaktiviert.

TLS-Verschlüsselung aktivieren

Um die TLS-Verschlüsselung für sichere Benutzersitzungen zu aktivieren, installieren Sie Zertifikate und aktivieren Sie die TLS-Verschlüsselung sowohl auf dem Linux VDA als auch auf dem Delivery Controller™ (dem Controller).

Zertifikate auf dem Linux VDA installieren

Besorgen Sie sich Serverzertifikate im PEM-Format und Stammzertifikate im CRT-Format. Ein Serverzertifikat enthält die folgenden Abschnitte:

- Zertifikat
- Unverschlüsselter privater Schlüssel
- Zwischenzertifikate (optional)

Ein Beispiel für ein Serverzertifikat:

Ein Beispiel für ein Serverzertifikat(/en-us/linux-virtual-delivery-agent/2308/media/example-server-certificate.png)

TLS-Verschlüsselung aktivieren

TLS-VERSCHLÜSSELUNG AUF DEM LINUX VDA AKTIVIEREN

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 im Skript verfügbaren Optionen erhalten Sie, indem Sie den Befehl `/opt/Citrix/VDA/sbin/enable_vdassl.sh -help` ausführen.

Das Skript zum Aktivieren von SSL(/en-us/linux-virtual-delivery-agent/2308/media/script-for-enabling-ssl.png)

Tipp: Ein Serverzertifikat muss auf jedem Linux VDA-Server installiert werden, und Stammzertifikate müssen auf jedem Linux VDA-Server und -Client installiert werden.

TLS-VERSCHLÜSSELUNG AUF DEM CONTROLLER AKTIVIEREN

> **Hinweis:**

> Sie können die TLS-Verschlüsselung nur für ganze Bereitstellungsgruppen aktivieren. Sie können die TLS-Verschlüsselung nicht für bestimmte Anwendungen aktivieren.

> Führen Sie in einem PowerShell-Fenster auf dem Controller die folgenden Befehle nacheinander aus, um die TLS-Verschlüsselung für die Zielbereitstellungsgruppe zu aktivieren.

1. `Add-PSSnapin citrix.*`.
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule –HdxSslEnabled $true`

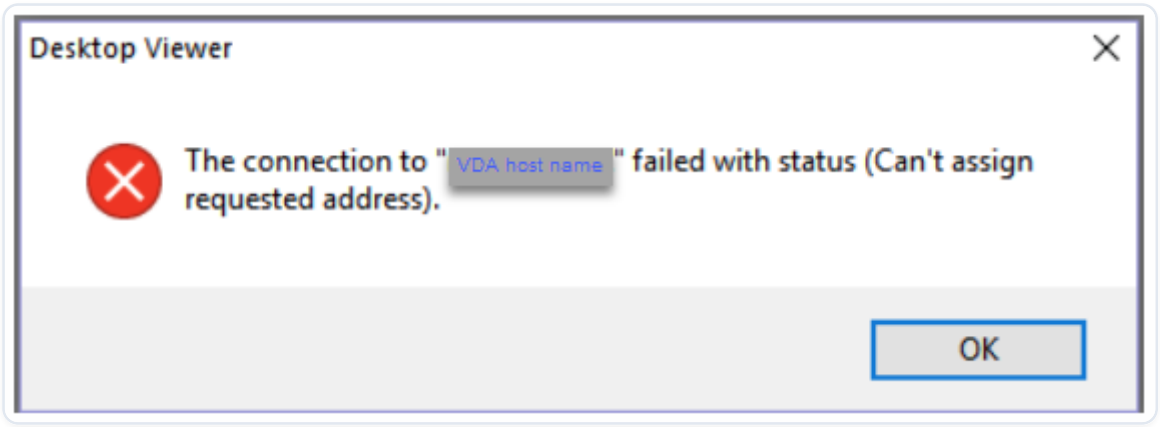
> **Hinweis:**
>
> Um sicherzustellen, dass nur VDA-FQDNs in einer ICA®-Sitzungsdatei enthalten sind, können Sie auch den Befehl `Set-BrokerSite –DnsResolutionEnabled $true` ausführen. Der Befehl aktiviert die DNS-Auflösung. Wenn Sie die DNS-Auflösung deaktivieren, legt eine ICA-Sitzungsdatei VDA-IP-Adressen offen und stellt FQDNs nur für TLS-bezogene Elemente wie `SSLProxyHost` und `UDPDTLSPort` bereit.

> Um die TLS-Verschlüsselung auf dem Controller zu deaktivieren, führen Sie die folgenden Befehle nacheinander aus:

1. `Add-PSSnapin citrix.*`.
2. `Get-BrokerAccessPolicyRule –DesktopGroupName 'GROUPNAME' | Set-BrokerAccessPolicyRule –HdxSslEnabled $false`
3. `Set-BrokerSite –DnsResolutionEnabled $false`

Problembehandlung

Der folgende Fehler „Can't assign requested address“ (Angeforderte Adresse kann nicht zugewiesen werden) kann in der Citrix Workspace™-App für Windows auftreten, wenn Sie versuchen, auf eine veröffentlichte Desktopsitzung zuzugreifen:



Fügen Sie als Problemumgehung einen Eintrag zur Datei **hosts** hinzu, der dem folgenden ähnelt:

```
<IP address of the Linux VDA>      <FQDN of the Linux VDA>
```

Auf Windows-Computern befindet sich die Datei **hosts** normalerweise unter `C:\Windows\System32\drivers\etc\hosts`.

Sitzungszuverlässigkeit

Citrix® führt die Sitzungszuverlässigkeitsfunktion für alle unterstützten Linux-Plattformen ein. Die Sitzungszuverlässigkeit ist standardmäßig aktiviert.

Die Sitzungszuverlässigkeit stellt ICA-Sitzungen bei Netzwerkunterbrechungen nahtlos wieder her. Weitere Informationen zur Sitzungszuverlässigkeit finden Sie unter Automatische Clientwiederverbindung und Sitzungszuverlässigkeit.

Hinweis: Daten, die über eine Sitzungszuverlässigkeitsverbindung übertragen werden, liegen standardmäßig im Klartext vor. Aus Sicherheitsgründen empfehlen wir, die TLS-Verschlüsselung zu aktivieren. Weitere Informationen zur TLS-Verschlüsselung finden Sie unter Sichern von Benutzersitzungen mit TLS.

Konfiguration

Richtlinieneinstellungen in Citrix Studio

Sie können die folgenden Richtlinien für die Sitzungszuverlässigkeit in Citrix Studio festlegen:

- Sitzungszuverlässigkeitsverbindungen
- Timeout für Sitzungszuverlässigkeit
- Portnummer für Sitzungszuverlässigkeit
- Transparenzgrad der Wiederverbindungs-Benutzeroberfläche

Weitere Informationen finden Sie unter Richtlinieneinstellungen für die Sitzungszuverlässigkeit und Richtlinieneinstellungen für die automatische Clientwiederverbindung.

Hinweis: Nachdem Sie die Richtlinie **Sitzungszuverlässigkeitsverbindungen** oder **Sitzungszuverlässigkeits-Portnummer** festgelegt haben, starten Sie den VDA-Dienst und den HDX™-Dienst in dieser Reihenfolge neu, damit Ihre Einstellungen wirksam werden.

Einstellungen auf dem Linux VDA

- **TCP-Listener für Sitzungszuverlässigkeit aktivieren/deaktivieren**

Standardmäßig ist der TCP-Listener für die Sitzungszuverlässigkeit aktiviert und lauscht auf Port 2598. Um den Listener zu deaktivieren, führen Sie den folgenden Befehl aus.

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cg
p"   -v  "fEnableWinStation" -d "0x00000000"
```

Hinweis: Starten Sie den HDX-Dienst neu, damit Ihre Einstellungen wirksam werden. Das Deaktivieren des TCP-Listeners deaktiviert die Sitzungszuverlässigkeit nicht. Die Sitzungszuverlässigkeit ist weiterhin über andere Listener (z. B. SSL) verfügbar, wenn die Funktion über die Richtlinie **Sitzungszuverlässigkeitsverbindungen** aktiviert ist.

- **Sitzungszuverlässigkeits-Portnummer**

Sie können die Portnummer für die Sitzungszuverlässigkeit auch mit dem folgenden Befehl festlegen (Portnummer 2599 als Beispiel).

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations\cg
p"   -v  "PortNumber" -d  "2599"
```

Hinweis: Starten Sie den HDX-Dienst neu, damit Ihre Einstellung wirksam wird. Wenn die Portnummer über die Richtlinieneinstellung in **Citrix Studio** festgelegt wurde, wird Ihre Einstellung auf dem Linux VDA ignoriert. Stellen Sie sicher, dass die Firewall auf dem VDA so konfiguriert ist, dass sie den Netzwerkverkehr über den festgelegten Port nicht verbietet.

- **Server-zu-Client-Keep-Alive-Intervall**

Keep-Alive-Nachrichten werden zwischen dem Linux VDA und dem Client gesendet, wenn in einer Sitzung keine Aktivität stattfindet (z. B. keine Mausbewegung oder Bildschirmaktualisierung). Die Keep-Alive-Nachrichten werden verwendet, um festzustellen, ob der Client noch reagiert. Wenn

keine Antwort vom Client erfolgt, wird die Sitzung angehalten, bis der Client die Verbindung wiederherstellt. Diese Einstellung gibt die Anzahl der Sekunden zwischen aufeinanderfolgenden Keep-Alive-Nachrichten an. Standardmäßig ist diese Einstellung nicht konfiguriert. Um sie zu konfigurieren, führen Sie den folgenden Befehl aus (10 Sekunden als Beispiel).

```
/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**

Diese Einstellung gibt die Anzahl der Sekunden zwischen aufeinanderfolgenden Keep-Alive-Nachrichten an, die vom ICA®-Client an den Linux VDA gesendet werden. Standardmäßig ist diese Einstellung nicht konfiguriert. Um sie zu konfigurieren, führen Sie den folgenden Befehl aus (10 Sekunden als Beispiel).

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XTEConfig"  -t "REG_DWORD"  -v
"CgpClientToServerKeepAlive"  -d  "10"  --force
```

Problembehandlung

Sitzungen können nach dem Aktivieren der Sitzungszuverlässigkeit über die Richtlinieneinstellung nicht gestartet werden.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der VDA-Dienst und der HDX-Dienst in dieser Reihenfolge neu gestartet werden, nachdem Sie die Sitzungszuverlässigkeit über die Richtlinieneinstellung in Citrix Studio aktiviert haben.
2. Führen Sie auf dem VDA den folgenden Befehl aus, um zu überprüfen, ob der TCP-Listener für die Sitzungszuverlässigkeit ausgeführt wird (Port 2598 als Beispiel).

   ```
   netstat -an | grep 2598
   ```

   Wenn kein TCP-Listener am Sitzungszuverlässigkeitsport vorhanden ist, aktivieren Sie den Listener, indem Sie den folgenden Befehl ausführen.

```
/opt/Citrix/VDA/bin/ctxreg update -k
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\WinStations
\cgp"   -v  "fEnableWinStation" -d "0x00000001"
```

Sitzungsaufzeichnung (Vorschau)

Sie können auf einem Linux-VDA gehostete Sitzungen aufzeichnen und wiedergeben.

Hinweis:

Diese Funktion ist eine Vorschauversion. Vorschaufunktionen sind möglicherweise nicht vollständig lokalisiert und werden für die Verwendung in Nicht-Produktionsumgebungen empfohlen. Probleme, die bei Vorschaufunktionen auftreten, werden vom technischen Support von Citrix nicht unterstützt.

Sitzungsaufzeichnung aktivieren oder deaktivieren

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
```

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\SmartAuditor" -t "REG_DWORD"
-v "SmAudAllowed" -d "0x00000000" --force
```

Hinweis:

Nachdem Sie die Sitzungsaufzeichnung auf einem Linux-VDA aktiviert haben, werden Benutzer beim Anmelden bei ihren Sitzungen darüber informiert, dass ihre Sitzungen aufgezeichnet werden.

Dateigröße für Aufzeichnungen angeben

Wenn Aufzeichnungen größer werden, dauert das Herunterladen der Aufzeichnungsdateien länger und die Reaktion ist langsamer, wenn Sie den Suchregler zur Navigation während der Wiedergabe verwenden. Um die Dateigröße zu steuern, geben Sie eine Schwellenwertbegrenzung für eine Datei an. Wenn die Aufzeichnung diese Grenze erreicht, wird die aktuelle Datei geschlossen und eine zusätzliche Datei erstellt, um die Aufzeichnung fortzusetzen. Diese Aktion wird als Rollover bezeichnet.

Mit den folgenden Befehlen können Sie zwei Schwellenwerte für einen Rollover festlegen:

```
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
```

- **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 geöffnet. Standardmäßig erfolgt der Rollover, wenn die Sitzung 12 Stunden lang aufgezeichnet wurde. Unterstützte Werte: 1–24.

Rollover treten ein, wenn die erste der beiden oben genannten Bedingungen erfüllt ist. Sie geben beispielsweise 17 MB für die Dateigröße und 6 Stunden für die Dauer an. Wenn Ihre Aufzeichnung in 3 Stunden 17 MB erreicht, schließt die Sitzungsaufzeichnung die Datei und öffnet eine neue.

Um die Erstellung vieler kleiner Dateien zu verhindern, erfolgt der Rollover erst nach mindestens einer Stunde, unabhängig vom für die Dateigröße angegebenen Wert. Eine Ausnahme von dieser Regel ist, wenn die Dateigröße 300 MB überschreitet.

Speicherort für Aufzeichnungen angeben

Aufzeichnungsdateien werden standardmäßig unter `/var/xdl/session_recordings` gespeichert. Um einen anderen Pfad anzugeben, führen Sie den folgenden Befehl aus:

```
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
```

Sie können Aufzeichnungen auf einem lokalen Laufwerk oder einem Bereitstellungspunkt speichern, der auf einen Netzwerkpfad verweist. Konfigurieren Sie die entsprechenden Zugriffsberechtigungen für den von Ihnen festgelegten Speicherpfad und erteilen Sie dem Benutzer `ctxsrvr` die Schreibberechtigung für den Pfad.

Aufzeichnungen anzeigen

Um Aufzeichnungen anzuzeigen, führen Sie die folgenden Schritte aus, um den Sitzungsaufzeichnungsplayer oder den Sitzungsaufzeichnungs-Webplayer zu installieren:

1. Verwenden Sie Ihre Citrix-Kontodaten, um auf die Citrix Virtual Apps and Desktops-Downloadseite zuzugreifen und die Produktdatei herunterzuladen. 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 Sitzungsaufzeichnungs-Webplayer zu verwenden, installieren Sie ihn nur auf dem Sitzungsaufzeichnungsserver und stellen Sie sicher, dass Aufzeichnungen auf dem Sitzungsaufzeichnungsserver verfügbar sind. Weitere Informationen finden Sie in der Citrix Session Recording-Dokumentation.

Einschränkungen

- Bei virtuellen App-Sitzungen sind die Aufzeichnungsbenachrichtigungen möglicherweise nicht zentriert.

Virtual Channel SDK (Vorschau)

Mit dem Virtual Channel Software Development Kit (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 steht auf der Citrix Virtual Apps and Desktops Downloadseite zum Download bereit. erweitern Sie die entsprechende Version von Citrix Virtual Apps and Desktops und klicken Sie auf **Components**, um den Linux VDA-Download auszuwählen.

> **Hinweis:**
>
> Diese Funktion befindet sich in der Vorschauphase. Vorschaufunktionen sind möglicherweise nicht vollständig lokalisiert und werden für den Einsatz in Nicht-Produktionsumgebungen empfohlen. Der technische Support von Citrix unterstützt keine Probleme, die bei Vorschaufunktionen auftreten.

Wayland (Vorschau)

Der Linux VDA unterstützt Wayland 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
- Clientlaufwerkszuordnung (CDM)
- Drucken
- USB-Geräteumleitung

> **Hinweis:**
>
> - Diese Funktion befindet sich in der Vorschau. Vorschaufunktionen sind möglicherweise nicht vollständig lokalisiert und werden für den Einsatz in Nicht-Produktionsumgebungen empfohlen. Probleme, die bei Vorschaufunktionen gefunden werden, **werden nicht vom technischen Support von Citrix unterstützt**.
> - HDX™ 3D Pro wird nicht unterstützt.
> - Linux-Sitzungen für virtuelle Apps werden nicht unterstützt.

Wayland aktivieren

Um Wayland zu verwenden, setzen Sie den Registrierungsschlüssel **EnableWayland** auf **1**, indem Sie den folgenden Befehl ausführen:

```
/opt/Citrix/VDA/bin/ctxreg create -k
"HKLM\System\CurrentControlSet\Control\Citrix\Wayland" -t "REG_DWORD" -v
"EnableWayland" -d "0x00000001" --force
```

Standardmäßig ist der Registrierungsschlüssel **EnableWayland** auf **0** gesetzt, was bedeutet, dass X11 verwendet wird.

Prüfen, ob Wayland verwendet wird

1. Öffnen Sie ein Terminalfenster in Linux.
2. Führen Sie den Befehl **echo $XDG_SESSION_TYPE** aus.

Wenn Wayland verwendet wird, erhalten Sie **'wayland'** in der Ausgabe.

Einschränkungen

Bei Verwendung von Wayland wurden die folgenden Einschränkungen festgestellt:

- Das Tastaturlayout des Clientgeräts wird nicht mit dem Tastaturlayout des VDA synchronisiert.
- Es dauert etwa 20 Sekunden, sich von einer Sitzung auf RHEL 9.1/9.0 oder Rocky Linux 9.1/9.0 abzumelden.

Linux Virtual Delivery Agent-Dokumentverlauf

Die folgende Tabelle enthält wichtige Änderungen an der Linux Virtual Delivery Agent 2308-Dokumentation. Abonnieren Sie den RSS-Feed, um Benachrichtigungen über diese Updates zu erhalten.

DATUM	ÄNDERUNG	BESCHREIBUNG
14 Sep 2023	Erstrelease von Linux Virtual Delivery Agent 2308	Siehe Neue Features.