XenApp and XenDesktop 7.15 LTSR

Contents

Neue Features

July 11, 2022

Info zu diesem Release

Informationen zu Cumulative Update 9 (CU9)

Informationen zu Cumulative Update 8 (CU8)

Informationen zu Cumulative Update 7 (CU7)

Informationen zu Cumulative Update 6 (CU6)

Informationen zu Cumulative Update 5 (CU5)

Informationen zu Cumulative Update 4 (CU4)

Informationen zu Cumulative Update 3 (CU3)

Informationen zu Cumulative Update 2 (CU2)

Informationen zu Cumulative Update 1 (CU1)

Info zu 7.15 LTSR (Erstrelease)

Cumulative Update 9 (CU9)

August 2, 2022

Releasedatum: 8. Juli 2022

Info zu diesem Release

XenApp and XenDesktop 7.15 LTSR Cumulative Update 9 (CU9) behebt mehr als 15 Probleme, die seit dem Release von 7.15 LTSR CU8 gemeldet wurden.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR CU8 behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Download von 7.15 LTSR CU9

> **Wichtig:**
>
> Dieses Release weist Änderungen an der Art und Weise der Installation und des Upgrades von StoreFront auf. Wenn Sie in früheren Releases auf der Hauptseite des Komplettinstallationsprogramms auf die Kachel **Erste Schritte** geklickt haben, wurde auf der Seite **Kernkomponenten** auch StoreFront aufgeführt. Sie können StoreFront und andere Kernkomponenten zur Installation auf derselben Maschine auswählen.
>
> Ab diesem Release enthält die Seite **Kernkomponenten** kein Kontrollkästchen für StoreFront mehr. Um StoreFront zu installieren oder zu aktualisieren, klicken Sie auf der Hauptseite im Bereich **Bereitstellung erweitern** auf **Citrix StoreFront**. Damit wird `CitrixStoreFront-x64.exe` auf dem Installationsmedium gestartet.
>
> In dem Befehl `XenDesktopServerSetup.exe` können Sie `/components storefront` nicht mehr angeben. Andernfalls schlägt der Befehl fehl. Führen Sie zum Installieren von StoreFront über die Befehlszeile `CitrixStoreFront-x64.exe` aus. Die Datei ist im Ordner `x64` des Citrix Virtual Apps and Desktops-Installationsmediums.
>
> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.16.3.0 Build 30000 erreicht. Verwenden Sie den Citrix Licensing Manager.

Neue Bereitstellungen

Wie stelle ich das CU9 von Grund auf bereit?

Mit dem CU9-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf dem CU9 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU9 umfasst Updates für Basiskomponenten von 7.15 LTSR. Citrix empfiehlt die Aktualisierung aller LTSR-Komponenten Ihrer Bereitstellung auf CU9. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU9-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU9

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.9000	
VDA für Serverbetriebssystem	7.15.9000	
Citrix Studio	7.15.9000	
Citrix Director	7.15.9000	
Delivery Controller	7.15.9000	
Citrix Verbundauthen-tifizierungsdienst	7.15.9000	
Citrix Gruppenrichtlinienverwaltung	3.1.9000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	3.1.9000	
Linux VDA	7.15.6000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15.9000	
Provisioning Services	7.15.45	
Sitzungsaufzeichnung	7.15.9000	Nur Premium Edition
StoreFront	3.12.9000	
Universeller Druckserver	7.15.9000	

XenApp und XenDesktop 7.15 LTSR CU9-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht

beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU9 kompatible Komponenten und Plattformen	Version
App Layering	2011
*Browserinhaltsumleitung	15.19.2000
Citrix SCOM Management Pack für den Lizenzserver	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.4.3000
Lizenzserver	11.16.6.0 Build 33000
Self-Service-Kennwortzurücksetzung	1.1.20.0
Workspace Environment Management	2012

***Browserinhaltsumleitung**

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonymisierte Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren oder aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp 7.15 LTSR CU9. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der XenApp 7.15-LTSR CU9-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU9-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU9-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU9-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

August 2, 2022

Citrix Director

- In Citrix Director werden auf der Seite **Sitzungsdetails** angewendete Richtlinien möglicherweise zweimal angezeigt, wenn für die Richtlinien sowohl Computer- als auch Benutzereinstellungen definiert sind. [CVADHELP-19205]

Citrix Studio

- Versuche, in Citrix Studio eine Hostingverbindung zu Azure herzustellen, schlagen möglicherweise mit einer Ausnahme fehl. Das Problem tritt aufgrund der von Microsoft in Azure

vorgenommenen Änderungen auf. Ein privater Fix ist unter CTX457802 verfügbar. [CVADHELP-18741]

- Delivery Controller zeigt eine verzögerte Reaktion, wenn Sie Richtlinien über die Registerkarte **Richtlinien** in Citrix Studio hinzufügen, erstellen oder entfernen. Die typische Reaktionszeit ist 10 bis 15 Minuten. [CVADHELP-18743]

Delivery Controller

- Der Sitetest schlägt möglicherweise fehl, wenn die Netzwerkverbindung zwischen Delivery Controllern in verschiedenen Satellitenzonen blockiert ist. [CVADHELP-17273]
- Nach dem Upgrade von XenApp und XenDesktop 7.6 auf XenApp und XenDesktop 7.15 LTSR CU6 oder höher oder Citrix Virtual Apps and Desktops 1912 LTSR und nachdem Sie einen MCS (Maschinenerstellungsdienste)-Katalog erstellt haben, ist die Option **Größe des Datenträgercache (GB)** möglicherweise deaktiviert und kann nicht aktiviert werden. Um den Fix zu aktivieren, starten Sie den Hostdienst neu und öffnen Sie Citrix Studio nach dem DBschema-Upgrade neu. [CVADHELP-17705]
- Citrix Director zeigt bei der Suche möglicherweise nicht die IP-Adressen einiger VDA-Maschinen an. Das Problem tritt auf, wenn die Tabelle **MonitorData.[Machine]** doppelte Einträge enthält. [CVADHELP-18108]

Linux Virtual Delivery Agent

Die Dokumentation zu Linux Virtual Delivery Agent 7.15 LTSR CU9 enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

- Nach dem Aktivieren der Richtlinie “Ausgeschlossene Dateien oder Ordner löschen”kann der erste Anmeldeversuch mit der Profilverwaltung länger dauern. Dieses Problem tritt auf, wenn das Benutzerprofil unnötige Dateien enthält, die die Anmeldung verlangsamen. [CVADHELP-17230]
- Das Überprüfen der Active Directory-Gruppenmitgliedschaft schlägt möglicherweise fehl, wenn Benutzergeräte im Offlinemodus während der Anmeldung eine Verbindung zum Netzwerk herstellen. Infolgedessen schlägt auch die Profilverwaltung fehl. [CVADHELP-17364]
- Wenn Sie den Ordnerumleitungspfad über die Citrix Profilverwaltungsrichtlinie ändern, werden möglicherweise Daten im Umleitungspfad für Legacyordner gelöscht. [CVADHELP-17833]

- Der Versuch, Desktops zu starten, die die Profilverwaltung verwenden, schlägt möglicherweise mit dieser Fehlermeldung fehl:

  Gruppenrichtlinienclientdienstanmeldung ist fehlgeschlagen.

  Zugriff verweigert.

  [CVADHELP-18398]

- Der Profilverwaltungsdienst wird möglicherweise aufgrund einer nicht behandelten Ausnahme unerwartet beendet. [CVADHELP-18813]

- Wenn Sie auf einem Windows 10 20H2-Desktop den Benutzerspeicherpfad mit einer `!CTX_OSNAME!`-Variable konfigurieren, erstellt die Profilverwaltung möglicherweise Ordnernamen im Benutzerspeicher mit falschen Informationen. Folgendes wird beobachtet:

  - Für Version CU3 enthalten die neuen Profile möglicherweise als Betriebssystem Win10RS6.
  - Für Version CU4 enthalten die neuen Profile möglicherweise als Betriebssystem Win10_2009.

[CVADHELP-19016]

- Wenn Sie Edge Chromium auf einem veröffentlichten Desktop mit aktivierter Profilverwaltung starten, werden möglicherweise doppelte Profile erstellt, sobald Sie sich neu anmelden. Das Problem tritt auf, da die Profilverwaltung lokale Profile während der Abmeldung möglicherweise nicht löscht. [CVADHELP-19865]

Provisioning Services

Die Dokumentation zu Provisioning Services 7.15 LTSR CU9 enthält Informationen zu den Updates in diesem Release.

StoreFront

- Wenn das **CtxsClientVersion**-Cookie abläuft, während das Cookie **CtxsClientDetectionDone** noch aktiv ist, wechseln vorhandene native Anwendungen zu HTML5 und neue Anwendungen werden mit HTML5 gestartet. [CVADHELP-18040]

- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX377814. [CVADHELP-19161]

VDA für Desktopbetriebssystem

Tastatur

- Dieser Fix behebt Probleme mit dem russischen Tastaturlayout in der Citrix Workspace-App für HTML5-, Mac- und Linux-Clients. [CVADHELP-19012]

Drucken

- Wenn Sie mit der Option **Druckausgabe speichern unter** in einer Seamlesssitzung den Druck in eine Datei umleiten, wird das Druckfenster möglicherweise nicht richtig angezeigt. [CVADHELP-16614]
- Wenn Sie dem generischen universellen Drucker eine Richtlinie hinzufügen, wird möglicherweise der generische Citrix Universelle Drucker zum Standarddrucker anstelle des Client-Hauptdruckers. [CVADHELP-18157]

Sitzung/Verbindung

- Wenn Sie eine Sitzung beenden, reagiert der Server möglicherweise nicht mehr. Das Problem tritt auf, wenn Sie die generische USB-Umleitung verwenden. [CVADHELP-18204]

Systemausnahmen

- Auf VDAs kann es bei wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-16055]
- Auf VDAs kann es in icaussb.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x3B kommen. [CVADHELP-17339]

VDA für Serverbetriebssystem

Tastatur

- Dieser Fix behebt Probleme mit dem russischen Tastaturlayout in der Citrix Workspace-App für HTML5-, Mac- und Linux-Clients. [CVADHELP-19012]

Drucken

- Wenn Sie mit der Option **Druckausgabe speichern unter** in einer Seamlesssitzung den Druck in eine Datei umleiten, wird das Druckfenster möglicherweise nicht richtig angezeigt. [CVADHELP-16614]
- Wenn Sie dem generischen universellen Drucker eine Richtlinie hinzufügen, wird möglicherweise der generische Citrix Universelle Drucker zum Standarddrucker anstelle des Client-Hauptdruckers. [CVADHELP-18157]

Sitzung/Verbindung

- Wenn Sie eine Sitzung beenden, reagiert der Server möglicherweise nicht mehr. Das Problem tritt auf, wenn Sie die generische USB-Umleitung verwenden. [CVADHELP-18204]

Systemausnahmen

- Auf VDAs kann es bei wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-16055]
- Der Citrix Stack Control Service (SCService64.exe) wird möglicherweise unerwartet beendet. [CVADHELP-18707]
- Auf VDAs kann es in icaussb.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x3B kommen. [CVADHELP-17339]

Kumulatives Update 8 (CU8)

September 16, 2021

Releasedatum: 11. August 2021

Info zu diesem Release

Das kumulative Update 8 (CU8) für XenApp und XenDesktop 7.15 LTSR behebt über 40 seit 7.15 LTSR CU7 gemeldete Probleme.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR CU7 behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Download von 7.15 LTSR CU8

> **Wichtig:**
>
> Dieses Release weist Änderungen an der Art und Weise der Installation und des Upgrades von StoreFront auf. Wenn Sie in früheren Releases auf der Hauptseite des Komplettinstallationsprogramms auf die Kachel **Erste Schritte** geklickt haben, wurde auf der Seite **Kernkomponenten** auch StoreFront aufgeführt. Sie können StoreFront und andere Kernkomponenten zur Installation auf derselben Maschine auswählen.
>
> Ab diesem Release enthält die Seite **Kernkomponenten** kein Kontrollkästchen für StoreFront mehr. Um StoreFront zu installieren oder zu aktualisieren, klicken Sie auf der Hauptseite im Bereich **Bereitstellung erweitern** auf **Citrix StoreFront**. Damit wird `CitrixStoreFront-x64.exe` auf dem Installationsmedium gestartet.
>
> In dem Befehl `XenDesktopServerSetup.exe` können Sie `/components storefront` nicht mehr angeben. Andernfalls schlägt der Befehl fehl. Führen Sie zum Installieren von StoreFront über die Befehlszeile `CitrixStoreFront-x64.exe` aus. Die Datei ist im Ordner `x64` des Citrix Virtual Apps and Desktops-Installationsmediums.
>
> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.16.3.0 Build 30000 erreicht. Verwenden Sie den Citrix Licensing Manager.

Neue Bereitstellungen

Wie stelle ich das CU8 von Grund auf bereit?

Mit dem CU8-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf dem CU8 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU8 umfasst Updates für Basiskomponenten von 7.15 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU8 zu aktualisieren. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU8-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU8

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.8000	
VDA für Serverbetriebssystem	7.15.8000	
Citrix Studio	7.15.8000	
Citrix Director	7.15.8000	
Delivery Controller	7.15.8000	
Citrix Verbundauthentifizierungsdienst	7.15.8000	
Citrix Gruppenrichtlinienverwaltung	3.1.8000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	3.1.8000	
Linux VDA	7.15.6000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15.8000	
Provisioning Services	7.15.39	
Sitzungsaufzeichnung	7.15.8000	Nur Premium Edition
StoreFront	3.12.8000	
Universeller Druckserver	7.15.8000	

XenApp und XenDesktop 7.15 LTSR CU8-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU8 kompatible Komponenten und Plattformen	Version
App Layering	2011
*Browserinhaltsumleitung	15.19.2000
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.4.3000
Lizenzserver	11.16.6.0 Build 33000
Self-Service-Kennwortzurücksetzung	1.1.20.0
Workspace Environment Management	2012

*Browserinhaltsumleitung

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonymisierte Informationen über den Installationsvorgang

gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren oder aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp 7.15 CU8. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der XenApp 7.15-LTSR CU8-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU8-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU8-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU8-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

January 21, 2022

Citrix Director

- In Citrix Director werden möglicherweise falsche Informationen zur Anzahl der Benutzersitzungen angezeigt. [CVADHELP-14849]

Citrix Richtlinie

- Auf der Registerkarte **Richtlinien > Zugewiesen zu** werden evtl. Citrix Richtlinien angezeigt, die Sie einer oder mehreren Bereitstellungsgruppen zuweisen, falsch angezeigt. Beispiel: Sie weisen eine Richtlinie zwei Bereitstellungsgruppen zu und aktivieren die Zuweisung nur für eine. Auf der Registerkarte **Zugewiesen zu** werden beide Bereitstellungsgruppen angezeigt. Wenn Sie die Richtlinie deaktivieren, wird die Zuweisung aufgehoben. Auf der Registerkarte **Zugewiesen zu** wird sie jedoch weiterhin als zugewiesen angezeigt. [CVADHELP-15233]
- Wenn Sie eine Richtlinie in einer Citrix Cloud-Umgebung erstellen und anhand der Organisationseinheit nach Domäne A filtern, kann sich der Benutzer in Domäne B möglicherweise nicht anmelden. Das Problem tritt beim Zugriff auf eine veröffentlichte Anwendung oder einen veröffentlichten Desktop auf. [[CVADHELP-17179]

Citrix Studio

- Dieser Fix bietet erhöhte Sicherheit, da nur genehmigte StoreFront- und Citrix Gateway-Maschinen mit dem Delivery Controller kommunizieren können. Weitere Informationen finden Sie unter Sicherheitsschlüssel. [CVADHELP-15729]
- Der Versuch, virtuelle Maschinen aus einem bestehenden Katalog hinzuzufügen oder zu löschen, kann fehlschlagen. [CVADHELP-17316]

Delivery Controller

- Dieser Fix bietet erhöhte Sicherheit, da nur genehmigte StoreFront- und Citrix Gateway-Maschinen mit dem Delivery Controller kommunizieren können. Weitere Informationen finden Sie unter Sicherheitsschlüssel. [CVADHELP-15729]
- Wenn Sie Maschinen oder Kataloge löschen, die mit einer AWS-Hostingverbindung verknüpft sind, werden EBS-Stammgeräte möglicherweise nicht automatisch gelöscht. Das Problem tritt auf, weil sich das Flag **DeleteOnTermination** auf dem Basisimage auf Datenträgern, die bei der Maschinenkatalogerstellung für diese Kataloge erstellt wurden, von `$true` in `$false` ändert. [CVADHELP-16096]
- Der Citrix Broker-Dienst (Brokerservice.exe) reagiert möglicherweise nicht mehr und geht offline. [CVADHELP-16352]
- Nach einem Upgrade von XenApp und XenDesktop 7.15 CU6 auf Citrix Virtual Apps and Desktops 1912 LTSR CU2 können Probleme beim Aktualisieren der Datenbank auftreten. Das Problem tritt auf, wenn die **AdminAccountName/AdminUpn**-Einträge mehr als 64 Zeichen enthalten. [CVADHELP-17379]

- Der Versuch, einen Katalog mit einem Namen mit Sonderzeichen (z. B. & und $) zu aktualisieren, schlägt möglicherweise fehl, wenn das aktualisierte Masterimage nicht auf die VDAs hochgestuft wird. [CVADHELP-17686]
- Wenn die Multisiteaggregation konfiguriert ist und zugleich die Eigenschaft "SessionReconnection"in der Anspruchsrichtlinienregel auf **SameEndPointOnly** festgelegt ist, wird möglicherweise anstelle einer Wiederverbindung der aktiven Sitzung eine neue Sitzung gestartet. [CVADHELP-17692]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 7.15 LTSR CU8 Dokumentation enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

- Windows-Benutzeranmeldeinformationen bleiben möglicherweise erhalten, nachdem sie aus der Anmeldeinformationsverwaltung entfernt wurden. [CVADHELP-16083]
- Ordner, die vor dem Aktivieren von Ausgeschlossene Dateien oder Ordner löschen über die Richtlinie Anmeldeausschlussprüfung erstellt wurden, aber durch die Richtlinie Ausschlussliste —Verzeichnisse oder Standardausschlussliste der Verzeichnisse aktivieren ausgeschlossen wurden, werden möglicherweise nicht gelöscht. [CVADHELP-16439]
- Neue Dateien, die mit der Richtlinieneinstellung **Verarbeitung von großen Dateien: Dateien werden als symbolische Verknüpfungen erstellt** erstellt wurden, werden beim Abmelden möglicherweise nicht synchronisiert. [CVADHELP-16526]
- Bei installierter Citrix Profilverwaltung werden umgeleitete Ordner möglicherweise unter dem lokalen Benutzerprofil neu erstellt. [CVADHELP-16861]
- Dieser Fix behebt eine Sicherheitslücke im Citrix Profilverwaltungs-WMI-Plugin-Installationsprogramm. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX319750. [CVADHELP-17728]
- Dieser Fix behebt eine Sicherheitslücke im Citrix Profilverwaltungs-Installationsprogramm. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX319750. [CVADHELP-17939]

Provisioning Services

Die Dokumentation zu Provisioning Services 7.15 LTSR CU8 enthält Informationen zu den Updates in diesem Release.

StoreFront

- Dieser Fix bietet erhöhte Sicherheit, da nur genehmigte StoreFront- und Citrix Gateway-Maschinen mit dem Delivery Controller kommunizieren können. Weitere Informationen finden Sie unter Sicherheitsschlüssel. [CVADHELP-15729]
- Wenn Socketpooling aktiviert ist, schlagen Anmeldeversuche bei StoreFront möglicherweise mit folgender Fehlermeldung fehl:

  Ihre Anforderung kann nicht abgeschlossen werden

  Das Problem tritt auf, wenn die dynamischen TCP-Ports aufgebraucht sind.

  [CVADHELP-16625]
- Wenn die Multisiteaggregation konfiguriert ist und zugleich die Eigenschaft **SessionReconnection** in der Anspruchsrichtlinienregel auf **SameEndPointOnly** festgelegt ist, wird möglicherweise anstelle einer Wiederverbindung der aktiven Sitzung eine neue Sitzung gestartet. [CVADHELP-16698]
- Nach dem Upgrade von StoreFront von Version 7.15 LTSR CU4 werden VDI-Desktops mit demselben Hostnamen möglicherweise in zufälliger Reihenfolge anstelle der fortlaufenden Reihenfolge angezeigt. [CVADHELP-16723]
- Beim Starten einer Benutzersitzung mit der Citrix StoreFront-Dienste-API sind die an die Startanforderung übergebenen Parameter möglicherweise falsch. [CVADHELP-16834]

Universeller Druckserver

Server

- Der universelle Druckserver (UPServer.exe) wird möglicherweise unerwartet beendet. Das Problem tritt aufgrund des fehlerhaften Moduls prntvpt.dll auf. [CVADHELP-12651]

Benutzerprofilverwaltung –VDA

- Wenn Sie sich an einer Sitzung anmelden, werden die Benutzerdaten möglicherweise unerwartet gelöscht. Das Problem tritt auf, wenn Sie die Dateiserveradresse von path1 in path2 in den Einstellungen der Citrix-Richtlinie Ordnerumleitungspfad ändern (z. B. die Einstellung Desktop path) und path1 und path2 auf denselben physischen Ort verweisen. Zur Problemvermeidung aktivieren Sie die Microsoft-Gruppenrichtlinieneinstellung **Vor der Umleitung überprüfen, ob das alte und das neue Ziel der Ordnerumleitung auf dieselbe Freigabe verweisen**. Weitere Informationen finden Sie im Abschnitt Beschreibung der Einstellungen der Citrix Richtlinie "Ordnerumleitungspfad". [CVADHELP-12439]

VDA für Desktopbetriebssystem

Drucken

- Das Ausdrucken einer PDF-Datei aus einer über die Citrix Workspace-App für Chrome gestarteten Sitzung kann fehlschlagen. [CVADHELP-15318]
- Bei Verwendung eines Remote-PC-Zugriffs-VDAs beim Drucken über die Citrix Workspace-App für Mac werden die Druckereinstellungen möglicherweise ignoriert. [CVADHELP-15320]
- Wird eine Datei mit dem universellen Citrix-Druckertreiber (UPD) gedruckt, werden möglicherweise falsche Bilder in der gedruckten Datei angezeigt. Das Problem tritt auf, wenn Sie einen VDA von Version 7.15.5000 auf Version 1912.1000 aktualisieren und die Heavyweight-Komprimierung aktivieren. [CVADHELP-15813]

Sitzung/Verbindung

- Bei Aufzeichnen einer Sitzung in der Citrix Workspace-App für Windows werden Bewegungen des Mauszeigers möglicherweise nicht aufgezeichnet. Das Problem tritt mit VDA-Version 7.15.400 auf. [CVADHELP-13300]
- Wenn Sie versuchen, über die Taskleistenvorschau zu einem Fenster zu wechseln, kann das Öffnen dieses Fensters lange dauern. [CVADHELP-15422]
- Bei Verwendung des generischen IME für Microsoft Windows 10 20H2 mit dem Update KB4586853 wird die Anwendung möglicherweise unerwartet beendet. [CVADHELP-16664]
- Mit diesem Fix können Sie jetzt in den erweiterten Tastatureinstellungen verschiedene Eingabemethoden für jedes Anwendungsfenster festlegen. [CVADHELP-16731]
- Bei Verwendung bestimmter Anwendungen von Drittanbietern wird möglicherweise ein schwarzer Bildschirm angezeigt, wenn die Anwendung ein anderes Fenster öffnet. [CVADHELP-16956]

Systemausnahmen

- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x93 (INVALID_KERNEL_HANDLE) kommen. [CVADHELP-15326]
- Der Citrix Desktop-Dienst (BrokerAgent.exe) generiert möglicherweise eine große Anzahl von ID 1010-Ereignissen, wenn die OU-basierte Controllererkennung über einen VPN-Tunnel mit direktem Zugriff verwendet wird. [CVADHELP-16754]
- Im Citrix Desktop-Dienst (BrokerAgent.exe) kann eine Zugriffsverletzung auftreten, worauf der Dienst unerwartet beendet wird. [CVADHELP-17055]

Benutzererfahrung

- Bei Verwendung von Explorer wird möglicherweise ein schwarzer Fleck auf dem Bildschirm angezeigt. Das Problem tritt bei Verbindung mit Endpunkten mit bestimmten AMD GPU-Modellen auf.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: MinTransientWidth

  Typ: DWORD

  Wert: 00000021

  [CVADHELP-17057]

VDA für Serverbetriebssystem

Drucken

- Das Ausdrucken einer PDF-Datei aus einer über die Citrix Workspace-App für Chrome gestarteten Sitzung kann fehlschlagen. [CVADHELP-15318]
- Bei Verwendung eines Remote-PC-Zugriffs-VDAs beim Drucken über die Citrix Workspace-App für Mac werden die Druckereinstellungen möglicherweise ignoriert. [CVADHELP-15320]
- Wird eine Datei mit dem universellen Citrix-Druckertreiber (UPD) gedruckt, werden möglicherweise falsche Bilder in der gedruckten Datei angezeigt. Das Problem tritt auf, wenn Sie einen VDA von Version 7.15.5000 auf Version 1912.1000 aktualisieren und die Heavyweight-Komprimierung aktivieren. [CVADHELP-15813]

Sitzung/Verbindung

- Bei Aufzeichnen einer Sitzung in der Citrix Workspace-App für Windows werden Bewegungen des Mauszeigers möglicherweise nicht aufgezeichnet. Das Problem tritt mit VDA-Version 7.15.400 auf. [CVADHELP-13300]
- Beim Starten einer Sitzung über die Citrix Workspace-App für HTML5 wird diese möglicherweise im Fenstermodus statt im Vollbildmodus ausgeführt. Das Problem tritt bei VDAs unter Windows Server 2012 auf. [CVADHELP-14865]
- Wenn Sie versuchen, über die Taskleistenvorschau zu einem Fenster zu wechseln, kann das Öffnen dieses Fensters lange dauern. [CVADHELP-15422]

- Eine Webcam wird möglicherweise nicht zur Registrierung hinzugefügt. Andere Anwendungen in einer Citrix-Sitzung können die Webcam daraufhin unter Umständen nicht erkennen.

  Legen Sie den folgenden Registrierungsschlüssel fest, damit die Benutzer die Wartezeit von **WebcamArrivalEvent** einstellen können:

  - Auf 32-Bit-Systemen:

    HEKY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime

    Name: RetryNumToWaitWebcamArrival

    Typ: DWORD

    Wert: Standardmäßig fehlt der Registrierungsschlüssel. Wenn der Registrierungsschlüssel nicht vorhanden ist oder nicht gelesen wird, wird der Standardwert von 1000 verwendet. Dieser Wert gibt die Standardwartungsdauer (20 Sekunden) an. Wenn der Wert kleiner als 1000 ist, wird der Standardwert (1000) verwendet.

  - Auf 64-Bit-Systemen:

    HEKY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxRealTime

    Name: RetryNumToWaitWebcamArrival

    Typ: DWORD

    Wert: Standardmäßig fehlt der Registrierungsschlüssel. Wenn der Registrierungsschlüssel nicht vorhanden ist oder nicht gelesen wird, wird der Standardwert von 1000 verwendet. Dieser Wert gibt die Standardwartungsdauer (20 Sekunden) an. Wenn der Wert kleiner als 1000 ist, wird der Standardwert (1000) verwendet.

    [CVADHELP-16318]

- Mit diesem Fix können Sie jetzt in den erweiterten Tastatureinstellungen verschiedene Eingabemethoden für jedes Anwendungsfenster festlegen. [CVADHELP-16731]
- Bei Verwendung bestimmter Anwendungen von Drittanbietern wird möglicherweise ein schwarzer Bildschirm angezeigt, wenn die Anwendung ein anderes Fenster öffnet. [CVADHELP-16956]

Systemausnahmen

- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x93 (INVALID_KERNEL_HANDLE) kommen. [CVADHELP-15326]
- Der Citrix Desktop-Dienst (BrokerAgent.exe) generiert möglicherweise eine große Anzahl von ID 1010-Ereignissen, wenn die OU-basierte Controllererkennung über einen VPN-Tunnel mit direktem Zugriff verwendet wird. [CVADHELP-16754]

- Im Citrix Desktop-Dienst (BrokerAgent.exe) kann eine Zugriffsverletzung auftreten, worauf der Dienst unerwartet beendet wird. [CVADHELP-17055]

Benutzererfahrung

- Bei Verwendung von Explorer wird möglicherweise ein schwarzer Fleck auf dem Bildschirm angezeigt. Das Problem tritt bei Verbindung mit Endpunkten mit bestimmten AMD GPU-Modellen auf.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: MinTransientWidth

  Typ: DWORD

  Wert: 00000021

  [CVADHELP-17057]

Virtual Desktop-Komponenten –Sonstiges

- Der Start von App-V-Anwendungen kann lange dauern. [CVADHELP-16732]

Kumulatives Update 7 (CU7)

September 16, 2021

Releasedatum: 9. Februar 2021

Info zu diesem Release

Das kumulative Update 7 (CU7) für XenApp und XenDesktop 7.15 LTSR behebt über 60 seit 7.15 LTSR CU6 gemeldete Probleme.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR CU6 behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Download von 7.15 LTSR CU7

> **Wichtig:**
>
> Dieses Release weist Änderungen an der Art und Weise der Installation und des Upgrades von StoreFront auf. Wenn Sie in früheren Releases auf der Hauptseite des Komplettinstallationsprogramms auf die Kachel **Erste Schritte** geklickt haben, wurde auf der Seite **Kernkomponenten** auch StoreFront aufgeführt. Sie können StoreFront und andere Kernkomponenten zur Installation auf derselben Maschine auswählen.
>
> Ab diesem Release enthält die Seite **Kernkomponenten** kein Kontrollkästchen für StoreFront mehr. Um StoreFront zu installieren oder zu aktualisieren, klicken Sie auf der Hauptseite im Bereich **Bereitstellung erweitern** auf **Citrix StoreFront**. Damit wird `CitrixStoreFront-x64.exe` auf dem Installationsmedium gestartet.
>
> In dem Befehl `XenDesktopServerSetup.exe` können Sie `/components storefront` nicht mehr angeben. Andernfalls schlägt der Befehl fehl. Führen Sie zum Installieren von StoreFront über die Befehlszeile `CitrixStoreFront-x64.exe` aus. Die Datei ist im Ordner `x64` des Citrix Virtual Apps and Desktops-Installationsmediums.
>
> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.16.3.0 Build 30000 erreicht. Verwenden Sie den Citrix Licensing Manager.

Neue Bereitstellungen

Wie stelle ich das CU7 von Grund auf bereit

Mit dem CU7-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf dem CU7 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU7 umfasst Updates für Basiskomponenten von 7.15 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU7 zu aktualisieren. Beispiel: Wenn Citrix Provisioning zur LTSR-Bereitstellung gehört, aktualisieren Sie die Citrix Provisioning-Komponenten auf die CU7-Version. Wenn Citrix Provisioning nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU7

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.7000	
VDA für Serverbetriebssystem	7.15.7000	
Citrix Studio	7.15.7000	
Citrix Director	7.15.7000	
Delivery Controller	7.15.7000	
Citrix Verbundauthentifizierungsdienst	7.15.7000	
Citrix Gruppenrichtlinienverwaltung	3.1.7000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	3.1.7000	
Linux VDA	7.15.6000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15.7000	
Provisioning Services	7.15.33	
Sitzungsaufzeichnung	7.15.7000	Nur Premium Edition
StoreFront	3.12.7000	
Universeller Druckserver	7.15.7000	

XenApp und XenDesktop 7.15 LTSR CU7-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht

beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU7 kompatible Komponenten und Plattformen	Version
App Layering	2011
*Browserinhaltsumleitung	15.19.2000
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.4.3000
Lizenzserver	11.16.6.0 Build 33000
Self-Service-Kennwortzurücksetzung	1.1.20.0
Workspace Environment Management	2012

***Browserinhaltsumleitung**

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonymisierte Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren oder aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp 7.15 CU7. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach Installation der Kernkomponenten von XenApp 7.15 LTSR CU7 und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU7-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU7-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15-CU7-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

August 15, 2023

Citrix Director

- Bei Verwendung von Director in einer Umgebung mit großen Sites verbraucht der IIS-Workerprozess (w3wp.exe) schlechter Netzwerkverbindung evtl. viel Arbeitsspeicher. Die Director-Seite wird nicht weiter geladen. [CVADHELP-14959]
- Nach der Deinstallation eines VDA bleiben die Namespaces für Citrix Windows Management Instrumentation (WMI) möglicherweise erhalten. [CVADHELP-14965]
- Auf der Seite **Historische Maschinenauslastung** wird die Tabelle **Top-10-Prozesse** auf möglicherweise nicht angezeigt. Folgende Meldung wird angezeigt:

Die Datensammlung für Prozesse ist auf dieser Maschine deaktiviert. Aktivieren Sie die Richtlinie für die Prozessüberwachung, um mit dem Sammeln von Daten zu beginnen.

[CVADHELP-15893]

- Wenn Sie auf der Seite **Director > Trends > Anmeldungsleistung > Bericht exportieren** einen Bericht generieren und exportieren, enthält dieser möglicherweise falsche Brokering-Zeitwerte. Das Problem tritt bei dem deutschsprachigen Bericht auf, in dem **.** durch **,** ersetzt wird. [CVADHELP-16097]

Citrix Richtlinie

- Wenn Sie die Citrix Gruppenrichtlinienengine von Version 1.7 auf Version 7.15 aktualisieren, wird die Richtlinie **Druckerzuweisungen** unter **Citrix Benutzerrichtlinien** möglicherweise nicht angezeigt. [CVADHELP-15608]

Citrix Studio

- Beim Erstellen einer Hostingverbindung mit Azure schlagen Versuche, einen Dienstprinzipal zu erstellen, möglicherweise mit dem Fehler ADSTS700016 fehl. [CVADHELP-16219]

Delivery Controller

- Einige veröffentlichte Anwendungen können dazu führen, dass die Anwendungsauflistung fehlschlägt. Das Problem tritt auf, wenn eine EXE-Datei ein beschädigtes Anwendungssymbol enthält. [CVADHELP-13133]
- In einer großen Citrix Virtual Apps and Desktops-Umgebung funktionieren gespeicherte Prozeduren für die Überwachungsdatenbankoptimierung möglicherweise nicht. Das Problem tritt auf, wenn die Überwachungsdatenbank groß ist. [CVADHELP-13287]
- Für Delivery Controller wird möglicherweise folgender, den lokalen Hostcache betreffenden Fehler 505 im Ereignisprotokoll angezeigt: Unbekannter Fehler [CVADHELP-14428]
- Nachdem ein VDA aufgrund einer hohen Speicherauslastung Volllast meldet, bleibt der Lastindexwert möglicherweise bei 10.000, selbst wenn die Speicherauslastung auf einen niedrigen Wert abfällt. [CVADHELP-14563]
- Der Versuch, einen MCS-Katalog (Maschinenerstellungsdienste) in Azure mit PowerShell zu erstellen, schlägt möglicherweise fehl, und es wird folgende Fehlermeldung angezeigt:

  Could not locate item with path=Citrix.AzureRmPlugin.InventoryItemPath.

Das Problem tritt auf, wenn Sie freigegebene Azure-Abonnements in Verbindung mit Dienstprinzipalen mit eingeschränktem Gültigkeitsbereich verwenden. [CVADHELP-14640]

- Wenn Sie sich mit Citrix Director bei einer neuen Sitzung anmelden, wird die Anmeldung möglicherweise nicht im Diagramm **Durchschnittliche Anmeldedauer** auf der Registerkarte **Anmeldungsleistung** unter **Trends** angezeigt. Die Anmeldung wird jedoch im Formular **Anmeldedauer per Benutzersitzung** angezeigt. [CVADHELP-14740]
- vSAN-Speicherrichtlinien werden möglicherweise nicht auf einer virtuellen Maschine angewendet, die mit MCS (Maschinenerstellungsdienste) erstellt wurde. Das Problem tritt auf, wenn die Version eines Datenträgers, der an die Maschine angeschlossen ist, falsch ist. [CVADHELP-14935]
- Wenn Sie Maschinenkataloge im Studio-Navigationsbereich auswählen, kann Studio die Liste der Kataloge möglicherweise nicht anzeigen. Die folgende Fehlermeldung wird angezeigt:

  Sie können keine Kataloge sehen.

  Das Problem tritt auf, weil Studio die Liste der Objekte nicht mit dem PowerShell-Befehl **Get-ProvSchemeMasterVMImageHistory** abrufen kann. [CVADHELP-15211]
- Versuche, einen Maschinenerstellungsdienste-Katalog unter Einsatz von VMware vSphere 7.0 zu erstellen, schlagen möglicherweise fehl. [CVADHELP-15237]
- Dieser Fix behebt Leistungsprobleme, die beim Delivery Controller (XML-Dienst) in langsamen Active Directory-Umgebungen auftreten können.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer

  oder

  HKEY_LOCAL_MACHINE\Software\Policies\Citrix\DesktopServer

  Name: DisableGetPasswordExpiryInfo

  Typ: DWORD

  Wert: 1

  [CVADHELP-15536]
- Dieser Fix sorgt dafür, dass MCS von Microsoft System Center Virtual Machine Manager (SCVMM) 2019 unterstützt wird. [CVADHELP-15779]

Metainstaller

- Bei der Installation von VDAs werden möglicherweise zusätzliche Komponenten wie persönliche vDisks installiert, selbst wenn Sie diese nicht über die GUI ausgewählt haben. [CVADHELP-

15572]

- Wenn Sie einen VDA aktualisieren, können Sie die Funktion **Leistung optimieren** auf der Seite **Features** nicht deaktivieren. Außerdem können Sie keine anderen Features auf dieser Seite aktivieren. [CVADHELP-14560]

Profilverwaltung

- Wenn die Richtlinie **Profilstreaming** in der Profilverwaltung aktiviert ist, schlagen Versuche, eine Datei in Internet Explorer 11 herunterzuladen, möglicherweise fehl. [CVADHELP-12970]
- Unter **Systemsteuerung > System und Sicherheit > System > Einstellungen ändern > Erweitert > Benutzerprofile > Einstellungen** enthält das Profil des angemeldeten Benutzers ein Fragezeichen im Feld "Größe". Für die anderen Benutzerprofile wird die richtige Größe angezeigt. [CVADHELP-13993]
- Wenn Sie Appdata\local\temp zu **Ausschlussliste - Verzeichnisse** hinzufügen, erstellt die Profilverwaltung nicht den Ordner Appdata\local\temp im Benutzerprofil und es treten Laufzeitfehler bei einigen Anwendungen auf, wie z. B. Microsoft Outlook. Das Problem tritt bei der zweiten oder nachfolgenden Anmeldungen auf, wenn die Richtlinie **Lokal zwischengespeicherte Profile nach Abmeldung löschen** aktiviert ist. [CVADHELP-14054]
- Die Profilverwaltung synchronisiert nicht die Unterschlüssel eines Registrierungsschlüssels, der auf der **Aufnahmeliste für die Registrierung** steht. Wenn Sie beispielsweise Software\Citrix der **Aufnahmeliste für die Registrierung** hinzufügen, wird nur HKEY_CURRENT_USER\SOFTWARE\Citrix im Benutzerspeicher gespeichert. Die Unterschlüssel werden nicht gespeichert. [CVADHELP-14815]
- Wenn ein Ordner in der Liste **Zu spiegelnde Ordner** bei der Anmeldung nicht im Benutzerspeicher ist, wird das lokale Benutzerprofil gelöscht. [CVADHELP-15248]
- Nach dem Hinzufügen von **Desktop** zur Richtlinie **Ausschlussliste - Verzeichnisse** kann beim Speichern von Änderungen in veröffentlichten Anwendungen bzw. Desktops ein Fehler auftreten. [CVADHELP-15792]

Provisioning Services

Provisioning Services 7.15 LTSR CU7 enthält Informationen zu den Updates in diesem Release.

StoreFront

- Unter iPadOS 13 oder höher können StoreFront-Webseiten hängen bleiben, wenn eine Benutzeranmeldung versucht wird. Das Problem tritt auf, wenn die Richtlinie "Klassische

Oberfläche aktivieren"für die StoreFront-Bereitstellung aktiviert ist. [CVADHELP-14905]

- Ist eine benutzerdefinierte Konfigurationsdatei im Store-Ordner, ersetzt sie möglicherweise den Inhalt der web.config-Datei im Store-Ordner. Das Problem tritt auf, wenn Sie StoreFront aktualisieren. [CVADHELP-13485]

VDA für Desktopbetriebssystem

Sitzung/Verbindung

- Wenn mehrere USB-Geräte an eine Sitzung umgeleitet werden, funktioniert eines von ihnen möglicherweise nicht ordnungsgemäß. [CVADHELP-12516]
- Das Standardaudiogerät einer Sitzung ist möglicherweise nicht mit dem Standardgerät auf dem Benutzergerät identisch. In der Sitzung wird das erste Gerät in der Audiogeräteliste zum Standardgerät. [CVADHELP-13324]
- Wenn Sie in einer Site, in der XenApp und XenDesktop Version 7.15 LTSR CU 4 unter Microsoft Windows Server 2016 ausgeführt wird, eine veröffentlichte Anwendung starten, reagiert die Anwendungssitzung möglicherweise nicht mehr. Die folgende Fehlermeldung wird angezeigt:

  Bitte warten Sie auf den lokalen Sitzungsmanager…

  [CVADHELP-13967]
- Wenn die **SAS-Benachrichtigung** aktiviert ist, beobachten Benutzer mit mehreren Monitoren, die eine Verbindung zu einer vorhandenen Sitzung in der Konsole herstellen, dass das Monitorlayout nicht korrekt wiederhergestellt wird. Wenn beispielsweise rechts Monitor 1 ist, der als Hauptmonitor ausgewählt wurde, und links Monitor 2, beobachten Benutzer, dass die Positionen beim Wiederverbinden ausgetauscht sind. Dieses Problem betrifft nur RemotePC-Benutzer mit einem physischen Desktop. Dies ist auf eine Inkompatibilität zwischen zwei Features zurückzuführen.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: UseDCForLocalModes

  Typ: DWORD

  Wert: 1

  [CVADHELP-14249]
- Die Registrierung von VDAs wird möglicherweise zeitweise aufgehoben, wenn IPv6 aktiviert ist. [CVADHELP-14847]

- Dieser Fix bietet einen Timer zum Senden eines kleinen Datagramms über eine UDP-Verbindung, um die Verbindung zwischen Host und Client aufrechtzuerhalten.

  Zum Implementieren dieses Fixes legen Sie den Registrierungsschlüssel wie folgt fest:

  - *32-Bit-Systeme*

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

    Name: KeepAliveTimer

    Typ: DWORD

    Wert: Intervall (in Sekunden) zwischen den Keep-Alive-Meldungen. Wird kein Wert angegeben oder der Wert auf 0 gesetzt, werden keine Keep-Alive-Pakete gesendet und das Keep-Alive-Feature funktioniert nicht. Der empfohlene Wert ist 15.

  - *64-Bit-Systeme*

    HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

    Name: KeepAliveTimer

    Typ: DWORD

    Wert: Intervall (in Sekunden) zwischen den Keep-Alive-Meldungen. Wird kein Wert angegeben oder der Wert auf 0 gesetzt, werden keine Keep-Alive-Pakete gesendet und das Keep-Alive-Feature funktioniert nicht. Der empfohlene Wert ist 15.

    [CVADHELP-15122]

- Wenn der CtxUvi Hooking-Treiber deaktiviert ist, werden möglicherweise keine Ereignisprotokolle generiert. Das Problem tritt auf, wenn nur wenige Systemressourcen verfügbar sind. [CVADHELP-15241]
- Dieser Fix bietet Unterstützung für ein neues Feature, mit dem Sie mehrere Gesamtstrukturbereitstellungen konfigurieren können, ohne die NTLM-Authentifizierung für VDAs zu aktivieren. Das frühere Feature zur Aktivierung der NTLM-Authentifizierung ist jedoch anderen Bereitstellungen ohne Vertrauensstellung vorbehalten. Ein Registrierungseintrag **SupportMultipleForestDdcLookup** wird hinzugefügt, um eine unerwünschte Aktivierung der NTLM-Authentifizierung auf VDAs zu verhindern. (NTLM ist weniger sicher als Kerberos.) Sie können **SupportMultipleForestDdcLookup** anstelle von **SupportMultipleForest** verwenden. Sie können **SupportMultipleForest** zur Gewährleistung von Abwärtskompatibilität weiterverwenden. Der Registrierungsschlüssel **SupportMultipleForestDdcLookup** steuert, wie VDAs Delivery Controller suchen. Weitere Informationen finden Sie unter Bereitstellen in einer Active Directory-Umgebung mit mehreren Gesamtstrukturen. [CVADHELP-15467]
- Wenn ein VDA versucht, sich bei einem Delivery Controller zu registrieren, führt der Brokeragent eine erste DNS-Suche in der lokalen Domäne durch. Diese Suche stellt sicher, dass der Delivery

Controller erreichbar ist. Wenn die DNS-Suche fehlschlägt, führt der Brokeragent Top-Down-Abfragen in Active Directory zurück zur wiederholten Suche in allen Domänen durch. Wenn die Adresse des Delivery Controllers ungültig ist (z. B. weil der Administrator den FQDN bei der VDA-Installation falsch eingegeben hat), können diese Abfragen eine DDoS-ähnliche Wirkung auf dem Domänencontroller haben. Weitere Informationen finden Sie unter Controllersuche während der VDA-Registrierung. [CVADHELP-15484]

- Wenn die Zeitzonenrichtlinie auf **Serverzeitzone verwenden** festgelegt ist, wird die Clientzeitzone möglicherweise dennoch über eine Benutzersitzung auf einem VDA umgeleitet. [CVADHELP-15628]
- Wenn die Legacygrafikmodus-Richtlinie aktiviert ist, wird bei Sitzungsstart möglicherweise ein grauer Bildschirm angezeigt. Dieses Problem tritt bei VDA-Version 7.15.6000 auf. [CVADHELP-15841]
- Auf Server-VDI-VDAs bietet die Schaltfläche Ein/Aus im Startmenü möglicherweise nicht die Option Trennen. [CVADHELP-16595]

Systemausnahmen

- Nach einem VDA-Upgrade von Version 7.15 CU 5 auf CU 6 oder Version 2003 wird die Gruppenrichtlinienengine (CseEngine.exe) möglicherweise unerwartet beendet. [CVADHELP-14515]
- Der Citrix Audioumleitungsdienst (CtxAudioSvc) wird möglicherweise unerwartet beendet und es wird eine Ereignis-ID 1000 und ein Ausnahmecode 0x0c0000005 angezeigt. Das Problem tritt aufgrund eines Fehlers im Modul CtxVorbisDmo64.dll auf. [CVADHELP-14898]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode APC_INDEX_MISMATCH (1) kommen. Das Problem tritt auf, wenn Sie versuchen, auf ein zugeordnetes Clientlaufwerk zuzugreifen. [CVADHELP-15003]
- Auf VDAs kann es in tdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x1000007e kommen. Das Problem tritt auf, wenn Sie eine Sitzung über die Citrix Workspace-App für HTML5 starten. [CVADHELP-15220]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x93 (INVALID_KERNEL_HANDLE) kommen. [CVADHELP-15326]
- Wenn Sie versuchen, eingebettete Windows Media-Dateien in einer Webanwendung anzuzeigen, wird Internet Explorer möglicherweise unerwartet beendet. Das Problem tritt aufgrund des fehlerhaften Moduls HostMMTransport.dll auf. [CVADHELP-15598]

VDA für Serverbetriebssystem

Sitzung/Verbindung

- Wenn mehrere USB-Geräte an eine Sitzung umgeleitet werden, funktioniert eines von ihnen möglicherweise nicht ordnungsgemäß. [CVADHELP-12516]
- Wenn Sie in einer Site, in der XenApp und XenDesktop Version 7.15 LTSR CU 4 unter Microsoft Windows Server 2016 ausgeführt wird, eine veröffentlichte Anwendung starten, reagiert die Anwendungssitzung möglicherweise nicht mehr. Die folgende Fehlermeldung wird angezeigt:

  Bitte warten Sie auf den lokalen Sitzungsmanager…

  [CVADHELP-13967]
- Wenn die Richtlinie **Allow the audio sandbox to run** aktiviert ist, funktioniert Audio in Google Chrome, wenn es über Citrix Virtual Apps and Desktops geöffnet wurde, möglicherweise nicht. [CVADHELP-14784]
- Die Lizenzstatistik ist von Site zu Site möglicherweise inkonsistent. Beispielsweise kann eine Diskrepanz zwischen den verbrauchten Citrix CCU-Lizenzen und den eindeutigen Benutzern für mehrere Sites zugewiesenen Lizenzen auftreten. [CVADHELP-14950]
- Dieser Fix bietet einen Timer zum Senden eines kleinen Datagramms über eine UDP-Verbindung, um die Verbindung zwischen Host und Client aufrechtzuerhalten.

  Zum Implementieren dieses Fixes legen Sie den Registrierungsschlüssel wie folgt fest:

  - *32-Bit-Systeme*

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

    Name: KeepAliveTimer

    Typ: DWORD

    Wert: Intervall (in Sekunden) zwischen den Keep-Alive-Meldungen. Wird kein Wert angegeben oder der Wert auf 0 gesetzt, werden keine Keep-Alive-Pakete gesendet und das Keep-Alive-Feature funktioniert nicht. Der empfohlene Wert ist 15.
  - *64-Bit-Systeme*

    HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

    Name: KeepAliveTimer

    Typ: DWORD

    Wert: Intervall (in Sekunden) zwischen den Keep-Alive-Meldungen. Wird kein Wert angegeben oder der Wert auf 0 gesetzt, werden keine Keep-Alive-Pakete gesendet und das Keep-Alive-Feature funktioniert nicht. Der empfohlene Wert ist 15.

[CVADHELP-15122]

- Wenn der CtxUvi Hooking-Treiber deaktiviert ist, werden möglicherweise keine Ereignisprotokolle generiert. Das Problem tritt auf, wenn nur wenige Systemressourcen verfügbar sind. [CVADHELP-15241]
- Microsoft Teams kann bei einer Taktabweichung möglicherweise nicht im optimierten Modus geladen werden. Die Abweichung führt zu einem ungültigen oder abgelaufenen Citrix Zertifikat. Ändern Sie als Workaround den Starttyp des HTML5-Videoumleitungsdiensts (txHdxWebSocketService) von **Automatisch** in **Automatisch (verzögerter Start)**. [CVADHELP-15298]
- Dieser Fix bietet Unterstützung für ein neues Feature, mit dem Sie mehrere Gesamtstrukturbereitstellungen konfigurieren können, ohne die NTLM-Authentifizierung für VDAs zu aktivieren. Das frühere Feature zur Aktivierung der NTLM-Authentifizierung ist jedoch anderen Bereitstellungen ohne Vertrauensstellung vorbehalten. Ein Registrierungseintrag **SupportMultipleForestDdcLookup** wird hinzugefügt, um eine unerwünschte Aktivierung der NTLM-Authentifizierung auf VDAs zu verhindern. (NTLM ist weniger sicher als Kerberos.) Sie können **SupportMultipleForestDdcLookup** anstelle von **SupportMultipleForest** verwenden. Sie können **SupportMultipleForest** zur Gewährleistung von Abwärtskompatibilität weiterverwenden. Der Registrierungsschlüssel **SupportMultipleForestDdcLookup** steuert, wie VDAs Delivery Controller suchen. Weitere Informationen finden Sie unter Bereitstellen in einer Active Directory-Umgebung mit mehreren Gesamtstrukturen. [CVADHELP-15467]
- Wenn ein VDA versucht, sich bei einem Delivery Controller zu registrieren, führt der Brokeragent eine erste DNS-Suche in der lokalen Domäne durch. Diese Suche stellt sicher, dass der Delivery Controller erreichbar ist. Wenn die DNS-Suche fehlschlägt, führt der Brokeragent Top-Down-Abfragen in Active Directory zurück zur wiederholten Suche in allen Domänen durch. Wenn die Adresse des Delivery Controllers ungültig ist (z. B. weil der Administrator den FQDN bei der VDA-Installation falsch eingegeben hat), können diese Abfragen eine DDoS-ähnliche Wirkung auf dem Domänencontroller haben. [CVADHELP-15484]
- Eine ungültige XenApp-Sitzung kann auf einem VDA für Serverbetriebssysteme beginnen, wenn eine Remotedesktopsitzung getrennt und wiederverbunden wird. Die ungültige Sitzung bleibt bestehen, bis Sie den VDA neu starten. [CVADHELP-16453]

Systemausnahmen

- Der Diensthost (svchost.exe)-Prozess, der den Windows-Audiodienst hostet, wird möglicherweise unerwartet in einer Benutzersitzung beendet. Das Problem tritt aufgrund eines Speicherverlusts auf. [CVADHELP-13687]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode APC_INDEX_MISMATCH (1) kommen. Das Problem tritt auf, wenn Sie versuchen,

auf ein zugeordnetes Clientlaufwerk zuzugreifen. [CVADHELP-15003]

- Auf VDAs kann es in tdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x1000007e kommen. Das Problem tritt auf, wenn Sie eine Sitzung über die Citrix Workspace-App für HTML5 starten. [CVADHELP-15220]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x93 (INVALID_KERNEL_HANDLE) kommen. [CVADHELP-15326]
- Wenn Sie versuchen, eingebettete Windows Media-Dateien in einer Webanwendung anzuzeigen, wird Internet Explorer möglicherweise unerwartet beendet. Das Problem tritt aufgrund des fehlerhaften Moduls HostMMTransport.dll auf. [CVADHELP-15598]
- Wenn Sie versuchen, die Verbindung zu einer multiportfähigen TCP-Sitzung wiederherzustellen, die über die Citrix Workspace-App für Linux gestartet wurde, wird der VDA möglicherweise unerwartet beendet. [CVADHELP-15674]

Virtual Desktop-Komponenten –Sonstiges

- Wenn Sie eine App-V-Anwendung von einem VDA starten, der viele App-V-Anwendungen hostet, wird die Registrierung des VDAs möglicherweise aufgehoben. Das Problem tritt auf, wenn die Verarbeitung zugeordneter Richtliniendateien zu lange dauert. [CVADHELP-12592]
- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX285059. [CVADHELP-14755]

Kumulatives Update 6 (CU6)

September 16, 2021

Releasedatum: 30. Juni 2020

Info zu diesem Release

Das kumulative Update 6 (CU6) für XenApp und XenDesktop 7.15 LTSR behebt über 94 seit 7.15 LTSR CU5 gemeldete Probleme.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR CU5 behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Download von 7.15 LTSR CU6

> **Wichtig:**
>
> Dieses Release weist Änderungen an der Art und Weise der Installation und des Upgrades von StoreFront auf. Wenn Sie in früheren Releases auf der Hauptseite des Komplettinstallationsprogramms auf die Kachel **Erste Schritte** geklickt haben, wurde auf der Seite **Kernkomponenten** auch StoreFront aufgeführt. Sie können StoreFront und andere Kernkomponenten zur Installation auf derselben Maschine auswählen.
>
> Ab diesem Release enthält die Seite **Kernkomponenten** kein Kontrollkästchen für StoreFront mehr. Um StoreFront zu installieren oder zu aktualisieren, klicken Sie auf der Hauptseite im Bereich **Bereitstellung erweitern** auf **Citrix StoreFront**. Damit wird `CitrixStoreFront-x64.exe` auf dem Installationsmedium gestartet.
>
> In dem Befehl `XenDesktopServerSetup.exe` können Sie `/components storefront` nicht mehr angeben. Andernfalls schlägt der Befehl fehl. Führen Sie zum Installieren von StoreFront über die Befehlszeile `CitrixStoreFront-x64.exe` aus. Die Datei ist im Ordner `x64` des Citrix Virtual Apps and Desktops-Installationsmediums.
>
> **Wichtig:**
>
> Die Citrix License Administration Console hat das Ende des Lebenszyklus und das Ende der Unterstützung in Lizenzserver 11.16.3.0 Build 30000 erreicht. Verwenden Sie den Citrix Licensing Manager.

Neue Bereitstellungen

Wie stelle ich das CU6 von Grund auf bereit

Mit dem CU6-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf dem CU6 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU6 umfasst Updates für Basiskomponenten von 7.15 LTSR. Citrix empfiehlt die Aktualisierung aller LTSR-Komponenten Ihrer Bereitstellung auf CU6. Beispiel: Wenn Provisioning Services zur LTSR-Bereitstellung gehört, aktualisieren Sie die Provisioning Services-Komponenten auf die CU6-Version. Wenn Provisioning Services nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU6

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.6000	
VDA für Serverbetriebssystem	7.15.6000	
Citrix Studio	7.15.6000	
Citrix Director	7.15.6000	
Delivery Controller	7.15.6000	
Citrix Verbundauthen-tifizierungsdienst	7.15.6000	
Citrix Gruppenrichtlinienverwaltung	3.1.6000	
Citrix Gruppenrichtlinie - clientseitige Erweiterung	3.1.6000	
Linux VDA	7.15.5000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15.6000	
Provisioning Services	7.15.27	
Sitzungsaufzeichnung	7.15.6000	Nur Premium Edition
StoreFront	3.12.6000	
Universeller Druckserver	7.15.6000	

XenApp und XenDesktop 7.15 LTSR CU6-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU6 kompatible Komponenten und Plattformen	Version
App Layering	1903
*Browserinhaltsumleitung	15.15
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.4.3000
Lizenzserver	11.16.6.0 Build 31000
Self-Service-Kennwortzurücksetzung	1.1.20.0
Workspace Environment Management	1906.0.1.1

*Browserinhaltsumleitung

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonymisierte Informationen über den Installationsvorgang

gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren oder aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp 7.15 CU6. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der Kernkomponenten von XenApp 7.15 LTSR CU6 und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU6-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU6-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU6-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

August 18, 2021

Citrix Director

- Wenn Sie sich nach dem Neustart der Internetinformationsdienste (IIS) das erste Mal bei Citrix Director anmelden, wird auf der Seite **Trends** möglicherweise folgende Fehlermeldung angezeigt:

Keine Details verfügbar.

[CVADHELP-12426]

- Das Senden einer Nachricht an mehrere Benutzer kann fehlschlagen und die folgende Fehlermeldung wird angezeigt:

  Nachricht kann nicht gesendet werden. Unerwarteter Serverfehler. Weitere Informationen finden Sie in den Serverereignisprotokollen von Director.

  [CVADHELP-12601]

- Wenn Citrix Director versucht, eine E-Mail-Konfiguration mit einem SMTP-Server einzurichten, wird möglicherweise folgende Fehlermeldung angezeigt:

  Ungültiger E-Mail-Server

  [CVADHELP-14449]

- Wenn Sie versuchen, einen E-Mail-Server auf einem eigenständigen Server mit Citrix Director zu konfigurieren, wird möglicherweise folgende Fehlermeldung angezeigt:

  Ungültiger E-Mail-Server.

  Das Problem tritt auf, wenn Sie den E-Mail-Server für Warnungen und Benachrichtigungen konfigurieren. [CVADHELP-14648]

Citrix Richtlinie

- Server werden möglicherweise getrennt und reagieren erst wieder, wenn Sie die Gruppenrichtlinienengine (CseEngine.exe) neu starten. [CVADHELP-12987]

Citrix Studio

- Das Starten einer App-V-Anwendung kann fehlschlagen und die folgende Fehlermeldung wird angezeigt:

  Fehler beim Start

  Das Problem tritt auf, wenn große App-V-Pakete unvollständig an VDAs gestreamt werden. [CVADHELP-12889]

- Wenn Sie Citrix Studio von Version 7.6 auf Version 7.15 aktualisieren, kann es länger dauern, einige Assistenten (z. B. Maschinenkatalog und Bereitstellungsgruppe) zu öffnen. [CVADHELP-13267]

- Wenn Sie App-V-Pakete in Citrix Studio hinzufügen, zeigen einige Pakete u. U. nur Standardsymbole (und keine benutzerdefinierten Symbole). [CVADHELP-13338]

- Beim Versuch, in Citrix Studio Geräte aus einer PVS-Sammlung zu einem Katalog hinzuzufügen, werden möglicherweise alle Zielgeräte aufgelistet, also auch Maschinen, die bereits im Katalog vorhanden sind. [CVADHELP-13403]
- Beim Versuch, für eine vorhandene App, die einer Anwendungsgruppe zugewiesen ist, den Pfad zur ausführbaren Datei oder den Symbolspeicherort zu ändern, wird möglicherweise folgende Fehlermeldung angezeigt:

  Maschinen in der Bereitstellungsgruppe können nicht durchsucht werden. Möchten Sie stattdessen die lokale Maschine durchsuchen?

  [CVADHELP-14199]
- Wenn Sie Studio als veröffentlichte App ausführen, hört es möglicherweise auf zu reagieren. [CVADHELP-14207]

Delivery Controller

- Der Versand von Nachrichten über Citrix Director an viele Benutzer kann fehlschlagen. Die folgende Fehlermeldung wird angezeigt:

  Nachricht kann nicht gesendet werden. Die Datenquelle reagiert nicht oder hat einen Fehler gemeldet.

  Der Fix soll das Auftreten dieses Problems minimieren.

  [CVADHELP-12066]
- Beim Anzeigen benutzerdefinierter Berichte für Anwendungsinstanzen in Citrix Director werden in einigen Feldern u. U. Nullwerte anstelle der Endzeiten der Anwendung angezeigt. [CVADHELP-12733]
- Die Anwendungsauflistung kann auf dem SQL-Server mit der Sitekonfigurationsdatenbank zu einem starken Anstieg der CPU-Last führen. [CVADHELP-13043]
- Das Bereinigen von Ressourcenauslastungsdaten aus einer Tabelle in der Überwachungsdatenbank kann zu einem Ausführungstimeout führen und fehlschlagen. [CVADHELP-13075]
- Wenn das **Wake-On-LAN-Feature von Remote-PC-Zugriff** für einen Maschinenkatalog aktiviert ist, stellt der lokale Hostcache möglicherweise die Synchronisierung ein. Das Problem tritt bei Verwendung von Microsoft System Center Configuration Manager als Hostingverbindung auf. [CVADHELP-13122]
- Eine virtuelle Maschine, auf der eine Benutzersitzung ausgeführt wird, kann unerwartet heruntergefahren werden. Das Problem tritt auf, wenn das Feature zur automatischen Wiederverbindung des Client eine in der Datenbank ausstehende Energieaktion Löschen nicht auslöst. [CVADHELP-13165]

- Nach dem Ende der Sommerzeit im Jahr 2019 und Konfigurieren des Neustart-Zeitplans trat nur für die Bereitstellungsgruppe ein unerwarteter geplanter Neustart auf. [CVADHELP-13486]
- Wenn Sie Administratoren anderer Domänen in Citrix Studio hinzufügen, wird möglicherweise folgende Fehlermeldung in Studio angezeigt:

  Fehler: Validieren des Speicherorts des zentralen Konfigurationsdienstes fehlgeschlagen.

  Sie verfügen nicht über die nötigen Berechtigungen, um diese Site mit Studio zu verwalten, oder es ist ein Problem mit der delegierten Administration aufgetreten.

  Das Problem tritt auf, wenn ein Domänencontroller in einer der Domänen nicht erreichbar ist. [CVADHELP-13651]
- Wenn Sie mit **udadmin** einen Lizenzserverbericht generieren, zeigt der Bericht möglicherweise an, dass die Lizenzen mehrmals demselben Gerät ausgestellt sind. Das Problem tritt auf, wenn verschiedene Geräte mit den richtigen Hardware-IDs gegen doppelte Namen aktualisiert werden. Das Problem hat keinen Einfluss auf den Lizenzverbrauch, sondern nur auf den Bericht. [CVADHELP-13763]
- Daten im lokalen Hostcache (LHC) verschwinden möglicherweise nach dem Start des Downloads. Die alten Dateien bleiben daher erhalten oder die LHC-Dateien werden nicht am Speicherort angezeigt: C:\Windows\ServiceProfiles\NetworkService. [CVADHELP-13980]
- Der Versuch, eine synchronisierte Konfiguration in die lokale Hostcachedatenbank zu importieren, kann wiederholt mit Fehler 505 fehlschlagen. [CVADHELP-14237]
- Nach dem Upgrade von XenApp and XenDesktop 7.15 Cumulative Update 1 auf das Cumulative Update 3 kann der Versuch, den lokalen Hostcache (LHC) zu importieren, mit Fehler 505 fehlschlagen. [CVADHELP-14429]

Verbundauthentifizierungsdienst

- Die GUI unterstützt keine Server mit mehreren Zertifizierungsstellen. [CVADHELP-11919]

Linux Virtual Delivery Agent

Linux Virtual Delivery Agent 7.15 LTSR CU6 Dokumentation enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

- Versuche, ein Benutzerprofil unter Microsoft Windows 10 Version 2004 zu erstellen, schlagen möglicherweise fehl. [CVADHELP-14235]

- Wenn Sie sich mit einem temporären Profil bei einer Sitzung anmelden, wird möglicherweise unter C:\Users ein leerer Benutzerprofilordner erstellt. Die Profilverwaltung löscht das temporäre Profil bei der Abmeldung und hinterlässt den leeren Benutzerprofilordner. [CVADHELP-14297]
- Wenn die Richtlinie zur Umleitung des Ordners AppData(Roaming) aktiviert ist, verschwinden einige Kacheln möglicherweise aus dem Startmenü. Das Problem tritt auf, wenn Sie sich an einer Maschine mit Windows Server 2016 oder 2019 anmelden, auf der Citrix Virtual Apps and Desktops 1912 oder früher ausgeführt wird. [CVADHELP-14336]
- Wenn die Richtlinie **Anmeldeausschlussprüfung** aktiviert ist, synchronisiert die Profilverwaltung Dateien unter einem ausgeschlossenen Ordner möglicherweise nicht. Stattdessen löscht oder ignoriert die Profilverwaltung die Dateien bei der Anmeldung möglicherweise. Das Problem tritt bei Dateien auf, die Pfaden mit Platzhaltern in der **Liste der zu synchronisierenden Dateien** entsprechen. [CVADHELP-14347]

Provisioning Services

Provisioning Services 7.15 LTSR CU6 enthält Informationen zu den Updates in diesem Release.

StoreFront

- Wenn das StoreFront Version 3.12 CU 3 mit der SAML-Authentifizierung und einer komplexen AD-Architektur mit mehreren Domänen konfiguriert wird, kann der Verbundauthentifizierungsdienst (FAS) eine Anwendung möglicherweise nicht starten. Die folgende Fehlermeldung wird angezeigt:

  App kann nicht gestartet werden.

  Das Problem tritt auf, wenn der FAS für einen Store aktiviert ist.

  [CVADHELP-12865]
- Wenn Sie die StoreFront Verwaltungskonsole mit SAML-Authentifizierung konfigurieren und die IdP-URL (für PingID) in das Adressfeld eingeben, werden diese Änderungen möglicherweise nicht gespeichert. Die folgende Fehlermeldung wird angezeigt:

  Ein Fehler ist aufgetreten beim Speichern der Änderungen.

  [CVADHELP-13373]
- Die SAML-Authentifizierung (Security Assertion Markup Language) schlägt möglicherweise fehl, wenn Sie eine Anwendung eines Drittanbieters als Identitätsanbieter (IdP) verwenden.

  Die folgende Fehlermeldung wird angezeigt:

Im Zusammenhang mit dem zugeordneten Konto ist ein Fehler aufgetreten.

[CVADHELP-13396]

- Ist eine benutzerdefinierte Konfigurationsdatei im Store-Ordner, ersetzt sie möglicherweise den Inhalt der web.config-Datei im Store-Ordner. Das Problem tritt auf, wenn Sie StoreFront aktualisieren. [CVADHELP-13485]
- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. [CVADHELP-13602]
- Upgrades, die 2.6, 3.0.1, 3.5, 3.8 in ihrem Upgradeverlauf auf 3.12 CU* und höher enthalten, können fehlschlagen, wenn der Citrix StoreFront Protocol Transition-Dienst den Status **Angehalten** hat. [CVADHELP-13626]
- Wenn Sie sich bei StoreFront anmelden, dauert das Enumerieren der Anwendungen möglicherweise lange. Das Problem tritt auf, wenn Sie Ihren Benutzernamen im Format **domäne\benutzername** eingeben und die Benutzerauthentifizierung an Delivery Controller delegiert wird. [CVADHELP-13891]
- In der StoreFront-Konsole können Versuche, Domänennamen mit einem Unterstrich (_) zu einer Liste vertrauenswürdiger Domänen hinzuzufügen, fehlschlagen. [CVADHELP-14213]
- Dieser Fix behebt ein Sicherheitsrisiko in einer Hintergrundkomponente. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX277455. [LCM-7272]
- Wenn Sie einen Delivery Controller installieren, wird StoreFront möglicherweise nicht automatisch auch installiert. Um es zu installieren, verwenden Sie die Citrix StoreFront-Option im Metainstallationsprogramm für Citrix Virtual Apps and Desktops. [LCM-7335]

Universeller Druckserver

Client

- Aufgrund einer Zugriffsverletzung wird der universelle Druckserver (UPServer.exe) möglicherweise unerwartet beendet. [CVADHELP-10627]
- Beim Druckspooler-Dienst (spoolsv.exe) kann ein Deadlock auftreten. Dokumente können dann nicht gedruckt und Microsoft Office-Anwendungen werden nicht gestartet. [CVADHELP-13315]
- Beim Start einer Anwendung wird der Citrix Druckmanagerdienst (CpSvc.exe) möglicherweise unerwartet beendet. [CVADHELP-13945]
- Der Druckspoolerdienst wird möglicherweise unerwartet beendet. [CVADHELP-13954]

Server

- Aufgrund einer Zugriffsverletzung wird der universelle Druckserver (UPServer.exe) möglicherweise unerwartet beendet. [CVADHELP-10627]
- Der universelle Druckserver (UPServer.exe) wird möglicherweise unerwartet beendet. Das Problem tritt aufgrund des fehlerhaften Moduls prntvpt.dll auf. [CVADHELP-12651]

VDA für Desktopbetriebssystem

Tastatur

- Wenn das Citrix-Feature für den generischen Client-IME (Eingabemethoden-Editor) aktiviert ist, kann eine Anwendung unerwartet beendet werden, wenn Sie mit dem chinesischen Client-IME Sonderzeichen und Zahlen in der Anwendung eingeben. Das Problem tritt in Desktop- und App-Sitzungen auf, die unter Microsoft Windows 10 Version 1809 und Windows Server 2019 ausgeführt werden. [CVADHELP-13961]

Installieren, Deinstallieren und Aktualisieren

- Beim Upgrade eines VDAs wird der Registrierungsschlüssel **MaxVideoMemoryBytes** möglicherweise auf den Standardwert zurückgesetzt. [CVADHELP-13629]
- Wenn Sie einen VDA aktualisieren, können Sie die Funktion **Leistung optimieren** auf der Seite **Features** nicht deaktivieren. Außerdem können Sie keine anderen Features auf dieser Seite aktivieren. [CVADHELP-14560]

Drucken

- Nach dem Upgrade eines VDAs auf Version 7.15 - Kumulatives Update 4 wird der Citrix Druckmanagerdienst (CpSvc.exe) möglicherweise unerwartet beendet. [CVADHELP-12888]
- Beim Start einer Anwendung wird der Citrix Druckmanagerdienst (CpSvc.exe) möglicherweise unerwartet beendet. [CVADHELP-13945]

Sitzung/Verbindung

- Wenn Sie eine dedizierte Desktopsitzung starten, tritt möglicherweise ein Anmeldefehler auf, und der Abmeldeprozess kann hängen bleiben. In Citrix Studio wird die Sitzung als verbunden angezeigt, Sie können sich jedoch erst abmelden, wenn Sie die Maschine manuell neu starten. [CVADHELP-10931]

- Wenn Windows Media Player in der Playlist von einem Titel zum nächsten wechselt, fehlt zu Beginn des nächsten Titels möglicherweise die Audiowiedergabe. Das Problem tritt auf, wenn die Windows Media-Umleitung aktiviert ist. [CVADHELP-11639]
- Werden Audiogeräte einer Benutzersitzung hinzugefügt, ist mit Ausnahme von Skype for Business keine Tonausgabe von diesen Geräten zu hören. Die folgende Fehlermeldung wird angezeigt:

  Error - no more device slots available - failed to add the device.

  Das Problem tritt auf, wenn mehr als acht Wiedergabe- oder Aufzeichnungsgeräte an einen Endpunkt angeschlossen sind. [CVADHELP-12760]
- Sitzungsroaming funktioniert auf einem VDA möglicherweise nicht. Das Problem tritt bei Dell Wyse-Thin Clients auf. [CVADHELP-13003]
- Beim erneuten Verbinden mit einer aktiven Sitzung auf einer anderen Maschine fehlen möglicherweise umgeleitete Drucker und Clientlaufwerke. Das Problem tritt auf, wenn Sie von einer Maschine zur nächsten wechseln, ohne die aktive Benutzersitzung zu sperren oder zu trennen. [CVADHELP-13035]
- Wenn Sie auf die Schaltfläche **Abbrechen** klicken, wenn eine Anwendung Video mit einer Webcam aufzeichnet, hört die Anwendung möglicherweise auf zu reagieren. Das Problem tritt aufgrund des fehlerhaften Moduls MFDeviceSource.dll auf. [CVADHELP-13062]
- Das Lesen von Daten von einem Clientlaufwerk kann länger dauern, nachdem Sie auf einem VDA den Wert für folgenden Registrierungsschlüssel in 1 ändern:

  Um sie zu aktivieren, fügen Sie den folgenden Registrierungsschlüssel hinzu:

  HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Control\ Terminal Server\ Wds\ icawd

  Name: PacketIntegrityChecks

  Typ: DWORD

  Wert: 1

  [CVADHELP-13063]
- Bei Aufzeichnen einer Sitzung in der Citrix Workspace-App für Windows werden Bewegungen des Mauszeigers möglicherweise nicht aufgezeichnet. Das Problem tritt mit VDA-Version 7.15.400 auf. [CVADHELP-13300]
- Das Starten einer Sitzung auf einem VDA kann fehlschlagen, wenn Sie den Schwachstellenscanner einiger Drittanbieter verwenden. [CVADHELP-13306]
- Ein VDA reagiert nach dem Neustart möglicherweise nicht mehr. Das Problem tritt auf, wenn durch Sicherheitssoftware wie Symantec SEP ein Sicherheitsscan erzwungen wird. [CVADHELP-13832]

- Teile eines Anwendungsfensters können transparent werden, was dazu führt, dass die Anwendung im Hintergrund statt im Vordergrund ausgeführt wird. Das Problem tritt im Seamless-modus auf. [CVADHELP-13903]
- In einer Umgebung mit mehreren Bildschirmen werden Anwendungen möglicherweise nicht konsistent auf demselben Bildschirm angezeigt. Das Problem tritt auf, wenn Sie zu einer neuen Arbeitsstation wechseln. [CVADHELP-13657]

Smartcards

- Nach dem Konfigurieren der Smartcard-Authentifizierung in Windows 10 kann die Passthrough-Authentifizierung mit Smartcards fehlschlagen, wenn Sie einen Desktop in einer Benutzersitzung starten. Das Problem tritt auf, wenn Sie einen Desktop von einem Thin Client starten. [CVADHELP-11757]

Systemausnahmen

- Bei der USB-Umleitung kann auf VDAs eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** auftreten. Außerdem wird möglicherweise die globale Sperre für USB-Umleitungen nicht aufgehoben, wodurch andere Umleitungen blockiert werden. [CVADHELP-9237]
- Auf VDAs kann es bei ctxdvcs.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-13000]
- Auf VDAs kann es in ctxdvcs.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0xc0000409 kommen. [CVADHELP-13102]
- Eine Anwendung, die das Electron-Framework verwendet, wird möglicherweise unerwartet beendet und es wird folgende Fehlermeldung angezeigt:

  {EXCEPTION} Illegal Instruction An attempt was made to execute an illegal instruction.

  [CVADHELP-13440]

Benutzeroberfläche

- Die Registerkarte "Geräte"fehlt möglicherweise im Fenster **Citrix Workspace** –**Voreinstellungen** (**Desktop Viewer-Symbolleiste > Einstellungen**). Das Problem tritt bei einem VDI-Desktop auf, der unter Microsoft Windows Server über einen Server VDI-Switch ausgeführt wird. [CVADHELP-14158]

VDA für Serverbetriebssystem

Tastatur

- Wenn das Citrix-Feature für den generischen Client-IME (Eingabemethoden-Editor) aktiviert ist, kann eine Anwendung unerwartet beendet werden, wenn Sie mit dem chinesischen Client-IME Sonderzeichen und Zahlen in der Anwendung eingeben. Das Problem tritt in Desktop- und App-Sitzungen auf, die unter Microsoft Windows 10 Version 1809 und Windows Server 2019 ausgeführt werden. [CVADHELP-13961]

Drucken

- Nach dem Upgrade eines VDAs auf Version 7.15 - Kumulatives Update 4 wird der Citrix Druckmanagerdienst (CpSvc.exe) möglicherweise unerwartet beendet. [CVADHELP-12888]
- Das Verwenden eines anderen Ausgabefachs beim Drucken von Dokumenten kann fehlschlagen. Es wird das Standardausgabefach verwendet, selbst wenn Sie im Dialogfeld "Drucken"ein anderes Fach auswählen. [CVADHELP-13492]
- Beim Start einer Anwendung wird der Citrix Druckmanagerdienst (CpSvc.exe) möglicherweise unerwartet beendet. [CVADHELP-13945]

Sitzung/Verbindung

- Wenn Windows Media Player in der Playlist von einem Titel zum nächsten wechselt, fehlt zu Beginn des nächsten Titels möglicherweise die Audiowiedergabe. Das Problem tritt auf, wenn die Windows Media-Umleitung aktiviert ist. [CVADHELP-11639]
- Wenn Sie eine veröffentlichte Anwendung auf einem VDA für Serverbetriebssysteme starten, wird der Registrierungsschlüssel "Windows RunOnce"möglicherweise nicht ausgeführt. [CVADHELP-11991]
- Ein Delivery Controller zeigt möglicherweise ungültige Sitzungsinformationen an. Das Problem tritt auf, wenn von einem VDA an den Delivery Controller gesendete Sitzungsinformationen die IP-Adresse 127.0.0.1 enthalten. [CVADHELP-12767]
- Versuche, eine Anwendung zu starten, schlagen möglicherweise fehl. Der **Task-Manager** enthält keine Sitzungsdetails und in Citrix Studio wird folgender Anwendungsstatus angezeigt: **Anwendung wird nicht ausgeführt**. Wenn das Problem auftritt, wird der VDA möglicherweise erneut registriert und die folgende Fehlermeldung wird angezeigt:

  Ereignis-ID 1048: WCF-Fehler oder Ablehnung durch Broker

  [CVADHELP-12856]

- Beim Hervorheben von Text in einer Benutzersitzung können Leistungsprobleme auftreten. Das Problem tritt in Microsoft Outlook Version 2016 auf, das auf einem veröffentlichten Desktop ausgeführt wird.

  Um sie zu aktivieren, fügen Sie den folgenden Registrierungsschlüssel hinzu:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\

  Name: CursorShapeChangeMinInterval

  Typ: DWORD

  Wert: 10 bis 100. Empfohlener Wert: 50 Der Standardwert ist 0 (= deaktiviert).

  [CVADHELP-12886]

- Wenn Sie auf die Schaltfläche **Abbrechen** klicken, wenn eine Anwendung Video mit einer Webcam aufzeichnet, hört die Anwendung möglicherweise auf zu reagieren. Das Problem tritt aufgrund des fehlerhaften Moduls MFDeviceSource.dll auf. [CVADHELP-13062]
- Das Lesen von Daten von einem Clientlaufwerk kann länger dauern, nachdem Sie auf einem VDA den Wert für folgenden Registrierungsschlüssel in 1 ändern:

  Um sie zu aktivieren, fügen Sie den folgenden Registrierungsschlüssel hinzu:

  HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Control\ Terminal Server\ Wds\ icawd

  Name: PacketIntegrityChecks

  Typ: DWORD

  Wert: 1

  [CVADHELP-13063]

- Bei Aufzeichnen einer Sitzung in der Citrix Workspace-App für Windows werden Bewegungen des Mauszeigers möglicherweise nicht aufgezeichnet. Das Problem tritt mit VDA-Version 7.15.400 auf. [CVADHELP-13300]
- Die Abmeldung von einer Sitzung mit Citrix Studio und Citrix Director kann fehlschlagen, wenn eine veröffentlichte Anwendung in der Sitzung gestartet wurde. [CVADHELP-13307]
- In einer Umgebung mit mehreren Bildschirmen werden Anwendungen möglicherweise nicht konsistent auf demselben Bildschirm angezeigt. Das Problem tritt auf, wenn Sie zu einer neuen Arbeitsstation wechseln. [CVADHELP-13657]
- Ein VDA reagiert nach dem Neustart möglicherweise nicht mehr. Das Problem tritt auf, wenn durch Sicherheitssoftware wie Symantec SEP ein Sicherheitsscan erzwungen wird. [CVADHELP-13832]
- Teile eines Anwendungsfensters können transparent werden, was dazu führt, dass die Anwendung im Hintergrund statt im Vordergrund ausgeführt wird. Das Problem tritt im Seamlessmodus auf. [CVADHELP-13903]

- Nach einer Netzwerkunterbrechung funktioniert die COM-Port-Umleitung u. U. nicht, nachdem die Verbindung zu einer Sitzung durch die automatische Client-Wiederverbindung (ACR) wiederhergestellt wurde. [CVADHELP-13926]
- Nachdem ein VDA aufgrund einer hohen Speicherauslastung Volllast meldet, bleibt der Lastindexwert möglicherweise bei 10.000, selbst wenn die Speicherauslastung auf einen niedrigen Wert abfällt. [CVADHELP-14563]
- Wenn Sie eine Seamlesssitzung sperren, kann das Anmeldefenster, unabhängig von der Größe des Sitzungsfensters, den gesamten Bildschirm abdecken. Es besteht dann kein Zugang zum Desktop und anderen Anwendungen des Endpunkts. [CVADHELP-14589]

Smartcards

- Die Passthrough-Authentifizierung mit Smartcards schlägt möglicherweise zeitweise fehl. Das Problem tritt auf, wenn Sie eine HDX-Sitzung unter Windows Server 2016 starten. [CVADHELP-13054]

Systemausnahmen

- Bei der USB-Umleitung kann auf VDAs eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** auftreten. Außerdem wird möglicherweise die globale Sperre für USB-Umleitungen nicht aufgehoben, wodurch andere Umleitungen blockiert werden. [CVADHELP-9237]
- Auf VDAs kann es bei ctxdvcs.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [CVADHELP-13000]
- Auf VDAs kann es in ctxdvcs.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0xc0000409 kommen. [CVADHELP-13102]
- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei icardd.dll mit einem Bluescreen und mit Bugcheckcode 0x0000003B kommen. [CVADHELP-13330]
- Eine Anwendung, die das Electron-Framework verwendet, wird möglicherweise unerwartet beendet und es wird folgende Fehlermeldung angezeigt:

  {EXCEPTION} Illegal Instruction An attempt was made to execute an illegal instruction.

  [CVADHELP-13440]
- In dem Service Host-Prozess (svchost.exe) oder in wfshell.exe kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls icaendpoint.dll auf. [CVADHELP-14276]

- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 kommen. [CVADHELP-14332]
- Auf einem Gerät mit mehr als neun Bildschirmen kann der Start einer Benutzersitzung mit einer schwerwiegenden Ausnahme, Bluescreen und Bugcheckcode 0x3B fehlschlagen. [CVADHELP-14775]

Virtual Desktop-Komponenten –Sonstiges

- Wenn Sie eine App-V-Anwendung von einem VDA starten, der viele App-V-Anwendungen hostet, wird die Registrierung des VDAs möglicherweise aufgehoben. Das Problem tritt auf, wenn die Verarbeitung zugeordneter Richtliniendateien zu lange dauert. [CVADHELP-12592]

Kumulatives Update 5 (CU5)

September 16, 2021

Releasedatum: 22. Oktober 2019

Info zu diesem Release

Das kumulative Update 5 (CU5) für XenApp und XenDesktop 7.15 LTSR behebt über 120 seit 7.15 LTSR CU4 gemeldete Probleme.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR CU4 behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Download von 7.15 LTSR CU5

Neue Bereitstellungen

Wie stelle ich das CU5 von Grund auf bereit?

Mit dem CU5-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf dem CU5 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU5 umfasst Updates für Basiskomponenten von 7.15 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU5 zu aktualisieren. Beispiel: Wenn Provisioning Services zur LTSR-Bereitstellung gehört, aktualisieren Sie die Provisioning Services-Komponenten auf die CU5-Version. Wenn Provisioning Services nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU5

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.5000	
VDA für Serverbetriebssystem	7.15.5000	
Citrix Studio	7.15.5000	
Citrix Director	7.15.5000	
Delivery Controller	7.15.5000	
Verbundauthentifizierungsdienst	7.15.5000	
Gruppenrichtlinienverwaltung	3.1.5000	
Linux VDA	7.15.5000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.

7.15 LTSR-Basiskomponente	Version	Hinweise
Profilverwaltung	7.15.5000	
Provisioning Services	7.15.21	
Sitzungsaufzeichnung	7.15.5000	Nur Premium Edition
StoreFront	3.12.5000	
Universeller Druckserver	7.15.5000	

XenApp und XenDesktop 7.15 LTSR CU5-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU5 kompatible Komponenten und Plattformen	Version
App Layering	1903
*Browserinhaltsumleitung	15.15
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.4.3000
Lizenzserver	11.16.3.0 Build 28000
Self-Service-Kennwortzurücksetzung	1.1.10.0
Workspace Environment Management	1906.0.1.1

*Browserinhaltsumleitung

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature

werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonymisierte Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren oder aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp 7.15 CU5. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der XenApp 7.15 LTSR CU5-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU5-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU5-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU5-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

August 18, 2021

Citrix Director

- In einer Active Directory-Gesamtstruktur gibt es zwei Domänen: eine übergeordnete und eine untergeordnete. Der Benutzer wird einer domänenlokalen Gruppe in der untergeordneten Domäne hinzugefügt, die automatisch zur XenDesktop-Bereitstellungsgruppe gehört. Wenn sich der Administrator der übergeordneten Domäne bei Director anmeldet, zeigt das Dashboard eine Liste der Sitzungen an. Wenn der Administrator versucht, die Sitzungsdetails anzuzeigen, wird die folgende Fehlermeldung angezeigt:

  Dieser Benutzer hat keine ausgeführten Sitzungen oder zugewiesene Desktops.

  Der Fehler tritt für den Administrator der untergeordneten Domäne nicht auf. [LD0178]

- Wenn Sie auf der Citrix Director-Konsole Nachrichten an mehrere Benutzer senden, die nach veröffentlichtem Namen für Anwendungsinstanzen gefiltert sind, wird möglicherweise folgende Fehlermeldung angezeigt:

  Nachricht kann nicht gesendet werden. Unerwarteter Serverfehler. Weitere Informationen finden Sie in den Serverereignisprotokollen von Director. [LD1257]

- Citrix Director zeigt möglicherweise keine Personalisierungsdaten im Abschnitt "Benutzerdaten"an und es wird folgende Fehlermeldung angezeigt:

  Unerwarteter Serverfehler. [LD1353]

- Wenn Sie in einer Umgebung mit mehreren Sitzungen **Filter** > **Sitzungen** > **Alle** aufrufen und sich von einer Sitzung abmelden, wird die Sitzung abgemeldet. Wenn Sie eine weitere Sitzung mit demselben Benutzernamen auswählen und eine Abmeldung versuchen, wird folgende Fehlermeldung angezeigt:

  Die Datenquelle reagiert nicht oder hat einen Fehler gemeldet. Weitere Informationen finden Sie in den Ereignisprotokollen des Director-Servers. [LD1441]

- Citrix Director zeigt möglicherweise nur wenige Tabelleneinträge gefolgt von einem leeren Bereich an. Sie können die verbleibenden Datensätze erst sehen, wenn Sie die Tabelle nach unten scrollen. [LD1706]

Citrix Studio

- Bei Auswahl von **Erweitert** für **XenApp Edition** können Sie möglicherweise keine neue Hostverbindung für Amazon Web Services (AWS) erstellen. [LD1988]
- Das Löschen virtueller Maschinen aus einem Katalog kann mit der Ausnahme **System.ArgumentNullException Value cannot be Null** fehlschlagen. [LD2014]
- Die App-V Pakete, die für VDAs bereitgestellt werden, werden möglicherweise fälschlicherweise von den VDAs entfernt. Dieser Fix schreibt einen Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features. Der Schlüssel steuert, ob die Bereinigung aktiviert oder deaktiviert werden soll. Standardmäßig ist die Bereinigung deaktiviert. [LD2025]

  Um sie zu aktivieren, fügen Sie den folgenden Registrierungsschlüssel hinzu:

  HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features

  Name: RedundantPackageCleanup

  Typ: REG_SZ

  Daten: True
- Das Hinzufügen von Maschinen über Citrix Studio zu einem Maschinenkatalog kann mit einer Ausnahme (**Fehler-ID: XDDS:081419B3**) fehlschlagen. Das Problem tritt auf, wenn eine Maschine aus einer Provisioning Services-Gerätesammlung hinzugefügt wird, die ein oder mehrere Zielgeräte mit einem ein `domainObjectSID`-NULL-Attribut in der `dbo.device`-Tabelle der Provisioning Services-Datenbank enthält. [LD2029]

Konfigurationsprotokollierungsdienst

- Der Sitekonfigurationstestbericht generiert möglicherweise einen Fehler beim Auflösen der Benutzer-Sicherheits-IDs (SIDs). Das Problem tritt auf, wenn überprüft wird, ob die Konfigurationsprotokollierungs-SID-Identitäten aus Active Directory aufgelöst werden können. [LD1569]

Controller

- Das Löschen eines Basisdatenträgerimages mit Machine Creation Services (MCS) schlägt möglicherweise fehl. [LD2143]
- Dieser Fix behebt ein Speicherverlustproblem, das beim Citrix Dienst für hohe Verfügbarkeit auftritt, wenn Sie einen VDA neu starten. [LD1121]

- Bei Verwendung von Amazon Web Services (AWS) kann es beim Maschinenneustart zu einer Verzögerung von mehreren Minuten kommen. [LD1220]
- Die CPU-Auslastung der Überwachungsdatenbank kann auf dem SQL Server-Rechner sehr hoch sein. Das Problem beeinträchtigt die Gesamtleistung. [LD1478]
- Eine manuell über Citrix Studio ausgeführte Energieaktion bzw. geplante Energieaktionen können fehlschlagen, wenn Amazon Web Services (AWS) verwendet wird. Das Problem tritt auf, wenn Sie virtuellen Maschinen zurücksetzen, während diese eingeschaltet sind. [LD1548]
- Das Anhalten des Citrix Broker-Diensts kann fehlschlagen. [LD1753]
- Dieser Fix behebt ein Problem in einer Hintergrundkomponente. [LD1808]
- Wenn Sie den Citrix Scout-Bericht ausführen, wird der Citrix Analytics-Dienst möglicherweise unerwartet beendet und folgende Fehlermeldung wird angezeigt:

  Der Citrix Analytics-Dienst wird nicht mehr ausgeführt. [LD1860]
- Eine Katalogaktualisierung kann fehlschlagen, ohne dass eine Fehlermeldung oder ein Fortschrittsbalken angezeigt wird. [LD1980]
- Bei Auswahl von **Erweitert** für **XenApp Edition** können Sie möglicherweise keine neue Hostverbindung für Amazon Web Services (AWS) erstellen. [LD1988]
- Das Löschen virtueller Maschinen aus einem Katalog kann mit der Ausnahme **System.ArgumentNullException Value cannot be Null** fehlschlagen. [LD2014]
- Wenn Sie **Citrix Director** > **Trends** > **Kapazitätsverwaltung** > **Server-OS-Nutzung** aufrufen, wird unter **Max. gleichzeitiger Desktopinstanzen auf Server-OS** möglicherweise eine höhere Sitzungsanzahl angezeigt als tatsächlich korrekt wäre. Das Problem tritt auf, wenn die Berechnung **Max. gleichzeitiger Desktopinstanzen auf Server-OS** einzelne Sitzungen aufgrund von Wiederverbindungen mehrfach zählt. [LD2122]
- Wenn Sie versuchen, einen Maschinenkatalog mit Maschinenerstellungsdienste in einer VMware Umgebung zu erstellen, schlägt die Katalogerstellung mit der folgenden Fehlermeldung fehl:

  FailedToCreateImagePreparationVm [LD2158]
- Der Versuch, einen MCS-Maschinenkatalog in Microsoft Azure zu erstellen oder zu aktualisieren, kann mit der folgenden Fehlermeldung fehlschlagen:

  Fehler, Ausnahme vom Typ: "System.OutOfMemoryExceotion" [LD2160]

Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU5 Dokumentation enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

- Mit der Citrix Profilverwaltung funktioniert der Bugfix von Microsoft zum Löschen der Firewallregeln, die während der Benutzeranmeldung unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy erstellt wurden, möglicherweise nicht. Das Problem tritt auf, weil die Citrix Profilverwaltung nicht die Standard-API von Microsoft aufruft, um das lokale Profil zu löschen. Weitere Informationen über den Fix finden Sie im Microsoft Knowledge Base-Artikel KB4467684. [LD1074]
- Die Dateien, die Sie aus einer Sitzung löschen, werden möglicherweise nicht aus dem UPM-Speicher gelöscht. [LD1270]
- Bei den protokollierten Anmeldedauern in Citrix Director und den von den VDAs bereitgestellten Ereignisprotokollen können Diskrepanzen auftreten. [LD1679]
- Die Profilverwaltung bricht Kopiervorgänge in den Profilspeicher nicht ab, wenn ein beschädigtes lokales Profil `NTUSER.DAT` nicht geladen werden konnte. Stattdessen wird die beschädigte Registrierungsstruktur in den Profilspeicher kopiert und die `NTUSER.DAT`-Datei und deren Backup überschrieben. [LD1816]
- Ein Registrierungspfad, den Sie zur Ausschlussliste hinzufügen, wird möglicherweise dennoch gespeichert. Das Problem tritt auf, wenn am Ende des Registrierungspfads ein umgekehrter Schrägstrich (\) steht. [LD1862]
- Der Citrix Desktopdienst (BrokerAgent.exe) wird möglicherweise unerwartet beendet und die folgende Ausnahme tritt auf, bis Sie den Citrix Profilverwaltungsdienst neu starten:

  System_Management_Instrumentation_ni!WmiNative.WbemProvider.WmiNative.IWbemServices.Cr
  [LD2223]

Provisioning Services

Provisioning Services 7.15 LTSR CU5 enthält Informationen zu den Updates in diesem Release.

StoreFront

- Wenn Sie versuchen, eine Verbindung mit einer zuvor getrennten Sitzung wiederherzustellen, indem Sie auf das Symbol klicken, wird die Sitzung möglicherweise nicht wieder hergestellt. Dieses Problem tritt auf, wenn mehrere Desktops mit identischen Namen für Endbenutzer veröffentlicht werden. [LD1367]
- Wenn Sie den einer Benutzerfarm-Zuordnung zugewiesenen Controller bearbeiten und dann versuchen, die Änderungen zu speichern, wird die Microsoft Management Console (MMC)

möglicherweise unerwartet beendet. Das Problem tritt auf Servern mit Microsoft .NET Framework 4.7 auf. [LD1668]

Universeller Druckserver

Client

- Der Druckspoolerdienst wird möglicherweise unerwartet beendet. Das Problem tritt auf, wenn `CRawStreamHeaderWriter::EndPage` und `CRawStreamHeaderWriter::StartPage` versuchen, auf ein NULL-Objekt zuzugreifen. [LC7893]
- Der universelle Druckserver kann bewirken, dass der Druckspoolerdienst aufhört, zu reagieren. [LC9341]
- Bevor Sie ein Dokument drucken, wählen Sie im Druckdialogfeld der veröffentlichten Desktopsitzung einen Drucker aus der Liste der verfügbaren Drucker aus. Es kann zu einer Verzögerung kommen, bis der Drucker mit dem Drucken des Dokuments beginnt. [LC9601]
- Nach der Installation eines VDA werden die Druckerports in den **Druckereigenschaften** für einen zugeordneten Netzwerkdrucker möglicherweise nicht mehr angezeigt. [LD0949]
- Der Versuch, ein Dokument zu drucken, kann in einigen Workflows langsam sein. [LD1256]
- Wenn die Einstellung **Verwendung universeller Druckertreiber** auf **Nur universelles Drucken verwenden** festgelegt ist, werden Clientdrucker möglicherweise nicht automatisch in Sitzungen erstellt. [LD1395]

Benutzerprofilverwaltung –VDA

- Wenn Sie sich an einer Sitzung anmelden, werden die Benutzerdaten möglicherweise unerwartet gelöscht. Das Problem tritt auf, wenn Sie die Dateiserveradresse von path1 in path2 in den Einstellungen der Citrix-Richtlinie **Ordnerumleitungspfad** ändern (z. B. die Einstellung **Desktop path**) und path1 und path2 auf denselben physischen Ort verweisen. Zur Problemvermeidung aktivieren Sie die Microsoft-Gruppenrichtlinieneinstellung **Vor der Umleitung überprüfen, ob das alte und das neue Ziel der Ordnerumleitung auf dieselbe Freigabe verweisen**. Weitere Informationen finden Sie im Abschnitt **Beschreibung** der Einstellungen der Citrix Richtlinie "Ordnerumleitungspfad". [LD1500]

VDA für Desktopbetriebssystem

Tastatur

- Bei Verwendung des koreanischen Eingabemethoden-Editors (IME) zur Texteingabe verschwindet das letzte Zeichen möglicherweise, wenn Sie mit der Maus klicken. Das Problem tritt auf, wenn der generische Client-IME in Citrix Receiver aktiviert ist. [LD1380]
- Wenn Sie zu einer Website navigieren und die Tastatur als ausgeblendet festlegen, wird sie möglicherweise weiterhin im nicht bearbeitbaren Bereich der Website angezeigt. [LD1382]

Drucken

- Der Versuch, ein Dokument zu drucken, kann in einigen Workflows langsam sein. [LD1256]
- Wenn die Einstellung **Verwendung universeller Druckertreiber** auf **Nur universelles Drucken verwenden** festgelegt ist, werden Clientdrucker möglicherweise nicht automatisch in Sitzungen erstellt. [LD1395]
- Auf VDAs für Desktopbetriebssysteme kann das Drucken einer Datei mit einem zugeordneten Clientdrucker fehlschlagen. Das Problem tritt auf, wenn der VDA unter Windows 10 Version 1903 installiert ist. [LD2370]

Sitzung/Verbindung

- Bei der Audiowiedergabe in einer Benutzersitzung ist möglicherweise ein Knacken zu hören. Das Problem tritt auf, wenn Sie Audio wiedergeben. [LD0455]
- In Citrix Receiver für Windows wird die Audiowiedergabe möglicherweise ab und zu unterbrochen. [LD0624]
- Wenn Adobe Acrobat Reader und Microsoft Outlook im Seamlessmodus ausgeführt werden und Sie beide maximieren, reagieren die **Menüleiste** und die Schaltflächen **Minimieren** , **Wiederherstellen** und **Schließen** in Acrobat Reader möglicherweise nicht mehr. [LD1006]
- Wenn Sie ein USB-Mikrofon an ein Benutzergerät anschließen und eine Sitzung starten, wird das USB-Mikrofon möglicherweise nicht umgeleitet. Das USB-Gerät wird als **Optimiert, Von Richtlinie eingeschränkt** angezeigt. [LD1027]
- Bei manchen Anwendungen von Drittanbietern ist bei der Audiowiedergabe oder bei Wiedergabepausen möglicherweise ein Rauschen zu hören. [LD1136]
- Der Sitzungsstart kann auf dem VDA fehlschlagen. [LD1180]

- Wenn Sie einen VDA installieren, wird auch der USB-Root-Hub im Geräte-Manager installiert. Der USB-Root-Hub wird installiert, obwohl der USB-2.0-Root-Hub oder der USB-3.0-Root-Hub bereits installiert ist. [LD1196]
- Wenn die Richtlinie für den **Legacygrafikmodus** aktiviert ist, kann die Herstellung einer Verbindung zu einem VDA für das Desktopbetriebssystem fehlschlagen. Das Problem tritt auf, wenn der VDA als Server-VDI unter Microsoft Windows Server 2008 R2 installiert ist. [LD1296]
- Nach dem Neustart eines VDA wird die Richtlinie "Sitzungszuverlässigkeit - Timeout"möglicherweise nicht auf die erste Verbindung angewendet. Auf nachfolgende Verbindungen kann die Richtlinie möglicherweise angewendet werden. [LD1397]
- Bei aktiviertem EDT (Enlightened Data Transport) werden VDAs möglicherweise unerwartet mit dem Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)** beendet. Das Problem tritt beim externen Zugriff auf Benutzersitzungen über den Zscaler auf. [LD1493]
- Wenn Sie die clientseitige Auflösung ändern, werden bestimmte Legacyanwendungen wie Citrix Studio evtl. fälschlicherweise in einer Seamless-Sitzung neu aufgebaut. [LD1554]
- Wenn Sie die Verbindung zu einer Sitzung wiederherstellen, wird das VDA-Benachrichtigungssymbol im Benachrichtigungsbereich des Benutzergeräts möglicherweise ausgeblendet. [LD1629]
- Nach dem Upgrade von XenApp und XenDesktop 7.15 LTSR CU 2 auf CU 3 reagieren in veröffentlichten Desktopsitzungen einige .NET-Anwendungen möglicherweise nicht mehr. Das Problem tritt bei VDAs unter Windows Server 2008 R2 auf. [LD1726]
- Wenn Sie visuelle Effekte in einer Benutzersitzung ändern, wird der Wert `UserPreferencesMask` des Registrierungsschlüssels HKEY_CURRENT_USER\Control Panel\Desktop möglicherweise nicht auf einen neuen Wert aktualisiert. [LD1827]

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\UI Tweak\SystemPropertiesComputerNa

  Name: HookProcess

  Typ: REG_DWORD

  Wert: 1
- Die Gerätebeschreibung im Geräte-Manager kann in japanischen Microsoft Windows-Versionen fehlerhaft sein. [LD1834]
- Eine Zugriffsverletzung kann dazu führen, dass der Prozess wfshell.exe unerwartet beendet wird. Anwendungen können dann nicht gestartet werden. [LD2050]

Smartcards

- Die Smartcard-Passthrough-Authentifizierung kann unter Windows 8 oder Windows 10 fehlschlagen. Wenn Sie eine VDA-Sitzung sperren und entsperren, wechselt der Benutzer vom Smartcard- zum Domänenbenutzer. [LD1365]

Systemausnahmen

- Der Internet Explorer-Prozess (iexplore.exe) wird möglicherweise unerwartet beendet, wenn Sie Webanwendungen ausführen, die die Standort-API implementieren. [LD0677]
- Der Citrix Softwaregrafikprozess (Ctxgfx.exe) wird auf Rechnern des Modells AMD Opteron(tm) 6128 HE möglicherweise unerwartet beendet. [LD0954]
- Der wfshell.exe-Prozess kann auf VDAs unerwartet beendet werden. Das Problem tritt aufgrund des fehlerhaften Moduls CtxUiMon.dll auf. [LD1359]
- Auf VDAs mit XenApp und XenDesktop 7.15 LTSR kann für ctxdvcs.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode 0x0000007E auftreten. [LD1688]
- Der wfshell.exe-Prozess kann auf VDAs unerwartet beendet werden. [LD1847]
- Nach Anwendung von Fix LD0624 kann es auf VDAs für Desktopbetriebssysteme zu einer schwerwiegenden Ausnahme bei ctxad.sys mit Bluescreen und einem Audioclient-Checkcode kommen. [LD1995]
- Das Starten von Anwendungen kann fehlschlagen, wenn der Prozess wfshell.exe unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls cmpcom.dll auf. [LD2107]

Benutzeroberfläche

- Das Anmeldefenster wird möglicherweise nicht im Vordergrund angezeigt, wenn die Anmeldeinformationen manuell eingegeben werden müssen. [LC9861]
- Wenn die Citrix Schaltfläche **Trennen** installiert ist, ist das Öffnen durch Klicken auf die Schaltfläche “Start”möglicherweise langsam oder unmöglich. [LD1149]
- Wenn Sie in einer veröffentlichten Anwendung mit der rechten Maustaste das Kontextmenü öffnen, wird es möglicherweise nicht an der Cursorposition geöffnet. [LD1243]
- Ein Problem kann auftreten, wenn Sie eine VDA-Sitzung auf einem Surface Pro-Gerät starten und **Write in the handwriting panel with your fingertip** auf der Seite **Pen and Windows Ink** aktivieren. Die Schriftgröße von Text oder eines Bilds, das Sie eingeben, ist möglicherweise größer als bei der Eingabe mit der Maus. [LD1472]

- Auf dem **VDI-Desktopbildschirm** kann es vorkommen, dass ein Fenster herumspringt oder verschwindet. [LD1696]

VDA für Serverbetriebssystem

Tastatur

- Bei Verwendung des koreanischen Eingabemethoden-Editors (IME) zur Texteingabe verschwindet das letzte Zeichen möglicherweise, wenn Sie mit der Maus klicken. Das Problem tritt auf, wenn der generische Client-IME in Citrix Receiver aktiviert ist. [LD1380]
- Wenn Sie zu einer Website navigieren und die Tastatur als ausgeblendet festlegen, wird sie möglicherweise weiterhin im nicht bearbeitbaren Bereich der Website angezeigt. [LD1382]

Drucken

- Bevor Sie ein Dokument drucken, wählen Sie im Druckdialogfeld der veröffentlichten Desktopsitzung einen Drucker aus der Liste der verfügbaren Drucker aus. Es kann zu einer Verzögerung kommen, bis der Drucker mit dem Drucken des Dokuments beginnt. [LC9601]
- Der Versuch, ein Dokument zu drucken, kann in einigen Workflows langsam sein. [LD1256]
- Wenn die Einstellung **Verwendung universeller Druckertreiber** auf **Nur universelles Drucken verwenden** festgelegt ist, werden Clientdrucker möglicherweise nicht automatisch in Sitzungen erstellt. [LD1395]

Sitzung/Verbindung

- Wenn Adobe Acrobat Reader und Microsoft Outlook im Seamlessmodus ausgeführt werden und Sie beide maximieren, reagieren die **Menüleiste** und die Schaltflächen **Minimieren** , **Wiederherstellen** und **Schließen** in Acrobat Reader möglicherweise nicht mehr. [LD1006]
- Wenn Sie ein USB-Mikrofon an ein Benutzergerät anschließen und eine Sitzung starten, wird das USB-Mikrofon möglicherweise nicht umgeleitet. Das USB-Gerät wird als **Optimiert, Von Richtlinie eingeschränkt** angezeigt. [LD1027]
- Der Citrix Broker-Dienst meldet möglicherweise den folgenden Fehler im Ereignisprotokoll:

  Der Citrix Brokerdienst konnte die für den Virtual Desktop Agent auf Maschine ‘machine_name’ erforderlichen Grundeinstellungen nicht ermitteln.

  Ausnahme: System.ArgumentNullException

  Parametername: enumStr [LD1315]

- Die Startzeit kann sich erhöhen, wenn mehrere Active Directory-Sicherheitsgruppen auf "Sichtbarkeit beschränken"konfiguriert sind. [LD1368]
- Nach dem Neustart eines VDA wird die Richtlinie "Sitzungszuverlässigkeit - Timeout"möglicherweise nicht auf die erste Verbindung angewendet. Auf nachfolgende Verbindungen kann die Richtlinie möglicherweise angewendet werden. [LD1397]
- VDAs für Serverbetriebssysteme reagieren möglicherweise nicht mehr, wenn der Prozess "Winlogon.exe"unerwartet beendet wird. [LD1480]
- Bei aktiviertem EDT (Enlightened Data Transport) werden VDAs möglicherweise unerwartet mit dem Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)** beendet. Das Problem tritt beim externen Zugriff auf Benutzersitzungen über den Zscaler auf. [LD1493]
- Wenn Sie die clientseitige Auflösung ändern, werden bestimmte Legacyanwendungen wie Citrix Studio evtl. fälschlicherweise in einer Seamless-Sitzung neu aufgebaut. [LD1554]
- Wenn Sie die Verbindung zu einer Sitzung wiederherstellen, wird das VDA-Benachrichtigungssymbol im Benachrichtigungsbereich des Benutzergeräts möglicherweise ausgeblendet. [LD1629]
- Nach dem Upgrade von XenApp und XenDesktop 7.15 LTSR CU 2 auf CU 3 reagieren in veröffentlichten Desktopsitzungen einige .NET-Anwendungen möglicherweise nicht mehr. Das Problem tritt bei VDAs unter Windows Server 2008 R2 auf. [LD1726]
- Wenn Sie visuelle Effekte in einer Benutzersitzung ändern, wird der Wert `UserPreferencesMask` des Registrierungsschlüssels HKEY_CURRENT_USER\Control Panel\Desktop möglicherweise nicht auf einen neuen Wert aktualisiert. [LD1827]

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\UI Tweak\SystemPropertiesComputerNa

  Name: HookProcess

  Typ: REG_DWORD

  Wert: 1
- Die Gerätebeschreibung im Geräte-Manager kann in japanischen Microsoft Windows-Versionen fehlerhaft sein. [LD1834]
- Eine Zugriffsverletzung kann dazu führen, dass der Prozess wfshell.exe unerwartet beendet wird. Anwendungen können dann nicht gestartet werden. [LD2050]

Systemausnahmen

- Der Internet Explorer-Prozess (iexplore.exe) wird möglicherweise unerwartet beendet, wenn Sie Webanwendungen ausführen, die die Standort-API implementieren. [LD0677]

- Der Citrix Softwaregrafikprozess (Ctxgfx.exe) wird auf Rechnern des Modells AMD Opteron(tm) 6128 HE möglicherweise unerwartet beendet. [LD0954]
- Microsoft Internet Explorer kann unerwartet beendet werden. Das Problem tritt aufgrund des fehlerhaften Moduls icaendpoint.dll auf. [LD1266]
- Der wfshell.exe-Prozess kann auf VDAs unerwartet beendet werden. Das Problem tritt aufgrund des fehlerhaften Moduls CtxUiMon.dll auf. [LD1359]
- Auf VDAs mit XenApp und XenDesktop 7.15 LTSR kann für ctxdvcs.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode 0x0000007E auftreten. [LD1688]
- Der wfshell.exe-Prozess kann auf VDAs unerwartet beendet werden. [LD1847]
- Das Starten von Anwendungen kann fehlschlagen, wenn der Prozess wfshell.exe unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls cmpcom.dll auf. [LD2107]

Benutzererfahrung

- Wenn Sie mit der linken Maustaste auf den Lautstärkeregler in der Taskleiste klicken wird dieser möglicherweise nicht geöffnet. Das Problem tritt bei nicht englischsprachigen Microsoft Windows-Versionen auf. [LD0039]

Benutzeroberfläche

- Das Anmeldefenster wird möglicherweise nicht im Vordergrund angezeigt, wenn die Anmeldeinformationen manuell eingegeben werden müssen. [LC9861]
- Wenn Sie in einer veröffentlichten Anwendung mit der rechten Maustaste das Kontextmenü öffnen, wird es möglicherweise nicht an der Cursorposition geöffnet. [LD1243]
- Ein Problem kann auftreten, wenn Sie eine VDA-Sitzung auf einem Surface Pro-Gerät starten und **Write in the handwriting panel with your fingertip** auf der Seite **Pen and Windows Ink** aktivieren. Die Schriftgröße von Text oder eines Bilds, das Sie eingeben, ist möglicherweise größer als bei der Eingabe mit der Maus. [LD1472]

Virtual Desktop-Komponenten –Sonstiges

- Bei Director sind Inkonsistenzen im Anwendungsnamen möglich, wenn die Anwendung in einer veröffentlichten Instanz von Internet Explorer abgerufen wird. Es wird der gleiche Anwendungsname für verschiedene Benutzer angezeigt, die mit derselben Maschine verbunden sind. [LD0351]

- Ein Problem kann auftreten, wenn Sie sich bei einer Sitzung mit dem Benutzerprinzipalnamen (UPN) (Benutzer@Domäne) anmelden. Wenn Sie den Bildschirm sperren, wird anstelle des UPN das SAM-Konto (Domäne\Benutzername) auf dem gesperrten Desktop angezeigt. [LD1141]
- Der Sitzungsstart kann auf dem VDA fehlschlagen. [LD1180]
- Der Citrix Broker-Dienst meldet möglicherweise den folgenden Fehler im Ereignisprotokoll:

  Der Citrix Brokerdienst konnte die für den Virtual Desktop Agent auf Maschine 'machine_name' erforderlichen Grundeinstellungen nicht ermitteln.

  Ausnahme: System.ArgumentNullException

  Parametername: enumStr [LD1315]
- Die Katalogerstellung über eine mit System Center Virtual Machine Manager erstellte VM als Vorlage kann fehlschlagen. Das Problem tritt auf, wenn auf der VM Windows 10 Version 1803 oder später installiert ist und Sie für die VM **Secure Boot** aktiviert haben. [LD1608]
- Bei den protokollierten Anmeldedauern in Citrix Director und den von den VDAs bereitgestellten Ereignisprotokollen können Diskrepanzen auftreten. [LD1679]
- Der Brokeragent schreibt die GPF-Dateien nicht in den Speicherort für persistente Daten. [LD1691]
- Die App-V Pakete, die für VDAs bereitgestellt werden, werden möglicherweise fälschlicherweise von den VDAs entfernt. Dieser Fix schreibt einen Registrierungsschlüssel unter HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features. Der Schlüssel steuert, ob die Bereinigung aktiviert oder deaktiviert werden soll. Standardmäßig ist die Bereinigung deaktiviert. [LD2025]

  Um sie zu aktivieren, fügen Sie den folgenden Registrierungsschlüssel hinzu:

  HKEY_LOCAL_MACHINE\Software\Citrix\AppV\Features

  Name: RedundantPackageCleanup

  Typ: REG_SZ

  Daten: True

Kumulatives Update 4 (CU4)

September 16, 2021

Releasedatum: 23. April 2019

Info zu diesem Release

Das kumulative Update 4 (CU4) für XenApp und XenDesktop 7.15 LTSR behebt über 140 seit 7.15 LTSR CU3 gemeldete Probleme.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR CU3 behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Download von 7.15 LTSR CU4

Neue Features in diesem kumulativen Update

- Wenn Sie Delivery Controller und eine Site auf 7.15 CU4 aktualisieren, werden vor dem eigentlichen Upgrade Vorbereitungstests an der Site ausgeführt. Dabei wird überprüft, ob wichtige Citrix Dienste ordnungsgemäß ausgeführt werden und ob die Sitedatenbank ordnungsgemäß funktioniert und vor Kurzem gesichert wurde. Nachdem die Tests ausgeführt wurden, können Sie einen Bericht anzeigen. Anschließend können Sie eventuelle Probleme beheben und die Tests gegebenenfalls wiederholen. Dadurch wird sichergestellt, dass das Upgrade einwandfrei durchgeführt werden kann.
- In dieser Version wurde die Abhängigkeit von Version 2.0 von PowerShell in eigenständigen Bereitstellungen von Citrix Studio und seinen Komponenten beseitigt.

> **Hinweis:**
> PowerShell ist weiterhin auf den Maschinen erforderlich, auf denen Sie eine oder mehrere dieser Komponenten installieren. Es muss jedoch nicht mehr Version 2.0 sein. Auf Delivery Controllern und StoreFront-Servern ist PowerShell 2.0 weiterhin erforderlich. Weitere Informationen finden Sie unter [LD0184].

- Wenn eine VDA- oder Delivery Controller-Installation fehlschlägt, wird das Protokoll des fehlerhaften MSI von einem Analysetool analysiert und der exakte Fehlercode angezeigt. Das Tool empfiehlt einen CTX-Artikel, wenn es sich um ein bekanntes Problem handelt. Das Tool sammelt außerdem anonymisierte Daten über den Fehlercode. Diese Daten werden anderen, vom CEIP gesammelten Daten beigefügt. Wenn Sie die Registrierung beim CEIP beenden, werden die gesammelten MSI-Analysedaten nicht mehr an Citrix gesendet.

Neue Bereitstellungen

Wie stelle ich das CU4 von Grund auf bereit?

Mit dem CU4-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf dem CU4 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU4 umfasst Updates für Basiskomponenten von 7.15 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU4 zu aktualisieren. Beispiel: Wenn Provisioning Services zur LTSR-Bereitstellung gehört, aktualisieren Sie die Provisioning Services-Komponenten auf die CU4-Version. Wenn Provisioning Services nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU4

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.4000	
VDA für Serverbetriebssystem	7.15.4000	
Citrix Studio	7.15.4000	
Citrix Director	7.15.4000	
Delivery Controller	7.15.4000	
Verbundauthentifizierungsdienst	7.15.4000	
Gruppenrichtlinienverwaltung	3.1.4000	
Linux VDA	7.15.4000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.

7.15 LTSR-Basiskomponente	Version	Hinweise
Profilverwaltung	7.15.4000	
Provisioning Services	7.15.15	
Sitzungsaufzeichnung	7.15.4000	nur Platinum Edition
StoreFront	3.12.4000	
Universeller Druckserver	7.15.4000	

XenApp und XenDesktop 7.15 LTSR CU4-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU4 kompatible Komponenten und Plattformen	Version
App Layering	1903
*Browserinhaltsumleitung	15.15
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.4.3000
Lizenzserver	11.15.0.0 Build 26000
Self-Service-Kennwortzurücksetzung	1.1.10.0
Workspace Environment Management	1811

*Browserinhaltsumleitung

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature

werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

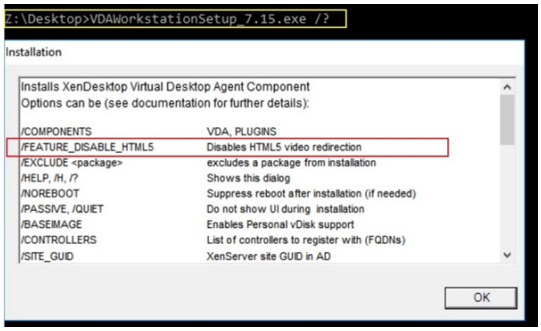
Systemanforderungen:

Diese Anforderungen gelten für das BCR.msi mit XenApp und XenDesktop 7.15 LTSR CU4. Ignorieren Sie sämtliche für andere Versionen von XenApp, XenDesktop und Citrix Virtual Apps and Desktops aufgeführten Systemanforderungen für die Browserinhaltsumleitung.

- Version 7.15 LTSR CU4 auf dem Delivery Controller und dem VDA.
- Citrix Workspace-App 1809 oder später für Windows.
- BCR.msi –verfügbar auf der Citrix Downloadseite.
- Chrome (mit installierter Browserinhaltsumleitungserweiterung aus dem Chrome WebStore) oder Internet Explorer 11 (mit aktiviertem Browser Helper Object (BHO) Citrix HDXJSInjector).

Installation:

1. Installieren Sie über die Befehlszeilenoption /FEATURE_DISABLE_HTML5 Version 7.15 LTSR CU4 des VDA (bzw. führen Sie ein Upgrade auf diese Version durch).



   Diese Option entfernt die HTML5-Videoumleitung, was vor dem Ausführen des BCR.msi-Pakets erforderlich ist. Durch das BCR.msi werden das Feature selbst sowie die entsprechenden Dienste während der Installation wieder hinzugefügt. Öffnen Sie nach diesem Schritt die services.msc-Konsole und vergewissern Sie sich, dass **Citrix HDX HTML5 Video Redirection Service** nicht aufgeführt wird.

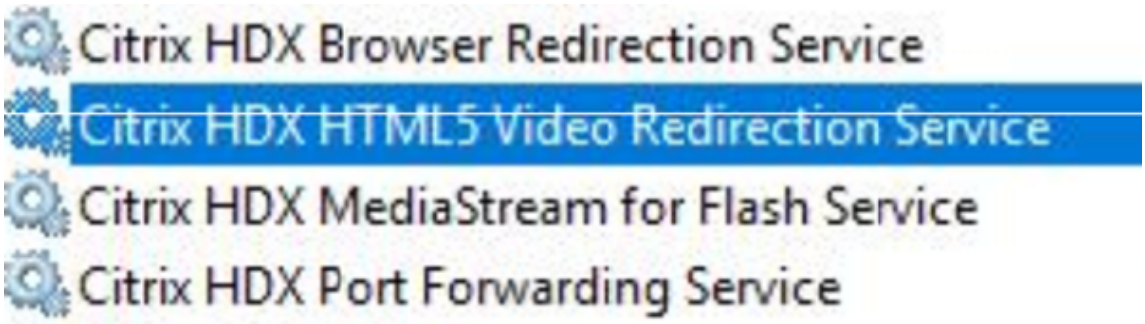
2. Starten Sie die Installation der Browserinhaltsumleitung mit dem BCR.msi. Systemabhängig werden die BCR.msi-Dateien unter einem der folgenden Pfade installiert:

   C:\Programme\Citrix\ICAService

   oder

C:\Programme(86)\Citrix\ICAService

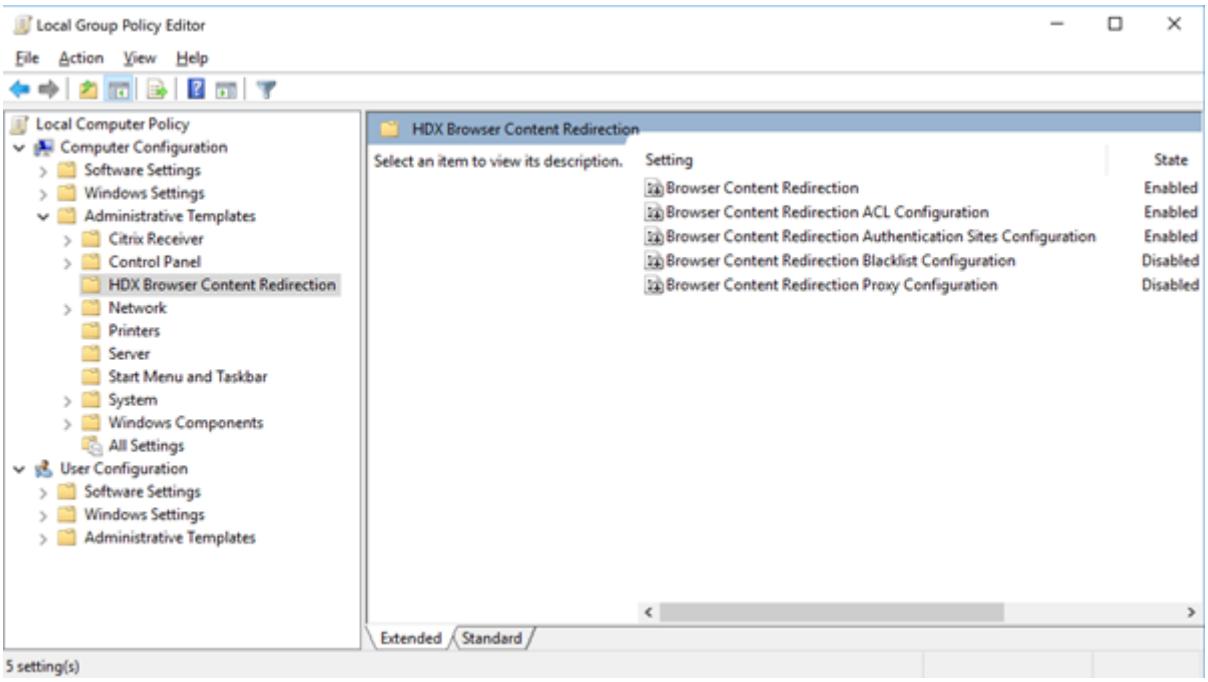
Da die Installation schnell erfolgt, wird das Dialogfeld möglicherweise schnell geschlossen. Führen Sie in diesem Fall services.msc erneut aus, um zu prüfen, ob die Dienste hinzugefügt wurden.



Richtlinien:

Sie können Richtlinien über Registrierungseinträge unter HKEY_LOCAL_MACHINE auf dem VDA oder die administrative Vorlage **HDX Browser Content Redirection** von Citrix für die Gruppenrichtlinien-Verwaltungskonsole steuern.

Sie können die Vorlage von citrix.com unter Citrix Virtual Apps and Desktops (XenApp & XenDesktop) > XenApp 7.15 LTSR / XenDesktop 7.15 LTSR > Components herunterladen. Citrix Studio enthält diese Richtlinien nicht.



Weitere Informationen finden Sie unter Richtlinieneinstellungen für die Browserinhaltsumleitung. Informationen zur Problembehandlung finden Sie im Knowledge Center-Artikel CTX230052.

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonyme Informationen über den Installationsvorgang gesammelt

und auf der Maschine gespeichert, auf der Sie die Komponente installieren/aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp LTSR 7.15 CU4. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der XenApp 7.15-LTSR CU4-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU4-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU4-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU4-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

August 18, 2021

Citrix Director

- Wenn Sie in Citrix Director zu **Filter** > **Sitzungen** navigieren, werden anstelle der Sitzungsdaten Kontrollkästchen angezeigt. [LC9871]

- Benutzerdefinierte Administratoren können möglicherweise keine Sitzungsdetails von einem VDA der Version 7.15 abrufen, wenn Citrix Director mit einem Delivery Controller der Version 7.6 verbunden ist. [LD0134]
- Die Integration von NetScaler Management and Analytics System (MAS) in Citrix Director schlägt möglicherweise fehl. Das Problem tritt auf, wenn durch eine Gruppenrichtlinie das integrierte Administratorkonto geändert oder umbenannt wird. Director verwendet das lokale Administratorkonto zum Verschlüsseln und Entschlüsseln von **C:\inetpub\wwwroot\Director\bin..\plugin\hdxInsight\data.xml**. Dieser Fix behebt das Problem bei Änderungen am Code. Nachdem die Änderungen vorgenommen wurden, verwendet Director das Maschinenkonto der Maschine, auf welcher Director installiert ist, um **C:\inetpub\wwwroot\Director\bin..\plugin\hdxInsight\data.xml** zu verschlüsseln oder zu entschlüsseln. [LD0231]
- Die Sommerzeit ist im Betriebssystem aktiviert. Beim Datenexport für den Vormonat unter Auswahl des Formats CSV fehlen die beiden Optionsfelder **Diagrammdaten exportieren**und **Tabellendaten exportieren**. [LD0569]
- Wenn Sie zu **Trends** > **Ressourcenauslastung** > **Serverbetriebssystemmaschinen** navigieren und versuchen, mithilfe der Bildlaufleiste die vollständige Liste der Maschinen anzuzeigen, werden nur wenige Tabellendatensätze angezeigt. Die restlichen Datensätze bleiben verborgen. Das Problem tritt auf, wenn die Bildlaufleiste nicht ordnungsgemäß funktioniert. [LD0789]
- Wenn Sie benutzerdefinierte Berichte für Verbindungen in Director erstellen, werden einige DateTime-Felder, z. B. Sitzungsfehlerzeit (Session.FailureDate) und Sitzungsänderungszeit (Session.ConnectionStateChangeDate), möglicherweise nicht von UTC in die lokale Zeit umgerechnet. [LD1001]
- Wenn Sie in Citrix Director nach einem Benutzer mit einem langen Benutzernamen suchen, wird der Name möglicherweise abgeschnitten. [LD1106]

Citrix Richtlinie

- Das Kopieren eines Gruppenrichtlinienobjekts mit Citrix Richtlinieneinstellungen unter Verwendung der Gruppenrichtlinien-Verwaltungskonsole kann fehlschlagen. Die Microsoft Management Console (MMC) wird unerwartet beendet. [LD0322]
- Das Objekt "Citrix Universeller Drucker"wird mit dem universellen EMF-Druckertreiber in einer Sitzung erstellt, selbst wenn Sie die Einstellungen für den universellen Druckertreiber auf **XPS** oder **Native Treiber** festlegen. Installieren Sie zum Erhalt des Fixes Citrix Receiver für Windows 4.9.5000 LTSR kumulatives Update 5 oder eine spätere Version. [LD0360]
- Wenn Sie eine Richtlinie in Citrix Studio ändern, wird möglicherweise folgende Fehlermeldung in der **Konfigurationsprotokollierung**angezeigt.

Fehler beim Versuch, Details zur Richtlinienänderung zu ermitteln.

Wenn diese Fehlermeldung angezeigt wird, können Sie die Details der Richtlinienänderung nicht mithilfe der Konfigurationsprotokollierung ermitteln. [LD0596]

- Wenn eine große Anzahl von Standortrichtlinien konfiguriert ist und IP- oder OU-basierte Filter aktiviert sind, kann es zu einer Verzögerung bei der Anmeldung kommen. [LD0221]

Citrix Studio

- In dieser Version wurde die Abhängigkeit von Version 2.0 von PowerShell in eigenständigen Bereitstellungen von Citrix Studio und seinen Komponenten beseitigt.

> **Hinweis:**
> PowerShell ist weiterhin auf den Maschinen erforderlich, auf denen Sie eine oder mehrere dieser Komponenten installieren. Es muss jedoch nicht mehr Version 2.0 sein. Auf Delivery Controllern und StoreFront-Servern ist PowerShell 2.0 weiterhin erforderlich. Unter Windows 7 oder Windows Server 2008 R2 ist PowerShell Version 3.0 oder höher erforderlich, wenn Sie Controller-Komponenten, einschließlich Citrix Studio, installieren. [LD0184]

- Wenn Sie einer Site mehrere App-V-Pakete hinzufügen, zeigt Studio möglicherweise folgende Fehlermeldung an und der Administrator kann keine neuen Anwendungen veröffentlichen:

  Ein Problem ist aufgetreten bei der Kommunikation mit dem Server.
  Get-AppLibAppVPackage : The maximum message size quota for incoming messages (41943040) has been exceeded. [LD0232]

- Wenn Sie einen Maschinenkatalog für ein Zielgerät erstellen, das auf einem anderen Domänenserver erstellt wurde, wird das Zielgerät möglicherweise nicht erkannt. [LD0319]

- Das Objekt "Citrix Universeller Drucker"wird mit dem universellen EMF-Druckertreiber in einer Sitzung erstellt, selbst wenn Sie die Einstellungen für den universellen Druckertreiber auf **XPS** oder **Native Treiber** festlegen. Installieren Sie zum Erhalt des Fixes Citrix Receiver für Windows 4.9.5000 LTSR kumulatives Update 5 oder eine spätere Version. [LD0360]

- Wenn Sie eine Anwendung über die Anwendungseigenschaften umbenennen und anschließend in Citrix Studio versuchen, die Bereitstellungsgruppe aus der Anwendung zu entfernen, wird folgende Fehlermeldung angezeigt:

  Objekt ist nicht vorhanden.

  Das Problem tritt auf, wenn die Anwendungseigenschaft **ApplicationNameWithFolder** nach Ihrer Änderung des Anwendungsnamens den alten Namen weiterverwendet. [LD0594]

- Beim Hinzufügen von Maschinen zu einer vorhandenen oder neuen Bereitstellungsgruppe mit dem **Assistenten zum Hinzufügen von Maschinen** wird möglicherweise folgender Fehler zurückgegeben:

Maschine ist bereits zugeteilt.

Die Meldung wird nur angezeigt, wenn Sie mindestens ein Mal mithilfe der Schaltfläche "Zurück" zur ersten Assistentenseite zurückkehren. [LD0924]

- Möglicherweise können Sie Maschinen aus anderen Katalogen in einer Bereitstellungsgruppe nicht anzeigen. Das Problem tritt auf, wenn Sie Maschinen mithilfe des **Assistenten zum Hinzufügen von Maschinen** zu einer neuen oder vorhandenen Bereitstellungsgruppe hinzufügen. [LD0988]
- Mit diesem Fix werden der temporäre Datencache sowie "Dem Cache zugewiesener Speicher (MB)"und "Größe des Datenträgercache (GB)"standardmäßig deaktiviert, wenn Sie einen Maschinenkatalog erstellen. [LD1120]

Controller

- Wenn für Bereitstellungsgruppen Mehrfachlizenzen konfiguriert sind, wird möglicherweise eine Lizenz eines falschen, nicht für eine Bereitstellungsgruppe konfigurierten Lizenztyps ausgecheckt. [LC9086]
- In dieser Version wurde die Abhängigkeit von Version 2.0 von PowerShell in eigenständigen Bereitstellungen von Citrix Studio und seinen Komponenten beseitigt.

> **Hinweis:**
> PowerShell ist weiterhin auf den Maschinen erforderlich, auf denen Sie eine oder mehrere dieser Komponenten installieren. Es muss jedoch nicht mehr Version 2.0 sein. Auf Delivery Controllern und StoreFront-Servern ist PowerShell 2.0 weiterhin erforderlich. Unter Windows 7 oder Windows Server 2008 R2 ist PowerShell Version 3.0 oder höher erforderlich, wenn Sie Controller-Komponenten, einschließlich Citrix Studio, installieren. [LD0184]

- Wenn eine Bereitstellungsgruppe einen oder mehrere VDAs im Entlastungsmodus enthält, wird sie möglicherweise nicht zum Starten einer veröffentlichten Anwendung ausgewählt. [LD0194]
- Wenn Sie einer Site mehrere App-V-Pakete hinzufügen, zeigt Studio möglicherweise folgende Fehlermeldung an und der Administrator kann keine neuen Anwendungen veröffentlichen:

  Ein Problem ist aufgetreten bei der Kommunikation mit dem Server.
  Get-AppLibAppVPackage : The maximum message size quota for incoming messages (41943040) has been exceeded. [LD0232]
- Bei Verwendung des PowerShell-Befehls **get-brokericon -filename** mit dem Parameter **-servername** wird ein Fehler gemeldet. [LD0324]
- Über Citrix Virtual Apps veröffentlichte Anwendungen werden evtl. zeitweise nicht aufgelistet. Nach dem Start der Sitzung wird dann ein leerer Bildschirm angezeigt oder die Anwendungen

können nicht gestartet werden. Die CPU des SQL Server-Computers ist möglicherweise stark ausgelastet und in SQL Monitor werden blockierte und ressourcenintensive Prozesse angezeigt. [LD0336]

- Das Objekt "Citrix Universeller Drucker"wird mit dem universellen EMF-Druckertreiber in einer Sitzung erstellt, selbst wenn Sie die Einstellungen für den universellen Druckertreiber auf **XPS** oder **Native Treiber** festlegen. Installieren Sie zum Erhalt des Fixes Citrix Receiver für Windows 4.9.5000 LTSR kumulatives Update 5 oder eine spätere Version. [LD0360]
- Die Ressourcenauslastungsdaten in Citrix Director werden möglicherweise nicht richtig sortiert. Das Problem tritt auf, wenn die SQL-Anweisungen in der falschen Reihenfolge präsentiert werden. [LD0388]
- Wenn Sie eine Sitzung starten, wählt der Broker möglicherweise neu erstellte VDAs anstelle zuvor gestarteter VDAs. Dies kann zu einer erhöhten Anmeldezeit führen. Die Erhöhung tritt auf, wenn die ausgewählte VM die Nachstart-Vorgänge nicht ausgeführt hat, bevor sie eine Sitzungsanforderung erhält. [LD0511]
- Wenn Sie eine Anwendung über die Anwendungseigenschaften umbenennen und anschließend in Citrix Studio versuchen, die Bereitstellungsgruppe aus der Anwendung zu entfernen, wird folgende Fehlermeldung angezeigt:

  Objekt ist nicht vorhanden.

  Das Problem tritt auf, wenn die Anwendungseigenschaft **ApplicationNameWithFolder** nach Ihrer Änderung des Anwendungsnamens den alten Namen weiterverwendet. [LD0594]
- Wenn Sie eine Richtlinie in Citrix Studio ändern, wird möglicherweise folgende Fehlermeldung in der **Konfigurationsprotokollierung**angezeigt.

  Fehler beim Versuch, Details zur Richtlinienänderung zu ermitteln.
- Wenn diese Fehlermeldung angezeigt wird, können Sie die Details der Richtlinienänderung nicht mithilfe der Konfigurationsprotokollierung ermitteln. [LD0596]
- Citrix Director zeigt möglicherweise falsche Benutzerverbindungsfehler an, wenn die Spalte **FailureDate** in der Tabelle **MonitorData.Session** für Sitzungen auf **Null** festgelegt ist. Aufgrund dieses Fehlers werden die Fehlertypen in der Tabelle **MonitorData.ConnectionFailureLog** nicht aktualisiert. Der aus der Monitordatenbank abgerufene Verbindungsfehlerwert stimmt nicht mit dem der **Get-BrokerConnectionLog**-Ausgabe von der Sitedatenbank überein. [LD0726]
- Steht die Erweiterung "vhd"in Großbuchstaben (".VHD"), erkennt die VHD-Auswahl sie möglicherweise nicht als gültiges VHD-Image. Das Problem tritt auf, wenn Sie einen Maschinenerstellungsdienste-Katalog in einer Azure-Umgebung erstellen. [LD0746]
- Die Identitätsdatenträger werden möglicherweise aus den in Amazon Web Services (AWS) vorhandenen Maschinenerstellungsdiensten (MCS) entfernt. [LD1043]

- Bei Verwendung entsprechender Produktversionen kann der Administrator möglicherweise keine Hostverbindung in Studio erstellen, wenn NSX-T-Netzwerk in der VMware-Umgebung aktiviert ist. Das Problem tritt auf, wenn der MCS das opake Netzwerk in NSX-T nicht aufzählt. [LD1102]
- Die HDX-Verbindungsanmeldedaten fehlen möglicherweise im Diagramm der Anmeldedauer. [LD1113]
- `CreateNewInstanceOnReset` ist außer Betrieb genommen. Die VM bleibt beim Aus- und Wiedereinschalten oder Aktualisieren eines Maschinenkatalogs immer erhalten. [LD1114]
- Bei Verwendung von Amazon Web Services (AWS) kann es beim Maschinenneustart zu einer Verzögerung von mehreren Minuten kommen. [LD1220]
- Der Citrix Überwachungsdienst belegt möglicherweise viel Arbeitsspeicher. Infolgedessen reagiert der Delivery Controller nicht mehr und bei den Anrufanforderungen von Director tritt ein Timeout auf. [LD1370]

HDX RealTime Optimization Pack

Die Dokumentation zu HDX RealTime Optimization Pack 7.15 LTSR CU4 enthält Informationen zu den Updates in dieser Version.

Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU4 Dokumentation enthält spezifische Informationen zu den Updates in diesem Release.

Personalisierung für App-V

Studio

- Aus App-V-Paketen kann die falsche Anwendung gestartet werden, wenn der Anwendungsname in einer anderen Sprache als Englisch vorliegt. [LD0222]

VDA

- Aus App-V-Paketen kann die falsche Anwendung gestartet werden, wenn der Anwendungsname in einer anderen Sprache als Englisch vorliegt. [LD0222]

Profilverwaltung

- Wenn Sie sich zum zweiten Mal am Citrix Virtual Apps-Server anmelden, ist das Benutzerprofil beschädigt. Das Problem tritt auf, wenn die Profilverwaltung das Profil beim Abmelden nicht löschen kann, da das Profil vom System verwendet wird. Starten Sie den Profilverwaltungsdienst neu, um das Profil zu löschen. [LD0560]
- Wenn die **CopyFileWithRetries**-Funktion eine Datei in einem Verzeichnis nicht kopieren kann, werden die übrigen Dateien möglicherweise nicht kopiert. Das Problem tritt auf, wenn der Citrix Profilverwaltungsdienst versucht, Dateien aus einem Standardvorlagenprofilverzeichnis in das Profilverzeichnis des aktuellen Benutzers zu kopieren. Während des Kopiervorgangs beendet die entsprechende **CopyDirectory**-Funktion den Kopiervorgang, wenn eine Datei unter dem aktuellen Verzeichnis aufgrund von Berechtigungseinschränkungen nicht kopiert werden kann. Infolgedessen werden andere Dateien nicht kopiert. [LD0648]
- Der VDA für Serverbetriebssysteme wird unter Microsoft Windows 10, Version 1709 oder höher ausgeführt. Wenn Sie die *.tmp-Datei für die Synchronisierung der Profilverwaltungsrichtlinie ausschließen, werden die Änderungen, die Sie an allen Microsoft Office-Dokumenten vornehmen, z. B. Word- und PowerPoint-Dateien beim Abmelden möglicherweise nicht gespeichert. Ihre Änderungen werden nicht beibehalten, wenn Sie sich anmelden und die Dateien neu öffnen. [LD0782]
- Die Umleitung für den AppData(Roaming)-Ordner funktioniert möglicherweise nicht, wenn die Profilverwaltung unter Microsoft Windows 10 ausgeführt wird. Das Problem tritt auf, wenn der AppData(Roaming)-Ordner nicht bereits im Dateispeicherverzeichnis vorhanden ist. [LD0797]

Provisioning Services

Provisioning Services 7.15 LTSR CU4 enthält Informationen zu den Updates in diesem Release.

Sitzungsaufzeichnung

Verwaltung

- Mit der Sitzungsaufzeichnung kann es zu Skalierbarkeits- und Leistungsproblemen kommen. [LD0970]
- Versuche, Sitzungsaufzeichnung von Version 7.15 auf Version 7.15 Kumulatives Update 2 zu aktualisieren, können sehr lange dauern. [LD1042]

Agent

- Versuche, den Sitzungsaufzeichnungsagent Version 7.15 Kumulatives Update 3 auf der französischen und spanischen Version des Microsoft Windows-Betriebssystems zu installieren, schlagen möglicherweise fehl. [LD1161]

Player

- Wenn Sie die Verbindung zu einer getrennten Sitzung wiederherstellen, zeigt der Sitzungsaufzeichnungsplayer den vollständigen Pfad der Anwendung zur ausführbaren Datei für die Sitzung an. Stattdessen müsste der Name der veröffentlichten Anwendung für die Sitzung angezeigt werden. [LD0426]
- Der Sitzungsaufzeichnungsplayer Version 7.15, kumulatives Update 2, kann aufgenommene Dateien möglicherweise nicht wiedergeben und reagiert nicht mehr, wenn der Sitzungsaufzeichnungsplayer als Anwendung gestartet wird. [LD0578]

StoreFront

- Wenn Sie einen StoreFront mit einer Basis-URL konfigurieren, die einen Unterstrich (_) enthält und ihn mit Citrix Gateway verwenden, kann ein Fehler auftreten. [LC9678]
- Wenn Sie sich bei StoreFront anmelden und die Citrix Receiver für Web-Seite aktualisieren, wird das Dialogfeld für die Zeitüberschreitung möglicherweise unterdrückt. [LD0214]
- Bei der Anmeldung bei StoreFront kann der Fehler **Ihre Anforderung kann nicht abgeschlossen werden** auftreten. Das Problem tritt auf, wenn die dynamischen TCP-Ports aufgebraucht sind. [LD0573]
- Nach dem Upgrade von StoreFront 3.5 auf 3.12 können die folgenden Ereignisprotokolldetails in der Ereignisanzeige angezeigt werden:

  Authentifizierung mit Benutzername und Kennwort ist nicht aktiviert in StoreFront. Citrix.DeliveryServicesClients.Authentication.Exceptions.ProtocolNotAvailableException, Citrix.DeliveryServicesClients.Authentication, Version=3.12.0.0, Culture=neutral, PublicKeyToken=null Invalid protocol exception. Das angeforderte Protokoll ist: ExplicitForms Protocol: ExplicitForms at Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.Crea
  [LD0608]
- Die Meldung **Im Moment sind keine Apps oder Desktops verfügbar** wird weiterhin angezeigt, wenn verfügbare Apps oder Desktops angezeigt werden. [LD0857]

- Bei Verwendung des Browsers Safari 12 und höher kann die Clienterkennung unter Citrix Receiver für Web fehlschlagen, da die NPAPI-Schnittstelle nicht länger unterstützt wird. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX238286. [LD0863]
- Sie deaktivieren die **Desktop Viewer**-Symbolleiste für eine Bereitstellungsgruppe, indem Sie die Eigenschaft **ConnectionBar = 0** in jedem Anwendungsabschnitt der Datei default.ica im Store hinzufügen. Wenn Sie die Verbindung der Sitzung trennen und wiederherstellen, wird die **Desktop Viewer**-Symbolleiste wieder angezeigt. [LD1051]
- Die Reihenfolge der Secure Ticket Authoritys (STAs) kann in der StoreFront-Verwaltungskonsole nur geändert werden, wenn die Option **Lastausgleich von mehreren STA-Servern** ausgewählt ist. Die Logik müsste umgekehrt vorgeben, dass die STA-Reihenfolge nur geändert werden kann, wenn die Option **Lastausgleich von mehreren STA-Servern** nicht ausgewählt ist. [LD1118]
- Die Standardwebsiteeinstellung wird den anderen Knoten in einer On-Premises-Gruppe mit mehreren Servern möglicherweise nicht korrekt angezeigt. Der Browser wird dann an die HTTP-URL für den Knoten anstelle der richtigen URL weitergeleitet. [LD1119]
- Dieser Fix behebt ein Sicherheitsrisiko. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX251988. [LD1361]

Universeller Druckserver

Client

- Bevor Sie ein Dokument drucken, wählen Sie im Druckdialogfeld der veröffentlichten Desktopsitzung einen Drucker aus der Liste der verfügbaren Drucker aus. Es kann zu einer Verzögerung kommen, bis der Drucker mit dem Drucken des Dokuments beginnt. [LC9601]
- Der Druckspoolerdienst wird möglicherweise unerwartet beendet. Das Problem tritt auf, wenn **CRawStreamHeaderWriter::EndPage** und **CRawStreamHeaderWriter::StartPage** versuchen, auf ein NULL-Objekt zuzugreifen. [LC7893]
- Nach der Installation eines VDA werden die Druckerports in den Druckereigenschaften für einen zugeordneten Netzwerkdrucker möglicherweise nicht mehr angezeigt. [LD0949]

Server

- Aufgrund einer Zugriffsverletzung wird der universelle Druckserver (UPServer.exe) möglicherweise unerwartet beendet und Ereignis 7031 generiert. [LC7821]
- Eine Zugriffsverletzung in **CPTStream::ThisStream** kann dazu führen, dass der Druckerspoolerdienst nicht mehr reagiert. [LC8856]

- Benutzer, die Mitglieder vieler Active Directory-Gruppen sind, können möglicherweise keine Verbindung zu ihren Druckern über den universellen Druckserver herstellen. [LC8714]
- Die Menüs für erweiterte Druckfunktionen (z. B. Heften oder Druckmaterialbehälterwahl) des universellen Citrix-Druckertreibers können leer sein. [LC9711]

VDA für Desktopbetriebssystem

HDX RealTime Windows Media-Umleitung

- Citrix HDX RealTime Media Engine wird möglicherweise unerwartet beendet, wenn Sie versuchen, auf die HDX-Webkamera zuzugreifen. [LD0062]
- Wenn die **HDX MediaStream Windows Media-Umleitung** deaktiviert ist, kann beim Versuch des Öffnens bestimmter Videodateiformate in Windows Media Player folgende Fehlermeldung angezeigt werden:

  Beim Wiedergeben der Datei ist in Windows Media Player ein Problem aufgetreten.

  Bei einigen Videodateiformaten ist das Videoseitenverhältnis jedoch falsch. [LD0279]

Tastatur

- Bei Verwenden des chinesischen Tastaturlayouts in einer Benutzersitzung wechselt der Eingabemethoden-Editor (IME) automatisch zur Wubi-Eingabemethode für chinesische Zeichen. Das Problem tritt auf, wenn der Standard-IME nicht auf **Wubi**festgelegt ist. [LD0429]

Drucken

- Nach dem Upgrade von XenApp und XenDesktop von Version 7.9 auf Version 7.15 können Sie möglicherweise keine Drucke in einem anderen Ausgabefach ausgeben lassen. Es wird das Standardausgabefach verwendet, obwohl Sie im Dialogfeld "Drucken"ein anderes Fach auswählen können. [LC9247]
- Wenn Sie eine PDF-Datei im Rohdatenformat an die Druckwarteschlange senden, wird die PDF-Datei möglicherweise nicht gedruckt. [LC9755]
- Wenn Sie versuchen, eine Seite zu drucken, wird das Fenster für die Druckeinstellungen möglicherweise nicht korrekt angezeigt. Das Problem tritt bei Übersetzungsproblemen im Druckeinstellungsfenster auf. Hierdurch werden das **Citrix** Symbol und der Name der Schaltfläche **Lokale Druckereinstellungen** abgeschnitten. [LD0359]

- Microsoft Windows Server 2016 kann den Wert des Registrierungsschlüssels **HKEY_CURRENT_USER\SOFTW NT\CurrentVersion\Windows\Device**nicht aktualisieren, wenn der Standarddrucker der zugeordnete Citrix Drucker ist. Aufgrund dieses Fehlers ist der Standarddrucker für andere als .NET-Anwendungen möglicherweise nicht festgelegt. [LD1032]

Sitzung/Verbindung

- Bestimmte Anwendungen von Drittanbietern bleiben in Seamlesssitzungen möglicherweise hängen, bis Sie die Sitzung mit der Tastenkombination Umschalten + F2 in den Fenstermodus und dann wieder in den Seamlessmodus schalten. [LC9727]
- Wenn Sie die veröffentlichten Anwendungen maximieren, überlagern sie möglicherweise den oberen Bereich der Taskleiste. [LD0025]
- Wenn die Einstellung **Secure ICA aktivieren** in einer Bereitstellungsgruppe aktiviert und der Parameterwert **DHParaml** nicht im Registrierungsschlüssel "HKEY_LOCAL_MACHINE\System\CurrentControlS vorhanden ist, werden Anwendungen möglicherweise nicht gestartet. Die folgende Fehlermeldung wird angezeigt:

  Die Anwendung konnte nicht gestartet werden. Wenden Sie sich an Ihren Helpdesk und nennen Sie folgenden Fehler:
  Cannot connect to the Citrix XenApp server.protocol Driver error Desktop Viewer. The connection to "VOA Win 7 LTSR"failed with status (Unknown client error). [LD0117]
- Bei der Verarbeitung von Kreditkartentransaktionen über ein Benutzergerät können Anwendung und Benutzergerät aufhören zu reagieren oder es wird möglicherweise nur eine Teilmenge der Daten empfangen. [LD0152]
- Das Starten einer Anwendung von einem beliebigen Server aus kann fehlschlagen. Die folgende Fehlermeldung wird angezeigt:

  Die Anwendung konnte nicht gestartet werden. Es kann keine Verbindung zum Citrix XenApp-Server hergestellt werden. Der ausgewählte Citrix SSL-Server akzeptiert keine Verbindungen.

  Das Problem tritt auf, wenn der Server keine Verbindungen auf einem für SSL aktivierten VDA akzeptiert. [LD0239]
- Dieser Fix behebt ein Speicherleck, das auftritt, wenn die Richtlinie **Clientlaufwerke automatisch verbinden** deaktiviert ist. [LD0370]
- Die Funktion, die einen Thread im TWI-Modul (twi3.dll) beendet, kann dazu führen, dass der Server nicht mehr reagiert. [LD0406]
- Wenn der lokale App-Zugriff aktiviert ist und Sie Anwendungen auf veröffentlichten Desktops unter Microsoft Windows 10 Version 1803 öffnen, können die Anwendungen nicht minimiert

werden. [LD0411]

- Die Benutzergerätesitzung reagiert möglicherweise einige Minuten lang nicht mehr, wenn bestimmte Anwendungen von Drittanbietern verwendet werden. [LD0419]
- Sie öffnen eine E-Mail eines Google-Kontos in Internet Explorer, Chrome oder einem Firefox. Wenn Sie versuchen, eine neue E-Mail zu verfassen, funktioniert die Funktion **Automatische Anzeige der Tastatur** möglicherweise nicht. [LD0470]
- Anwendungen im Seamlessmodus reagieren möglicherweise nicht mehr, wenn Sie die Größe von "Maximiert"in "Fenstermodus"ändern oder umgekehrt. [LD0498]
- Ein Zielgerät kann unerwartet neu gestartet werden, wenn die scardhook64.dll die Ausnahme X64_CRITICAL_PROCESS_FAULT_INVALID_POINTER_READ_IN_CALL verursacht. [LD0504]
- Das Wiederherstellen einer Verbindung mit einer Sitzung kann fehlschlagen, wenn Sie **AutoLogon** auf einen Wert ungleich Null festlegen und die Citrix Diagnostics Facility-Ablaufverfolgung ausführen. [LD0602]
- Ein Teil des Fensters einer veröffentlichten Anwendung wird möglicherweise nicht aktualisiert. Das Problem kann auftreten, wenn eine im Hintergrund ausgeführte veröffentlichte Citrix Anwendung im Vordergrund angezeigt wird. [LD0711]
- Wenn Sie bestimmte Aufzeichnungsanwendungen von Drittanbietern auf einem veröffentlichten Desktop verwenden, wird Internet Explorer möglicherweise unerwartet beendet. [LD0830]
- Mit diesem Fix versucht der CtxUvi Hooking-Treiber nicht mehr, MfApHook.dll auf einen sicheren Prozess zu laden. [LD0847]
- Veröffentlichte Anwendungen werden möglicherweise blockiert, während auf eine Antwort von der Standort-API gewartet wird.

  Zum Implementieren des Fixes durch Konfigurieren eines Timeouts legen Sie folgende Registrierungsschlüssel fest:

  - *Auf 32-Bit-Systemen:*

    HKEY_LOCAL_MACHINES\SOFTWARE\Citrix\Location

    Name: LatlongWaitTime

    Typ: REG_DWORD

    Wert: Millisekunden. Der Standardwert ist 60000 Millisekunden. Der Wert ist die beim Abrufen der Standortinformationen zulässige Wartezeit.

  - *Auf 64-Bit-Systemen*

    HKEY_LOCAL_MACHINES\SOFTWARE\Wow6432Node\Citrix\Location

Name: LatlongWaitTime

Typ: REG_DWORD

Wert: Millisekunden. Der Standardwert ist 60000 Millisekunden. Der Wert ist die beim Abrufen der Standortinformationen zulässige Wartezeit. [LD0905]

- Mit diesem Fix kann der CtxUvi-Treiber den vmsp.exe-Prozess vom Laden von Citrix DLLs ausschließen. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX107825. [LD1024]
- Ein Problem kann auftreten, wenn Sie die Tasten Strg + Alt + Entf wiederholt in der lokalen Konsole drücken, während ein Anderer in der Benutzersitzung für dieselbe Aktion gleichzeitig **Nicht zulassen** auswählt. Ein neuer lokaler Konsolenbildschirm wird möglicherweise 30 Sekunden lang angezeigt. Dadurch erscheint der Inhalt der Konsole als zusätzlicher virtueller Bildschirm für dieselbe Sitzung. [LD1077]

Systemausnahmen

- Nach dem Upgrade eines Zielgeräts von Version 7.6 auf Version 7.15 werden Internet Explorer, Windows Media Player und der Themes-Dienst möglicherweise unerwartet beendet. [LC9872]
- Wenn Sie von einer VM gehostete Anwendungen starten, wird der Prozess mmvdhost.exe möglicherweise unerwartet beendet. [LC9976]
- Auf VDAs kann es in wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x3b (SYSTEM_SERVICE_EXCEPTION) kommen. [LD0089]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 kommen. [LD0119]
- Eine Zugriffsverletzung kann auf VDAs zu einer schwerwiegenden Ausnahme mit Bluescreen führen. [LD0281]
- Auf VDAs kann es bei vd3dk.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [LD0368]
- Der wfshell.exe-Prozess kann auf dem VDA aufgrund der Ausnahme **DivideByZeroException** unerwartet beendet werden. Es wird die Fehlermeldung **wfshell shell has stopped working** angezeigt. [LD0373]
- Auf VDAs kann es in wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x50 kommen. [LD0410]
- Aufgrund einer LIST_ENTRY-Beschädigung kann es auf VDAs bei CtxUVI.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [LD0421]
- Der wfshell.exe-Prozess wird möglicherweise unerwartet beendet, wenn Sie versuchen, auf lange URLs in einer veröffentlichten Instanz von Internet Explorer zuzugreifen. [LD0454]

- Aufgrund eines Nullzeigers kann der mmvdhost.exe-Prozess unerwartet beendet werden, wenn Sie sich bei einem VDA anmelden. [LD0474]
- Der Internet Explorer-Prozess (iexplore.exe) wird möglicherweise unerwartet mit dem Ausnahmecode **0xc00001a5** beendet. Das Problem tritt beim Abladen des fehlerhaften Moduls CtxSensVcLibDll.dll auf. [LD0485]
- Wenn Sie versuchen, Videoclips auf einem VDA für Desktopbetriebssysteme zu exportieren, werden bestimmte Anwendungen von Drittanbietern möglicherweise unerwartet beendet. [LD0506]

Benutzererfahrung

- Auf Windows 10-Clients kann die die Einstellung des hochauflösenden Monitors von 100 dpi erhöht werden. [LD0131]
- Wenn Sie mit der Maus auf ein Objekt zeigen, wird die QuickInfo möglicherweise ausgeblendet und die Anwendung verliert den Fokus. [LD0365]
- Wenn Sie die Verbindung zu einer Sitzung wiederherstellen, wird das Symbol für Verlustfreiheit im Benachrichtigungsbereich des Benutzergeräts ausgeblendet. Zur Umgehung dieses Problems legen Sie folgenden Registrierungsschlüssel fest [LD0919]:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator\Interval
Type: DWORD
Value: 3 (default: 0)

Benutzeroberfläche

- Wenn Sie während des Versuchs der Wiederverbindung einer getrennten Sitzung eine auf einer VM gehostete Anwendung starten, werden alle in der Sitzung vorhandenen Anwendungen angezeigt. [LD0189]
- Sie haben Fix LD0419 angewendet. Wenn Sie versuchen, die Cursorform in einer Anwendung zu ändern, ohne den Cursornamen zu ändern, wird die Cursorform möglicherweise nicht geändert. [LD0983]

VDA für Serverbetriebssystem

HDX MediaStream Windows Media-Umleitung

- Sie verwenden HDX MediaStream Windows Media-Umleitung und Windows Media Player, um VC-1-Livestreams umzuleiten. Es kann ein Fallback auf das serverseitige Rendering der

Livestreams erfolgen. [LD0251]

- Citrix HDX RealTime Media Engine wird möglicherweise unerwartet beendet, wenn Sie versuchen, auf die HDX-Webkamera zuzugreifen. [LD0062]
- Wenn die **HDX MediaStream Windows Media-Umleitung** deaktiviert ist, kann beim Versuch des Öffnens bestimmter Videodateiformate in Windows Media Player folgende Fehlermeldung angezeigt werden:

  Beim Wiedergeben der Datei ist in Windows Media Player ein Problem aufgetreten.

  Bei einigen Videodateiformaten ist das Videoseitenverhältnis jedoch falsch. [LD0279]

Tastatur

- Bei Verwenden des chinesischen Tastaturlayouts in einer Benutzersitzung wechselt der Eingabemethoden-Editor (IME) automatisch zur Wubi-Eingabemethode für chinesische Zeichen. Das Problem tritt auf, wenn der Standard-IME nicht auf **Wubi**festgelegt ist. [LD0429]

Drucken

- Nach dem Upgrade von XenApp und XenDesktop von Version 7.9 auf Version 7.15 können Sie möglicherweise keine Drucke in einem anderen Ausgabefach ausgeben lassen. Es wird das Standardausgabefach verwendet, obwohl Sie im Dialogfeld "Drucken"ein anderes Fach auswählen können. [LC9247]
- Wenn Sie eine PDF-Datei im Rohdatenformat an die Druckwarteschlange senden, wird die PDF-Datei möglicherweise nicht gedruckt. [LC9755]
- Microsoft Windows Server 2016 kann den Wert des Registrierungsschlüssels **HKEY_CURRENT_USER\SOFTW**
  NT\CurrentVersion\Windows\Devicenicht aktualisieren, wenn der Standarddrucker der zugeordnete Citrix Drucker ist. Aufgrund dieses Fehlers ist der Standarddrucker für andere als .NET-Anwendungen möglicherweise nicht festgelegt. [LD1032]

Sitzung/Verbindung

- Bestimmte Anwendungen von Drittanbietern bleiben in Seamlesssitzungen möglicherweise hängen, bis Sie die Sitzung mit der Tastenkombination Umschalten + F2 in den Fenstermodus und dann wieder in den Seamlessmodus schalten. [LC9727]
- Bei der Audiowiedergabe mit hoher Audioqualität ist möglicherweise ein Knistern oder Knallen zu hören. Das Problem tritt auf, wenn Sie das Audio für einige Sekunden anhalten und dann erneut starten. [LC9975]

- Wenn Sie die veröffentlichten Anwendungen maximieren, überlagern sie möglicherweise den oberen Bereich der Taskleiste. [LD0025]
- Wenn die Einstellung **Secure ICA aktivieren** in einer Bereitstellungsgruppe aktiviert und der Parameterwert **DHParaml** nicht im Registrierungsschlüssel "HKEY_LOCAL_MACHINE\System\CurrentControlS vorhanden ist, werden Anwendungen möglicherweise nicht gestartet. Die folgende Fehlermeldung wird angezeigt:

  Die Anwendung konnte nicht gestartet werden. Wenden Sie sich an Ihren Helpdesk und nennen Sie folgenden Fehler:
  Cannot connect to the Citrix XenApp server.protocol Driver error Desktop Viewer. The connection to "VOA Win 7 LTSR"failed with status (Unknown client error). [LD0117]
- Bei der Verarbeitung von Kreditkartentransaktionen über ein Benutzergerät können Anwendung und Benutzergerät aufhören zu reagieren oder es wird möglicherweise nur eine Teilmenge der Daten empfangen. [LD0152]
- Das Starten einer Anwendung von einem beliebigen Server aus kann fehlschlagen. Die folgende Fehlermeldung wird angezeigt:

  Die Anwendung konnte nicht gestartet werden. Es kann keine Verbindung zum Citrix XenApp-Server hergestellt werden. Der ausgewählte Citrix SSL-Server akzeptiert keine Verbindungen.

  Das Problem tritt auf, wenn der Server keine Verbindungen auf einem für SSL aktivierten VDA akzeptiert. [LD0239]
- Dieser Fix behebt ein Speicherleck, das auftritt, wenn die Richtlinie **Clientlaufwerke automatisch verbinden** deaktiviert ist. [LD0370]
- Die Funktion, die einen Thread im TWI-Modul (twi3.dll) beendet, kann dazu führen, dass der Server nicht mehr reagiert. [LD0406]
- Wenn der lokale App-Zugriff aktiviert ist und Sie Anwendungen auf veröffentlichten Desktops unter Microsoft Windows 10 Version 1803 öffnen, können die Anwendungen nicht minimiert werden. [LD0411]
- Serverbetriebssystem-VDAs können sporadisch neu registriert werden, wenn eine "Außer Betrieb"-Benachrichtigung an die Delivery Controller gesendet wird. [LD0466]
- Sie öffnen eine E-Mail eines Google-Kontos in Internet Explorer, Chrome oder einem Firefox. Wenn Sie versuchen, eine neue E-Mail zu verfassen, funktioniert die Funktion **Automatische Anzeige der Tastatur** möglicherweise nicht. [LD0470]
- Anwendungen im Seamlessmodus reagieren möglicherweise nicht mehr, wenn Sie die Größe von "Maximiert"in "Fenstermodus"ändern oder umgekehrt. [LD0498]

- Ein Zielgerät kann unerwartet neu gestartet werden, wenn die scardhook64.dll die Ausnahme X64_CRITICAL_PROCESS_FAULT_INVALID_POINTER_READ_IN_CALL verursacht. [LD0504]
- Bei der Aufzählung von Audiogeräten auf dem Endpunkt kann ein Timeout auftreten. Für die Sitzung gibt es dann kein Audio. [LD0663]
- Ein Teil des Fensters einer veröffentlichten Anwendung wird möglicherweise nicht aktualisiert. Das Problem kann auftreten, wenn eine im Hintergrund ausgeführte veröffentlichte Citrix Anwendung im Vordergrund angezeigt wird. [LD0711]
- Seamlessanwendungen werden im Modus mit fester Größe gestartet. Das Problem tritt auf, wenn die Netzwerkverbindung bei deaktivierter Sitzungszuverlässigkeit unterbrochen und dann wiederhergestellt wird. [LD0733]
- Mit diesem Fix kann der CtxUvi Hooking-Treiber sichere Prozesse vom Laden von Citrix DLLs ausschließen. [LD0847]
- Veröffentlichte Anwendungen werden möglicherweise blockiert, während auf eine Antwort von der Standort-API gewartet wird.

  Zum Implementieren des Fixes durch Konfigurieren eines Timeouts legen Sie folgende Registrierungsschlüssel fest:

  - *Auf 32-Bit-Systemen:*

    HKEY_LOCAL_MACHINES\SOFTWARE\Citrix\Location

    Name: LatlongWaitTime

    Typ: REG_DWORD

    Wert: Millisekunden. Der Standardwert ist 60000 Millisekunden. Der Wert ist die beim Abrufen der Standortinformationen zulässige Wartezeit.

  - *Auf 64-Bit-Systemen*

    HKEY_LOCAL_MACHINES\SOFTWARE\Wow6432Node\Citrix\Location

    Name: LatlongWaitTime

    Typ: REG_DWORD

    Wert: Millisekunden. Der Standardwert ist 60000 Millisekunden. Der Wert ist die beim Abrufen der Standortinformationen zulässige Wartezeit. [LD0905]
- Mit diesem Fix kann der CtxUvi-Treiber den vmsp.exe-Prozess vom Laden von Citrix DLLs ausschließen. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX107825. [LD1024]
- Nachdem Sie den VDA auf Version 7.15 CU 3 aktualisiert haben, ist der Anwendungsstart möglicherweise langsam. Das Problem tritt auf, wenn für die Benutzergruppen **Sichtbarkeit einschränken** konfiguriert ist. [LD1215]

Systemausnahmen

- Wenn Sie von einer VM gehostete Anwendungen starten, wird der Prozess mmvdhost.exe möglicherweise unerwartet beendet. [LC9976]
- Auf VDAs kann es in wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x3b (SYSTEM_SERVICE_EXCEPTION) kommen. [LD0089]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 kommen. [LD0119]
- Eine Zugriffsverletzung kann auf VDAs zu einer schwerwiegenden Ausnahme mit Bluescreen führen. [LD0281]
- Der wfshell.exe-Prozess kann auf dem VDA aufgrund der Ausnahme **DivideByZeroException** unerwartet beendet werden. Es wird die Fehlermeldung **wfshell shell has stopped working** angezeigt. [LD0373]
- Auf VDAs kann es in wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x50 kommen. [LD0410]
- Aufgrund einer LIST_ENTRY-Beschädigung kann es auf VDAs bei CtxUVI.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [LD0421]
- Der wfshell.exe-Prozess wird möglicherweise unerwartet beendet, wenn Sie versuchen, auf lange URLs in einer veröffentlichten Instanz von Internet Explorer zuzugreifen. [LD0454]
- Der Internet Explorer-Prozess (iexplore.exe) wird möglicherweise unerwartet mit dem Ausnahmecode **0xc00001a5** beendet. Das Problem tritt beim Abladen des fehlerhaften Moduls CtxSensVcLibDll.dll auf. [LD0485]

Benutzererfahrung

- Wenn Sie mit der Maus auf ein Objekt zeigen, wird die QuickInfo möglicherweise ausgeblendet und die Anwendung verliert den Fokus. [LD0365]

Benutzeroberfläche

- Wenn Sie während des Versuchs der Wiederverbindung einer getrennten Sitzung eine auf einer VM gehostete Anwendung starten, werden alle in der Sitzung vorhandenen Anwendungen angezeigt. [LD0189]
- Die Grafiken, die auf den Desktops angezeigt werden, sind möglicherweise beschädigt. [LD1115]

Cumulative Update 3 (CU3)

September 16, 2021

Releasedatum: 29. Oktober 2018

Info zu diesem Release

Das kumulative Update 3 (CU3) für XenApp und XenDesktop 7.15 LTSR behebt über 200 seit 7.15 LTSR CU2 gemeldete Probleme.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR CU2 behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Downloads

Download von 7.15 LTSR CU3

Neue Features in diesem kumulativen Update

Die Browserinhaltsumleitung ist eine neuerdings kompatible Komponente von XenApp und XenDesktop 7.15 LTSR, die als separater Download verfügbar ist. Weitere Informationen zur Browserinhaltsumleitung in diesem kumulativen Update finden Sie unter XenApp und XenDesktop 7.15 LTSR-kompatible Komponenten im Abschnitt *Browserinhaltsumleitung*.

Neue Bereitstellungen

Wie stelle ich das CU3 von Grund auf bereit?

Mit dem CU3-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf CU3 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU3 umfasst Updates für Basiskomponenten von 7.15 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU3 zu aktualisieren. Beispiel: Wenn Provisioning Services zur LTSR-Bereitstellung gehört, aktualisieren Sie die Provisioning Services-Komponenten auf die CU3-Version. Wenn Provisioning Services nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU3

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.3000	
VDA für Serverbetriebssystem	7.15.3000	
Delivery Controller	7.15.3000	
Citrix Studio	7.15.3000	
Citrix Director	7.15.3000	
Gruppenrichtlinienverwaltung	3.1.3000	
StoreFront	3.12.3000	
Provisioning Services	7.15.9	
Universeller Druckserver	7.15.3000	
Sitzungsaufzeichnung	7.15.3000	nur Platinum Edition
Linux VDA	7.15.3000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15.3000	
Verbundauthentifizierungsdienst	7.15.3000	

XenApp und XenDesktop 7.15 LTSR CU3-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht

beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU3 kompatible Komponenten und Plattformen	Version
App Layering	4.15.0
*Browserinhaltsumleitung	15.15
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.4.2000
Lizenzserver	11.15.0.0 Build 25000
Self-Service-Kennwortzurücksetzung	1.1.10.0
Workspace Environment Management	4.7

***Browserinhaltsumleitung**

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um. Weitere Informationen finden Sie unter Umleitung des Browserinhalts.

Systemanforderungen:

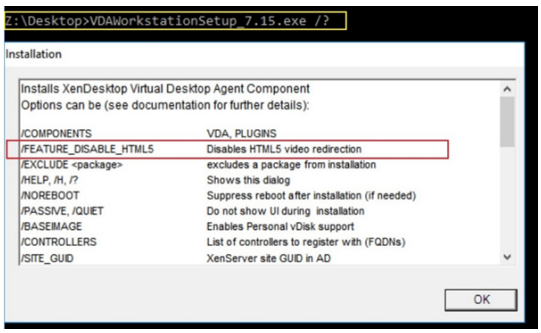
Diese Anforderungen gelten für das BCR.msi mit XenApp und XenDesktop 7.15 LTSR CU3. Ignorieren Sie sämtliche für andere Versionen von XenApp, XenDesktop und Citrix Virtual Apps and Desktops aufgeführten Systemanforderungen für die Browserinhaltsumleitung.

- Version 7.15 LTSR CU3 auf dem Delivery Controller und dem VDA.
- Citrix Workspace-App 1809 oder später für Windows.

- BCR.msi –verfügbar auf der Citrix Downloadseite.
- Chrome (mit installierter Browserinhaltsumleitungserweiterung aus dem Chrome WebStore) oder Internet Explorer 11 (mit aktiviertem Browser Helper Object (BHO) Citrix HDXJSInjector).

Installation:

1. Installieren Sie über die Befehlszeilenoption /FEATURE_DISABLE_HTML5 Version 7.15 LTSR CU3 des VDA (bzw. führen Sie ein Upgrade auf diese Version durch).



   Diese Option entfernt die HTML5-Videoumleitung, was vor dem Ausführen des BCR.msi-Pakets erforderlich ist. Durch das BCR.msi werden das Feature selbst sowie die entsprechenden Dienste während der Installation wieder hinzugefügt. Öffnen Sie nach diesem Schritt die services.msc-Konsole und vergewissern Sie sich, dass **Citrix HDX HTML5 Video Redirection Service** nicht aufgeführt wird.

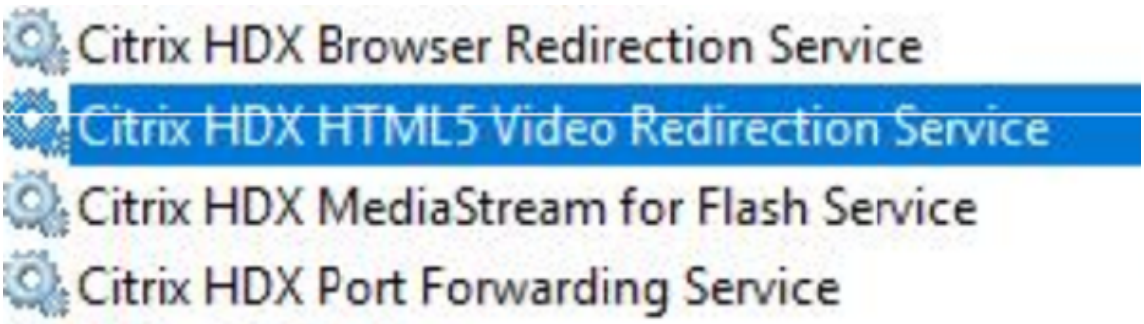
2. Starten Sie die Installation der Browserinhaltsumleitung mit dem BCR.msi. Systemabhängig werden die BCR.msi-Dateien unter einem der folgenden Pfade installiert:

   C:\Programme\Citrix\ICAService

   oder

   C:\Programme(86)\Citrix\ICAService

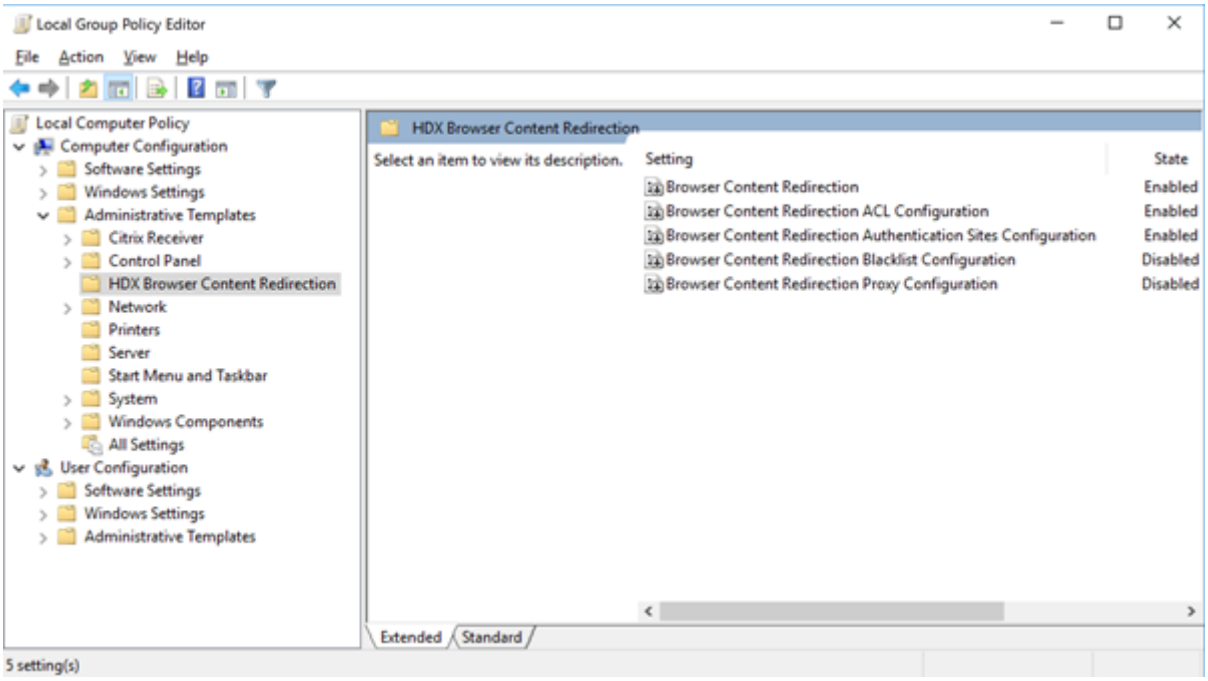
   Da die Installation schnell erfolgt, wird das Dialogfeld möglicherweise schnell geschlossen. Führen Sie in diesem Fall services.msc erneut aus, um zu prüfen, ob die Dienste hinzugefügt wurden.



Richtlinien:

Sie können Richtlinien über Registrierungseinträge unter HKEY_LOCAL_MACHINE auf dem VDA oder die administrative Vorlage **HDX Browser Content Redirection** von Citrix für die Gruppenrichtlinien-Verwaltungskonsole steuern.

Sie können die Vorlage von citrix.com unter Citrix Virtual Apps and Desktops (XenApp & XenDesktop) > XenApp 7.15 LTSR / XenDesktop 7.15 LTSR > Components herunterladen. Citrix Studio enthält diese Richtlinien nicht.



Weitere Informationen finden Sie unter Richtlinieneinstellungen für die Browserinhaltsumleitung. Informationen zur Problembehandlung finden Sie im Knowledge Center-Artikel CTX230052.

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und

die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonyme Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren/aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp LTSR 7.15 CU3. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der XenApp 7.15-LTSR CU3-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU3-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen VDA (Virtual Delivery Agent) für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU3-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU3-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

August 18, 2021

Citrix Director

- Der Versuch eines delegierten Administrators mit einer benutzerdefinierten Rolle, die Benutzerzuweisung von einem Desktop mit Citrix Studio, PowerShell oder Citrix Director zu entfernen, kann fehlschlagen. Das Problem tritt auf, wenn benutzerdefinierte Administratoren Berechtigung zum Ausführen dieser Vorgänge für Bereitstellungsgruppen aber nicht für Maschinenkataloge haben. [LC8174]
- Die Suche nach Benutzern, um sie Maschinen zuweisen, schlägt möglicherweise fehl. Der ausgewählte Benutzer wird als Null angezeigt. [LC8395]
- Citrix Director meldet möglicherweise Multi-Stream-ICA als inaktiv, wenn das **UDP-based Data Transfer Protocol (UDT)** verwendet wird. Das Problem tritt auf, wenn der HDX-WMI-Anbieter nicht für EDT- oder UDT-Sitzungen aktualisiert wird. [LC8960]
- Die CPU-Auslastung durch den Prozess w3wp.exe kann unter Citrix Director sehr hoch sein. [LC9222]
- Wenn Sie bestimmte Browsersprachen einstellen und Citrix Director starten, wird im Sitzungsdetailbereich möglicherweise eine Sitzung als aktiv angezeigt, selbst wenn keine Sitzungen ausgeführt werden. [LC9392]

- Bei Verwendung von Citrix Director werden in Microsoft Internet Explorer 11 möglicherweise nicht funktionsfähige Scrollleisten im Bereich **Maschinendetails** auf der Seite **Filter** > **Maschinen** > **Alle Maschinen** angezeigt. [LC9505]
- Auf der Seite **Trends** in **Citrix Director** fügt Internet Explorer möglicherweise Google Analytics (https://www.google-analytics.com) automatisch als vertrauenswürdige Website hinzu. Diese Aktion von Internet Explorer kann nicht unterbunden werden. Selbst wenn Sie die automatischen Uploads unter dem Registrierungsschlüsselwert **SendExperienceMetrics** HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall deaktivieren, werden Google Analytics-Aufrufe auf dem Citrix Director-Dashboard und auf der Seite "Anwendungen"eingerichtet. Um automatische Uploads zu deaktivieren, verwenden Sie das unter Citrix Insight Services beschriebene Verfahren. Nachdem Sie diesen Fix angewendet haben, wird bei einer Citrix Director-Anmeldung ein Ping an Google Analytics ausgeführt, die Daten werden jedoch nicht hochgeladen. [LC9736]
- In den CSV-Berichten der Anmeldungsleistung in Citrix Director wird möglicherweise die UTC-Zeitzone anstelle der lokalen Zeitzone verwendet. [LC9854]
- Einige Administratoren können möglicherweise nicht auf manche Domänen zugreifen, die der web.config-Domänenliste hinzugefügt wurden. Bei der Suche nach einer Benutzersitzung kann infolgedessen eine Ausnahme auftreten und die Sitzungsdetails werden nicht angezeigt. [LC9865]
- Der Wert für **ExportCsvDrilldownLimit** wird möglicherweise nicht auf benutzerdefinierte Berichte in Citrix Director angewendet. [LD0004]

Citrix Richtlinie

- Wenn Sie die Loopback-Richtlinie im Zusammenführungsmodus auf einen VDA anwenden und die StoreFront-URL einer Bereitstellungsgruppe des VDAs in Citrix Studio hinzufügen, werden die Symbole veröffentlichter Anwendungen möglicherweise doppelt angezeigt. [LC8889]
- Das Erstellen eines Maschinenkatalogs schlägt möglicherweise mit der Meldung fehl, dass die Zusammenfassung nicht erstellt werden kann. Bei Verwendung des Assistenten zum Erstellen von Katalogen ist außerdem vor Anzeige der Ausnahme die Dropdownliste der Domänen leer. [LC9636]
- Wenn Sie das Tool "Gruppenrichtlinienergebnisse"über die Gruppenrichtlinien-Verwaltungskonsole auf einer Maschine mit VDA-Version 7.15.2000 ausführen, wird folgende Fehlermeldung angezeigt: **An error occurred while generating report: Not Found** [LC9825]
- Der Citrix Druckmanagerdienst (cpsvc.exe) wird möglicherweise unerwartet beendet. Das Problem tritt auf, wenn der mit einem Gruppenrichtlinienobjekt verbundene Druckregistrierungsschlüssel Garbage-Einträge enthält. [LC9921]

- Das Gruppenrichtlinienmodul fügt möglicherweise nicht alle Werte in den Registrierungsschlüssel **ApplicationStartDetails** ein. Der Start von App-V-Anwendungen kann dann fehlschlagen. [LC9942]
- Wenn Registrierungseinträge manuell in Sitzungsschlüsseln unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix eingetragen werden, werden die Schlüssel beim Sitzungsstart möglicherweise nicht aktualisiert. [LC9977]
- Wenn Sie versuchen, eine Citrix Richtlinie in Citrix Studio unter Verwendung des Organisationseinheitsfilters anzuwenden, wird möglicherweise die folgende Fehlermeldung angezeigt: **Ein unbekannter Fehler ist aufgetreten**.

  Die folgende Ausnahme wird gemeldet:
  Collection was modified; enumeration operation may not execute.[LD0044]
- Wenn Sie eine Gruppenrichtlinie sichern und anschließend mit der Gruppenrichtlinien-Verwaltungskonsole (Version 3.1.2) importieren, bleibt die Verwaltungskonsole möglicherweise hängen. Die Richtlinie wird jedoch importiert. [LD0173]

Citrix Studio

- Der Versuch eines delegierten Administrators mit einer benutzerdefinierten Rolle, die Benutzerzuweisung von einem Desktop mit Citrix Studio, PowerShell oder Citrix Director zu entfernen, kann fehlschlagen. Das Problem tritt auf, wenn benutzerdefinierte Administratoren Berechtigung zum Ausführen dieser Vorgänge für Bereitstellungsgruppen aber nicht für Maschinenkataloge haben. [LC8174]
- Wenn ein Delivery Controller offline geht oder anderweitig nicht mehr verfügbar ist, kann es einige Minuten dauern, bis in Citrix Studio die folgende Meldung angezeigt wird:

  This snap-in is not responding. [LC8993]
- Versuche, die Veröffentlichung von App-V-Paketen aufzuheben und die Pakete vom VDA zu entfernen, schlagen möglicherweise fehl. [LC9161]
- Wenn Sie versuchen, die Seite **Maschinenzuteilung** nach Auswahl von **Bereitstellungsgruppe bearbeiten** im Bereich **Aktionen** ein zweites Mal anzuzeigen, wird die Seite **Maschinenzuteilung** möglicherweise geleert und enthält keinerlei Details wie Maschinennamen oder Benutzer mehr. [LC9465]
- Der Versuch, den **Anwendungsordner** in Citrix Studio zu löschen, nachdem die veröffentlichte Anwendung aus der **Anwendungsgruppe** verschoben wurde, kann mit einem Berechtigungsfehler fehlschlagen. [LC9520]
- Nach einem Upgrade von Citrix Studio auf Version 7.15 CU 2 sind die Richtlinien möglicherweise nicht lokalisiert. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX234711.

[LC9613]

- Das Erstellen eines Maschinenkatalogs schlägt möglicherweise mit der Meldung fehl, dass die Zusammenfassung nicht erstellt werden kann. Bei Verwendung des Assistenten zum Erstellen von Katalogen ist außerdem vor Anzeige der Ausnahme die Dropdownliste der Domänen leer. [LC9636]
- Wenn Sie versuchen, App-V-Anwendungen aus der Bereitstellungsgruppe zu löschen, werden die Anwendungen möglicherweise gelöscht. Es wird eine Fehlermeldung angezeigt. [LC9985]
- Wenn Sie versuchen, eine Citrix Richtlinie in Citrix Studio unter Verwendung des Organisationseinheitsfilters anzuwenden, wird möglicherweise die folgende Fehlermeldung angezeigt: **Ein unbekannter Fehler ist aufgetreten**.

  Die folgende Ausnahme wird gemeldet:
  Collection was modified; enumeration operation may not execute. [LD0044]
- Wenn Sie versuchen, eine Citrix Richtlinie in Citrix Studio unter Verwendung der Organisationseinheit als Filter anzuwenden oder eine Organisationseinheit im Katalogassistenten hinzuzufügen, tritt eine Ausnahme auf. [LD0112]

Controller

- Der Versuch eines delegierten Administrators mit einer benutzerdefinierten Rolle, die Benutzerzuweisung von einem Desktop mit Citrix Studio, PowerShell oder Citrix Director zu entfernen, kann fehlschlagen. Das Problem tritt auf, wenn benutzerdefinierte Administratoren Berechtigung zum Ausführen dieser Vorgänge für Bereitstellungsgruppen aber nicht für Maschinenkataloge haben. [LC8174]
- Für VDAs kann in Citrix Studio ein ungültiger Energiezustand angezeigt werden. In Studio wird **AUS** angezeigt, obwohl der VDA ausgeführt wird. [LC8898]
- Wenn ein Delivery Controller offline geht oder anderweitig nicht mehr verfügbar ist, kann es einige Minuten dauern, bis in Citrix Studio die folgende Meldung angezeigt wird:

  This snap-in is not responding [LC8993].
- Sie importieren Änderungen vom Hauptbroker in die Datenbank des lokalen Hostcache und entfernen dann einen Benutzer oder eine Maschine aus Active Directory, jedoch nicht aus Citrix Studio. Dadurch können Fehler auftreten und der lokale Hostcache wird nicht aktualisiert. [LC9054]
- Deadlocks mit **Ereignis-ID 2013** können in XenApp während Verbindungsspitzen auftreten. Die folgende Fehlermeldung wird angezeigt:

  Eine unerwartete Ausnahme ist aufgetreten bei der Verarbeitung einer HTTP-Anforderung durch den Citrix Brokerdienst. [LC9134]

- Beim Upgrade von XenApp 7.6 auf XenApp 7.15 werden die Berechtigungen für den Lizenzierungsordner auf dem Delivery Controller unter **C:\Windows\ServiceProfiles\NetworkService\Licensing** überschrieben. [LC9445]
- Die Speicherauslastung durch den Citrix Hochverfügbarkeitsdienst (HighAvailabilityService.exe) kann 2 GB überschreiten. [LC9446]
- Wenn Sie von Citrix Studio einen Neustartbefehl an den Ziel-VDA senden, wird der Ziel-VDA möglicherweise heruntergefahren. [LC9479]
- Der Versuch, den **Anwendungsordner** in Citrix Studio zu löschen, nachdem die veröffentlichte Anwendung aus der **Anwendungsgruppe** verschoben wurde, kann mit einem Berechtigungsfehler fehlschlagen. [LC9520]
- Die auf den ESXi-Hosts gehostete virtuelle Desktopinfrastruktur (VDI) kann einen unbekannten Betriebszustand annehmen und wird nicht automatisch eingeschaltet. Das Problem tritt auf, wenn virtuelle Maschinen auf die ESXi-Hosts verschoben werden, nachdem diese aus dem Wartungsmodus geschaltet wurden. [LC9619]
- Das Erstellen eines Maschinenkatalogs schlägt möglicherweise mit der Meldung fehl, dass die Zusammenfassung nicht erstellt werden kann. Bei Verwendung des Assistenten zum Erstellen von Katalogen ist außerdem vor Anzeige der Ausnahme die Dropdownliste der Domänen leer. [LC9636]
- In Citrix Studio wird die Option **Starten** nicht angezeigt. Der Remote-PC lässt sich dann nicht einschalten. [LC9702]
- Der Einsatz dieser Leistungsverbesserung für den Überwachungsdienst reduziert die CPU-Last auf dem SQL-Server, wenn die Überwachungsdatenbank groß ist. [LC9726]
- Mit MCS bereitgestellte virtuelle Maschinen werden möglicherweise nicht mit aktiviertem **Secure Boot** erstellt. Das Problem kann auch dann auftreten, wenn die Mastervorlage mit EFI (Extensible Firmware Interface) und aktiviertem **Secore Boot** erstellt wurde. [LC9841]
- Die AWS-ID (Amazon Web Services) einer mit MCS bereitgestellten Maschine ist standardmäßig nicht persistent. Dies kann dazu führen, dass Energieverwaltungsaktionen der virtuellen Maschine für AWS fehlschlagen.

  Zum Konfigurieren der AWS-ID-Persistenz stehen folgende Optionen zur Verfügung:

  - Zum Konfigurieren der AWS-ID als persistent legen Sie für die Hostverbindung die erweiterte Eigenschaft "Verbindung"auf **CreateNewInstanceOnReset=False** fest.
  - Zum Konfigurieren der AWS-ID als nicht persistent legen Sie für die Hostverbindung die erweiterte Eigenschaft "Verbindung"auf **CreateNewInstanceOnReset=True** fest.

  Die Änderung tritt erst nach zehn Sekunden in Kraft. [LC9960]

- Wenn Sie versuchen, eine Anwendung mit dem Befehl **New-BrokerApplication** und dem Parameter "-AdminFolder"zu erstellen, wird der angegebene Ordner in bestimmten Szenarien nicht erstellt. [LC9982]
- Wenn Sie versuchen, App-V-Anwendungen aus der Bereitstellungsgruppe zu löschen, werden die Anwendungen möglicherweise gelöscht. Es wird eine Fehlermeldung angezeigt. [LC9985]
- Wenn Sie in einer großen Umgebung mit vielen Anwendungsgruppen auf die Registerkarte "Anwendungen"in Studio klicken, tritt beim Abrufen der **Get-BrokerApplicationGroup**-Ausgabe ein Timeout auf. Es wird dann folgende Ausnahme angezeigt:

  Database could not be connected.

  Vor Anzeige der Ausnahme bleibt Studio beim Auflisten der Anwendungsgruppen hängen. [LD0012]
- Wenn Sie versuchen, eine Citrix Richtlinie in Citrix Studio unter Verwendung des Organisationseinheitsfilters anzuwenden, wird möglicherweise die folgende Fehlermeldung angezeigt: **Ein unbekannter Fehler ist aufgetreten**.

  Die folgende Ausnahme wird gemeldet:
  Collection was modified; enumeration operation may not execute. [LD0044]
- Der Versuch, den lokalen Hostcache mit einem Bereitstellungsgruppenamen neu zu erstellen, der Sonderzeichen enthält, kann mit Ereignis-ID **505** fehlschlagen. [LD0068]
- Für die Citrix Studio-Hostingverbindung wird möglicherweise eine Warnmeldung zur Verwendung von HTTPS für XenServer-Hostingverbindungen ausgegeben, obwohl HTTPS-Verbindungen nicht unterstützt werden. [LD0210]
- Nach dem Upgrade von XenApp und XenDesktop auf Version 7.15 beginnt der Neustartzeitplan möglicherweise sofort anstatt beim nächsten geplanten Ereignis. [LD0308]

HDX RealTime Optimization Pack

Die Dokumentation zu HDX RealTime Optimization Pack 7.15 LTSR CU3 enthält Informationen zu den Updates in dieser Version.

Identity Assertion

- Der Zugriff auf das in der Sitzung verfügbare Authentifizierungszertifikat zur Anmeldung kann fehlschlagen. [LC9728]
- Bei Verwendung eines sitzungsinternen Zertifikat des Verbundauthentifizierungsdiensts für die Authentifizierung einer TLS 1.1-(oder früheren)-Verbindung kann die Verbindung fehlschlagen.

Es wird Ereignis-ID 305 protokolliert, die eine nicht unterstützte Hash-ID anzeigt. Der Verbundauthentifizierungsdienst unterstützt SHAMD5-Hash nicht. [LD0018]

Installer

- Die Installation des VDA in einer Umgebung, in der Adobe Acrobat Reader 2015 DC installiert ist, kann unter Anzeige folgender Fehlermeldung fehlschlagen:

  The Program can't start because mfc120u.dll is missing from your computer. Try reinstalling the program to fix the problem. [LC9979]

Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU3 Dokumentation enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

- Wenn Sie die Ordnerumleitung mit der Microsoft Active Directory-Richtlinie konfigurieren, indem Sie in Citrix Director auf **Profil zurücksetzen** klicken, werden die umgeleiteten Ordner ebenfalls zurückgesetzt. Daher werden bestimmte Ordner wie **Dokumente**, **Bilder**, **Musik**, **Videos** und **Favoriten umbenannt**. Ordner wie **Startmenü**, **Kontakte**, **Downloads**, **Verknüpfungen**, **Suchvorgänge** und **Gespeicherte Spiele** werden jedoch nicht umbenannt. [LC9237]
- Der Profilverwaltungsdienst wird möglicherweise unerwartet mit dem Ausnahmecode 0xc0000374 beendet. [LC9355]
- Die Profilverwaltung synchronisiert möglicherweise bestimmte Einstellungen auf einem VDA nicht, der unter Microsoft Windows 10, Version 1709 ausgeführt wird. [LC9503]
- Ist die Registrierungsrichtlinie **Aktiv zurückschreiben** aktiviert, funktioniert die Standardrichtlinie des Registrierungsausschlusses, einschließlich Software\Microsoft\AppV\Client\Integration und Software\Microsoft\AppV\Client\Publishing, möglicherweise nicht. [LC9550]
- Sie haben die volle Rechte für das Standardbenutzerprofil. Bei der ersten Anmeldung löscht die Profilverwaltung möglicherweise die ausgeschlossenen Ordner, die über eine Richtlinie aus dem Standardbenutzerprofil konfiguriert wurden. Das Problem tritt auf, wenn die Anmeldeausschlussprüfung zum Löschen der ausgeschlossenen Dateien und Ordner konfiguriert ist. [LC9575]

- Ist die Profilverwaltung mit Aktives Zurückschreiben der Registrierung konfiguriert, werden alle Registrierungseinträge verarbeitet und alle Änderungen in einer temporären Datei aufgezeichnet, unabhängig davon, ob die Registrierungseinträge ausgeschlossen oder eingeschlossen sind. Dies hat eine hohe CPU-Auslastung zur Folge. [LC9624]
- 7.15 LTSR CU2-Sitzungen werden möglicherweise als schwarzer Bildschirm gestartet. Das Problem tritt bei Sitzungen auf, die auf XenApp und XenDesktop 7.15 LTSR CU2 und 7.17 VDAs ausgeführt werden, wenn die Profilverwaltung aktiviert ist. Weitere Informationen und ein Workaround finden Sie im Knowledge Center-Artikel CTX235100. [LC9648]
- Die Richtlinie "Zu spiegelnde Ordner"in der Profilverwaltung funktioniert möglicherweise nicht. [LC9691]
- Wenn die Profilverwaltung aktiviert ist, werden möglicherweise leere Symbole im Startmenü der veröffentlichten Desktops angezeigt. Das Problem tritt während der zweiten oder einer nachfolgenden Anmeldung auf.

  Hinweis: Dieser Fix ist nur bei Neuinstallationen wirksam. Für Upgradeszenarios müssen Sie die Richtlinie **Zu spiegelnde Ordner** entweder im HDX-Gruppenrichtlinieneditor oder im Active Directory-Richtlinieneditor manuell konfigurieren. [LC9692]
- Die Ordnerumleitung von AppData (Roaming) funktioniert möglicherweise nicht in der Profilverwaltung und diese Fehlermeldung wird angezeigt:

  Zugriff verweigert.

  Das Problem tritt auf, wenn die Profilverwaltung **AppData/Roaming** nicht korrekt mit dem freigegebenen Ordner verknüpft und fälschlicherweise versucht, /Application Data/Roaming anzuhängen. [LC9830]

Provisioning Services

Provisioning Services 7.15 LTSR CU3 enthält Informationen zu den Updates in diesem Release.

Remote Broker Provider

- Die AWS-ID (Amazon Web Services) einer mit MCS bereitgestellten Maschine ist standardmäßig nicht persistent. Dies kann dazu führen, dass Energieverwaltungsaktionen der virtuellen Maschine für AWS fehlschlagen.

  Zum Konfigurieren der AWS-ID-Persistenz stehen folgende Optionen zur Verfügung:

  - Zum Konfigurieren der AWS-ID als persistent legen Sie für die Hostverbindung die erweiterte Eigenschaft "Verbindung"auf **CreateNewInstanceOnReset=False** fest.

- Zum Konfigurieren der AWS-ID als nicht persistent legen Sie für die Hostverbindung die erweiterte Eigenschaft "Verbindung"auf **CreateNewInstanceOnReset=True** fest.

Die Änderung tritt erst nach zehn Sekunden in Kraft. [LC9960]

Sitzungsaufzeichnung

Verwaltung

- Ein Benutzer aus **Domäne B** meldet sich bei dem Sitzungsaufzeichnungsserver in Domäne A an und versucht, die Eigenschaft "Sitzungsaufzeichnung"zu aktualisieren. Die Maschinen-GUID wird nicht erstellt und es tritt ein Fehler auf. Das Problem tritt auf, weil der Benutzer in **Domäne B** und Sitzungsaufzeichnungsserver in **Domäne A** ist. [LC9562]

Agent

- Die veröffentlichte Instanz von Microsoft Internet Explorer wird möglicherweise als **explorer.exe** in der Playerliste der Sitzungsaufzeichnung angezeigt. Der korrekte Dateiname lautet **Iexplore.exe**. [LC9622]

StoreFront

- Wenn Sie den Browser auf 125 % zoomen, verschwindet möglicherweise das benutzerdefinierte Logo. [LC9018]
- Wenn **OverrideIcaClientname** aktiviert ist, können Versuche fehlschlagen, eine Remotesitzung vom Remotedesktopclient herzustellen. Das Problem tritt auf, wenn die Lizenz nicht erneuert wird. Eine dieser Fehlermeldungen könnte erscheinen:

  "The remote session could not be established from remote desktop client WR_XxXXxXXX because its license could not be renewed."

  ODER

  "The remote session could not be established from remote desktop client WR_XxXXxXXX because its temporary license has expired."[LC9246]
- Die Auflistung von Anwendungen kann nach einem Update des Delivery Controller-Zertifikats auf TLS v1.2 fehlschlagen. [LC9337]
- Wenn Sie während der Einrichtung von XenDesktop eine konfigurierte Site auswählen, wird möglicherweise ein Standardstore in StoreFront erstellt, der den Standardauthentifizierungsdienst verwendet. Wenn Sie diesen Store entfernen, können Benutzer von Citrix Receiver für Windows keine anderen Stores hinzufügen und die folgende Fehlermeldung wird angezeigt:

"Ein Protokollfehler ist bei der Kommunikation mit dem Authentifizierungsdienst aufgetreten." [LC9404]

- Bei der Anmeldung bei StoreFront kann der Fehler **Ihre Anforderung kann nicht abgeschlossen werden** auftreten. Das Problem tritt auf, wenn die veröffentlichten Anwendungen benutzerdefinierte Symbole mit minimalen Auflösungen haben. [LC9521]
- Beim Anpassen bestimmter Funktionen mit dem StoreFront SDK und Konfigurieren der Aggregation des Stores kann bei der Anmeldung der Fehler **Ihre Anforderung kann nicht abgeschlossen werden** auftreten. [LC9561]
- Der Sitzungsvorabstart funktioniert nach der Konfiguration von **Ressourcen nach Schlüsselwörtern filtern** möglicherweise nicht mehr. [LC9642]
- Im UDPICAPort-Eintrag der ICA-Datei ist möglicherweise der FQDN des VDA angegeben, obwohl die NetScaler Gateway-Verbindung verwendet wird. [LC9760]

Universeller Druckserver

Client

- Der universelle Druckserver kann bewirken, dass der Druckspoolerdienst aufhört, zu reagieren. [LC9341]

Benutzerprofilverwaltung –VDA

- Nach dem Upgrade des VDA von Version 7.13 auf 7.15.2000 werden in Citrix Director die umgeleiteten Ordner möglicherweise nicht mehr angezeigt. Die Ordnerumleitung funktioniert weiterhin. [LC9968]
- Der Prozess brokeragent.exe kann die CPU stark auslasten. [LD0310]

VDA für Desktopbetriebssystem

HDX

- Der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) wird möglicherweise unerwartet beendet und das Video wird auf der HTML5-Seite nicht umgeleitet. [LC8825]
- Wenn eine veröffentlichte Anwendung, die auf einem VDA ausgeführt wird, einen generischen Pfad, z. B. %ProgramFiles% oder %ProgramFiles(x86)% verwendet, wird beim Wiederverbinden der Sitzung möglicherweise das Fenster für eine Anwendung doppelt angezeigt. [LC9741]

Drucken

- Eine Zugriffsverletzung in **CpSvc!CDispatcher::UpdateCounters** kann dazu führen, dass der Citrix Print Manager-Dienst (cpsvc.exe) unerwartet beendet wird. [LC8804]
- Für Anwendungen ohne .NET ist möglicherweise kein Standarddrucker festgelegt. Microsoft Windows Server 2016 kann den Wert des Registrierungsschlüssels **HKEY_CURRENT_USER\SOFTWARE\Micr**
  NT\CurrentVersion\Windows\Devicenicht aktualisieren, wenn der Standarddrucker der zugeordnete Citrix Drucker ist. [LC8984]
- Der Standarddrucker ist möglicherweise in einer Sitzung falsch eingestellt. Das Problem tritt auf, wenn der Standarddrucker zu einem anderen beliebigen Drucker wechselt. [LC8999]
- Beim Wiederherstellen einer Verbindung zu einer Sitzung werden die zugeordneten Drucker möglicherweise nur langsam geladen, wenn ältere Druckernamen verwendet werden. [LC9079]
- Wenn Sie in bestimmten Microsoft Excel-Dateien **Excel** > **Drucken** und dann einen automatisch erstellten Clientdrucker mit dem universellen Citrix EMF-Treiber auswählen, werden die Zeichen in der Druckvorschau möglicherweise kleiner angezeigt. [LC9700]
- Der Citrix Druckmanagerdienst (cpsvc.exe) wird möglicherweise unerwartet beendet. Das Problem tritt auf, wenn **CpWSGetPrinterConnectionsFromPolicy** einen Nullzeiger an die Vergleichszeichenfolge **[MS] _wcsicmp** übergibt. [LC9796]

Sitzung/Verbindung

- Innerhalb einer Benutzersitzung kann die Webcam aufhören zu reagieren. Das Problem tritt auf, wenn eine der folgenden Aktionen ausgeführt wird:
  - Bei Verwendung bestimmter Anwendungen von Drittanbietern zur Auswahl einer Webcam in einer Benutzersitzung reagieren die Videobilder der Webcam nicht mehr.
  - Bei Verwendung von GraphEdit zum Starten einer virtuellen Webcam und Auswahl von .Use Clock im Menü
  - Bei der Analyse der CDF-Ablaufverfolgung (Citrix Diagnostics Facility) sehen Sie, dass nur ein Videosample übergeben wird, wenn die Pipeline zwischen dem VDA und Citrix Receiver für Windows erstellt ist. [LC8382]
- Das Deaktivieren von Citrix Hooks wird möglicherweise nicht wirksam, wenn **ExcludedImageNames** im Registrierungsschlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook** mehrere ausführbare Dateien im hinzugefügt werden. [LC8614]
- Citrix Director meldet möglicherweise Multi-Stream-ICA als inaktiv, wenn das **UDP-based Data Transfer Protocol (UDT)** verwendet wird. Das Problem tritt auf, wenn der HDX-WMI-Anbieter nicht für EDT- oder UDT-Sitzungen aktualisiert wird. [LC8960]

- In Umgebungen mit mehreren Monitoren mit H-Konfiguration kann es zu fehlerhaften Mausbewegungen kommen. Sie beginnen eine Microsoft Skype for Business-Sitzung und teilen den Bildschirm mit dem anderen Benutzer. Der Citrix Grafiktreiber empfängt vom Betriebssystem eine falsche Mausposition.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

  Name: DisableAppendMouse

  Typ: DWORD

  Wert: 00000001

  Wenn Sie die HDX-Sitzung jedoch nach dem Festlegen des Registrierungsschlüssels verwenden, funktionieren bestimmte Features, die die Mauszeigerposition programmgesteuert festlegen, möglicherweise nicht einwandfrei. Es handelt sich um folgende Features:

  - Snap-to-Feature
  - Synchronisierung der Mausposition zwischen Benutzern mit GotoMeeting-Bildschirmfreigabe
  - Synchronisierung der Mausposition zwischen Benutzern mit Skype for Business-Bildschirmfreigabe [LC8976]

- In bestimmten Szenarien registrieren sich VDAs möglicherweise automatisch erneut (Ereignis-ID 1048). Wenn Sie beispielsweise zwei Anwendungen mit ähnlichen Namen (z. B. Lotus Notes und Lotus Notes Standard) starten und die zweite Anwendung schließen, wird der Eintrag der ersten Anwendung aus der Registrierung entfernt. Wenn diese Informationen per Benachrichtigung an den Delivery Controller gesendet werden, wird die Benachrichtigung abgelehnt, was zu einer erneuten Registrierung führt. [LC9223]
- Der HDX RealTime-Connector wird möglicherweise unerwartet beendet. Das Videovorschaufenster wird geschlossen oder es erscheint kurzzeitig ein schwarzes Kästchen und das Fenster wird dann geschlossen. Das Problem tritt auf, wenn HDX RealTime Media Engine auf dem Benutzergerät nicht installiert ist. [LC9282]
- Der Citrix Audiodienst wird möglicherweise unerwartet beendet und dann erneut gestartet. Wenn Sie vom zweiten Endpunkt (Thin Client) aus die Verbindung mit der Sitzung wiederherstellen, werden die neuen Geräte der Sitzung nicht ordnungsgemäß zugeordnet. [LC9381]
- Wenn Sie die Funktion zum Löschen bzw. Leeren der Zwischenablage in einer veröffentlichten Anwendung auswählen, die auf einem VDA ausgeführt wird, wird die Zwischenablage auf dem VDA geleert, jedoch nicht auf dem Endpunkt. [LC9434]
- Wenn Sie eine Benutzersitzung über einen Endpunkt trennen und dann über einen zweiten Endpunkt (Thin Client) wieder eine Verbindung mit derselben Sitzung herstellen, werden die clientseitigen Audiogeräte im VDA möglicherweise in einer falschen Reihenfolge aufgelistet.

Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

Name: CleanMappingWhenDisconnect

Typ: DWORD

Wert: 1 [LC9440]

- Die veröffentlichten Anwendungssitzungen werden möglicherweise getrennt, und Benutzersitzungen werden möglicherweise nicht ordnungsgemäß von den VDAs abgemeldet. Wenn das Problem auftritt, kann die Verbindung möglicherweise nicht wiederhergestellt und die Verbindung mit Citrix Studio nicht getrennt werden. Legen Sie zur Behebung die Sitzungen über den PowerShell-Befehl auf Ausgeblendet fest oder starten Sie den VDA neu. [LC9444]
- Bei Verwendung eines VDAs in Version 7.15.1000 kann es dazu kommen, dass eine ungewöhnliche Zahl von twi3.dll stammender CPU-Anweisungen durch den Prozess "Winlogon.exe" übergeben werden. [LC9450]
- Wenn die Richtlinie Clientlaufwerkumleitung deaktiviert ist und Sie eine Anwendung zum zweiten Mal vom Benutzergerät aus starten, kann der Anwendungsstart sehr lange dauern. [LC9477]
- Wenn Sie versuchen, eine Verbindung mit einer aktiven Sitzung von einem anderen Endpunkt aus herzustellen, wird folgende Fehlermeldung angezeigt:

  Verbindung unterbrochen; Citrix Receiver versucht eine Wiederverbindung noch 5 Minuten.

  Das Problem tritt unter Microsoft Windows 7 auf, wenn ein VDA der Version 7.15 installiert ist. [LC9485]
- Eine webbasierte Anwendung wird mit Microsoft Internet Explorer oder Mozilla Firefox Browser geöffnet. Wenn Sie bestimmte Registerkarten in der Anwendung öffnen, reagiert der gesamte Desktop möglicherweise nicht mehr. [LC9508]
- Der Leistungsindikator **Server Total**-Instanz fehlt möglicherweise in den **ICA-Sitzungsindikatoren**. [LC9537]
- Die Dateitypzuordnung funktioniert bei aktiviertem lokalen App-Zugriff möglicherweise nicht, wenn die Dateien auf einem Laufwerk mit verteiltem Dateisystem sind. [LC9538]
- Die Ereignis-ID 31 **Überwachen auf Verbindungen starten** wird möglicherweise nicht an die **Ereignisanzeige** übergeben. [LC9556]
- Wenn die **Unicode-Tastaturbelegung** aktiviert ist, können veröffentlichte Anwendungen nicht abgemeldet werden. [LC9590]

- Wenn Sie zwischen den Tastaturlayouts wechseln, wird möglicherweise ein Popup-Fenster angezeigt. Legen Sie den folgenden Registrierungsschlüssel fest, um das Popup-Fenster zu unterdrücken:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

  Name: HideNotificationWindow

  Typ: DWORD

  Wert: 1 [LC9592]

- Eine veröffentlichte Anwendung wird aufgrund eines unerwarteten Fehlers unter Umständen unmittelbar nach dem Start beendet. Das Problem tritt auf, wenn die Informationen zu aktiven Prozessen abgerufen werden. [LC9661]
- Nach einem Upgrade von XenApp und XenDesktop von Version 7.6 auf Version 7.15 LTSR CU 1 werden bestimmte Dienste während der Anmeldung möglicherweise unerwartet beendet oder reagieren nicht mehr. [LC9679]
- Die VDAs reagieren nach der Installation von XenApp und XenDesktop 7.15 LTSR CU 2 möglicherweise nicht mehr. [LC9701]
- Nach dem Deaktivieren bestimmter Verschlüsselungsverfahren über den Registrierungsschlüssel "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers" ist TLS möglicherweise nicht aktiviert. [LC9743]
- Wenn Sie über Remote-PC-Zugriff auf eine Windows-Arbeitsstation zugreifen und die Verbindung der Remote-PC-Zugriffssitzung dann trennen, wird die Arbeitsstation möglicherweise nicht gesperrt. Sie ist dann für jeden zugänglich, der physischen Zutritt zu ihr hat. [LC9812]
- Die **Kana**-Spracheingabetaste des japanischen Eingabemethoden-Editors (IME) wird bei der Anmeldung bei einem VDA möglicherweise automatisch aktiviert. [LC9932]
- Mit diesem Fix wird SCardHook der Positivlisten-Prozessmechanismus hinzugefügt. Wenn die Positivliste in der Registrierung definiert ist, können nur auf der Positivliste stehende Prozesse die Smartcardumleitung verwenden.

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  Name: HookProcessWhitelist

  Typ: REG_SZ

  Wert: <process name> [LC9961]

- Wenn Sie eine Benutzersitzung über einen Endpunkt trennen und dann über einen Thin Client wieder eine Verbindung mit derselben Sitzung herstellen, werden die clientseitigen Audiogeräte im VDA möglicherweise in einer falschen Reihenfolge aufgelistet.

Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio

Name: CleanMappingWhenDisconnect

Typ: DWORD

Wert: 1 [LD0458]

Systemausnahmen

- Auf Servern kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 (FILE_SYSTEM) kommen. [LC7726]
- Bei Servern mit aktiviertem EDT (Enlightened Data Transport) kann bei tdica.sys eine schwerwiegende Ausnahme mit Bluescreen und dem Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLI (7e)** auftreten. [LC8794]
- Auf Servern kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x000000D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL) kommen. [LC8830]
- Auf VDAs kann es bei wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [LC9695]
- Der Prozess wfshell.exe wird beim Starten einer veröffentlichten Anwendung möglicherweise unerwartet beendet. Das Problem tritt auf, wenn die Richtlinie "Bidirektionale Inhaltsumleitung"aktiviert ist und keine URLs bereitgestellt werden. [LC9705]
- Bei Microsoft Windows Server 2008 R2 kann eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)** auftreten. Das Problem tritt auf, wenn XenApp und XenDesktop 7.15 LTSR CU2 auf dem Computer mit Microsoft Windows Server installiert ist. [LC9849]
- Bei Servern kann bei picavc.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** auftreten. [LD0006]

Benutzererfahrung

- Wenn Sie die Größe einer veröffentlichten Anwendung ändern und versuchen, sie von einem Bildschirm auf einen anderen zu verschieben, wird möglicherweise ein weißer Rand um die Anwendung angezeigt. [LC9570]
- Sie konfigurieren einen VDA mit der **Unicode-Tastaturlayoutzuordnung** und richten eine HDX-Sitzung von Citrix Receiver mit aktiviertem lokalen IME ein. Wenn Sie ein beliebiges Zeichen eingeben und dann einige oder alle Ausgabezeichen in einer veröffentlichten Anwendung

auswählen, werden die neuen Zeichen vor den ausgewählten Zeichen eingefügt, anstatt sie zu ersetzen. [LC9591]

- Wenn Sie die Bildschirmauflösung ändern und die Verbindung zu der veröffentlichten Anwendung von einem Desktop-OS-VDA aus wiederherstellen, wird das Anwendungsfenster möglicherweise abgeschnitten angezeigt. [LC9947]
- In einer Umgebung mit mehreren Bildschirmen erfolgt die Bildschirmsperre in bestimmten Szenarien nicht wie erwartet. [LD0186]

Benutzeroberfläche

- Wenn ein Anwendungsfenster in einer Seamless-Sitzung nicht mehr reagiert, wird das Taskleistensymbol des Anwendungsfensters möglicherweise entfernt und erneut erstellt. [LC9807]

VDA für Serverbetriebssystem

HDX

- Der Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) wird möglicherweise unerwartet beendet und das Video wird auf der HTML5-Seite nicht umgeleitet. [LC8825]
- Wenn eine veröffentlichte Anwendung, die auf einem VDA ausgeführt wird, einen generischen Pfad, z. B. %ProgramFiles% oder %ProgramFiles(x86)% verwendet, wird beim Wiederverbinden der Sitzung möglicherweise das Fenster für eine Anwendung doppelt angezeigt. [LC9741]

Drucken

- Eine Zugriffsverletzung in **CpSvc!CDispatcher::UpdateCounters** kann dazu führen, dass der Citrix Print Manager-Dienst (cpsvc.exe) unerwartet beendet wird. [LC8804]
- Für Anwendungen ohne .NET ist möglicherweise kein Standarddrucker festgelegt. Microsoft Windows Server 2016 kann den Wert des Registrierungsschlüssels HKEY_CURRENT_USER\SOFTWARE\Micros NT\CurrentVersion\Windows\Devicenicht aktualisieren, wenn der Standarddrucker der zugeordnete Citrix Drucker ist. [LC8984]
- Der Standarddrucker ist möglicherweise in einer Sitzung falsch eingestellt. Das Problem tritt auf, wenn der Standarddrucker zu einem anderen beliebigen Drucker wechselt. [LC8999]
- Beim Wiederherstellen einer Verbindung zu einer Sitzung werden die zugeordneten Drucker möglicherweise nur langsam geladen, wenn ältere Druckernamen verwendet werden. [LC9079]

- Wenn Sie in bestimmten Microsoft Excel-Dateien "Excel > Drucken"und dann einen automatisch erstellten Clientdrucker mit dem universellen Citrix EMF-Treiber auswählen, werden die Zeichen in der Druckvorschau möglicherweise kleiner angezeigt. [LC9700]
- Der Citrix Druckmanagerdienst (cpsvc.exe) wird möglicherweise unerwartet beendet. Das Problem tritt auf, wenn **CpWSGetPrinterConnectionsFromPolicy** einen Nullzeiger an die Vergleichszeichenfolge **[MS] _wcsicmp** übergibt. [LC9796]

Sitzung/Verbindung

- Nach dem Upgrade des VDA von Version 7.12 auf Version 7.13 funktionieren die Badgeleser möglicherweise nicht mehr. [LC7667]
- Innerhalb einer Benutzersitzung kann die Webcam aufhören zu reagieren. Das Problem tritt auf, wenn eine der folgenden Aktionen ausgeführt wird:
  - Bei Verwendung bestimmter Anwendungen von Drittanbietern zur Auswahl einer Webcam in einer Benutzersitzung reagieren die Videobilder der Webcam nicht mehr.
  - Bei Verwendung von GraphEdit zum Starten einer virtuellen Webcam und Auswahl von .Use Clock im Menü
  - Bei der Analyse der CDF-Ablaufverfolgung (Citrix Diagnostics Facility) sehen Sie, dass nur ein Videosample übergeben wird, wenn die Pipeline zwischen dem VDA und Citrix Receiver für Windows erstellt ist. [LC8382]
- Das Deaktivieren von Citrix Hooks wird möglicherweise nicht wirksam, wenn **ExcludedImageNames** im Registrierungsschlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook** mehrere ausführbare Dateien im hinzugefügt werden. [LC8614]
- Auf Serverbetriebssystem-VDAs kann eine XenApp-Scheinsitzung erstellt werden, wenn die Verbindung einer Remotedesktopsitzung getrennt und wiederhergestellt wird. [LC8706]
- In Umgebungen mit mehreren Monitoren mit H-Konfiguration kann es zu fehlerhaften Mausbewegungen kommen. Sie beginnen eine Microsoft Skype for Business-Sitzung und teilen den Bildschirm mit dem anderen Benutzer. Der Citrix Grafiktreiber empfängt vom Betriebssystem eine falsche Mausposition.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

  Name: DisableAppendMouse

  Typ: DWORD

  Wert: 00000001

Wenn Sie die HDX-Sitzung jedoch nach dem Festlegen des Registrierungsschlüssels verwenden, funktionieren bestimmte Features, die die Mauszeigerposition programmgesteuert festlegen, möglicherweise nicht einwandfrei. Es handelt sich um folgende Features:

  - Snap-to-Feature
  - Synchronisierung der Mausposition zwischen Benutzern mit GotoMeeting-Bildschirmfreigabe
  - Synchronisierung der Mausposition zwischen Benutzern mit Skype for Business-Bildschirmfreigabe [LC8976]

- In bestimmten Szenarien registrieren sich VDAs möglicherweise automatisch erneut (Ereignis-ID 1048). Wenn Sie beispielsweise zwei Anwendungen mit ähnlichen Namen (z. B. Lotus Notes und Lotus Notes Standard) starten und die zweite Anwendung schließen, wird der Eintrag der ersten Anwendung aus der Registrierung entfernt. Wenn diese Informationen per Benachrichtigung an den Delivery Controller gesendet werden, wird die Benachrichtigung abgelehnt, was zu einer erneuten Registrierung führt. [LC9223]
- Der HDX RealTime-Connector wird möglicherweise unerwartet beendet. Das Videovorschaufenster wird geschlossen oder es erscheint kurzzeitig ein schwarzes Kästchen und das Fenster wird dann geschlossen. Das Problem tritt auf, wenn HDX RealTime Media Engine auf dem Benutzergerät nicht installiert ist. [LC9282]
- Sie starten Microsoft Excel 2007 auf einem veröffentlichten Desktop, öffnen eine makrofähige XSLM-Datei und ändern die Größe im Fenstermodus im Desktop Viewer. Die Sitzung reagiert dann möglicherweise nicht mehr. Das Problem tritt auf, wenn Sie die Tastenkombination **Alt+Eingabe** verwenden. [LC9379]
- Der Citrix Audiodienst wird möglicherweise unerwartet beendet und dann erneut gestartet. Wenn Sie vom zweiten Endpunkt (Thin Client) aus die Verbindung mit der Sitzung wiederherstellen, werden die neuen Geräte der Sitzung nicht ordnungsgemäß zugeordnet. [LC9381]
- Wenn Sie die Funktion zum Löschen bzw. Leeren der Zwischenablage in einer veröffentlichten Anwendung auswählen, die auf einem VDA ausgeführt wird, wird die Zwischenablage auf dem VDA geleert, jedoch nicht auf dem Endpunkt. [LC9434]
- Die veröffentlichten Anwendungssitzungen werden möglicherweise getrennt, und Benutzersitzungen werden möglicherweise nicht ordnungsgemäß von den VDAs abgemeldet. Wenn das Problem auftritt, kann die Verbindung möglicherweise nicht wiederhergestellt und die Verbindung mit Citrix Studio nicht getrennt werden. Legen Sie zur Behebung die Sitzungen über den PowerShell-Befehl auf Ausgeblendet fest oder starten Sie den VDA neu. [LC9444]
- Bei Verwendung eines VDAs in Version 7.15.1000 kann es dazu kommen, dass eine ungewöhnliche Zahl von twi3.dll stammender CPU-Anweisungen durch den Prozess "Winlogon.exe" übergeben werden. [LC9450]
- Wenn die Richtlinie Clientlaufwerkumleitung deaktiviert ist und Sie eine Anwendung zum

zweiten Mal vom Benutzergerät aus starten, kann der Anwendungsstart sehr lange dauern. [LC9477]

- Eine webbasierte Anwendung wird mit Microsoft Internet Explorer oder Mozilla Firefox Browser geöffnet. Wenn Sie bestimmte Registerkarten in der Anwendung öffnen, reagiert der gesamte Desktop möglicherweise nicht mehr. [LC9508]
- Der Leistungsindikator **Server Total**-Instanz fehlt möglicherweise in den **ICA-Sitzungsindikatoren**. [LC9537]
- Die Dateitypzuordnung funktioniert bei aktiviertem lokalen App-Zugriff möglicherweise nicht, wenn die Dateien auf einem Laufwerk mit verteiltem Dateisystem sind. [LC9538]
- Wenn die **Unicode-Tastaturbelegung** aktiviert ist, können veröffentlichte Anwendungen nicht abgemeldet werden. [LC9590]
- Wenn Sie zwischen den Tastaturlayouts wechseln, wird möglicherweise ein Popup-Fenster angezeigt. Legen Sie den folgenden Registrierungsschlüssel fest, um das Popup-Fenster zu unterdrücken:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\IcaIme

  Name: HideNotificationWindow

  Typ: DWORD

  Value: 1 [LC9592]
- Eine veröffentlichte Anwendung wird aufgrund eines unerwarteten Fehlers unter Umständen unmittelbar nach dem Start beendet. Das Problem tritt auf, wenn die Informationen zu aktiven Prozessen abgerufen werden. [LC9661]
- In Umgebungen mit mehreren Domänen oder Gesamtstrukturen können Sie die zweite Anwendung möglicherweise nicht starten, wenn die lokalen Gruppen für beschränkte Sichtbarkeit konfiguriert sind. [LC9665]
- Nach einem Upgrade von XenApp und XenDesktop von Version 7.6 auf Version 7.15 LTSR CU 1 werden bestimmte Dienste während der Anmeldung möglicherweise unerwartet beendet oder reagieren nicht mehr. [LC9679]
- Die VDAs reagieren nach der Installation von XenApp und XenDesktop 7.15 LTSR CU 2 möglicherweise nicht mehr. [LC9701]
- Nach dem Deaktivieren bestimmter Verschlüsselungsverfahren über den Registrierungsschlüssel "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers" ist TLS möglicherweise nicht aktiviert. [LC9743]
- Sie schließen ein USB-Speichergerät während der Sitzungsanmeldung an und leiten es im generischen Modus um. Das Laufwerk wird möglicherweise weiterhin angezeigt, wenn Sie das USB-Gerät abgezogen haben. [LC9783]

- Die **Kana**-Spracheingabetaste des japanischen Eingabemethoden-Editors (IME) wird bei der Anmeldung bei einem VDA möglicherweise automatisch aktiviert. [LC9932]
- Mit diesem Fix wird SCardHook der Positivlisten-Prozessmechanismus hinzugefügt. Wenn die Positivliste in der Registrierung definiert ist, können nur auf der Positivliste stehende Prozesse die Smartcardumleitung verwenden.

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

  Name: HideNotificationWindow

  Typ: REG_SZ

  Wert: <process name> [LC9961]
- Der wfshell.exe-Prozess kann unerwartet beendet werden. Die veröffentlichte Anwendung werden dann nicht gestartet. [LD0102]
- Nach dem Upgrade des VDA auf Version 7.15 CU 2 oder von Version 7.15 CU 1 auf CU 2 werden die im Registrierungsschlüssel "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix" konfigurierten Werte **AnonymousUserIdleTime** und **MaxAnonymousUsers** möglicherweise entfernt. [LD0378]

Smartcards

- Sie legen den Registrierungswert "DisableLogonUISuppression"unter dem Registrierungsschlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent"auf 0 fest. Wenn Sie eine veröffentlichte Anwendung starten, erfordert der VDA möglicherweise die Eingabe der Smartcard-Pin. Die Meldung **Bitte warten Sie auf den lokalen Sitzungsmanager** erscheint in Citrix Receiver für Windows und es tritt ein Timeout auf, da der Wert für **DisableLogonUISuppression** 0 die Aufforderung zur Eingabe einer PIN (LogonUI PIN) unterdrückt. Daher wird die PIN-Eingabeaufforderung nie angezeigt.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent

  Name: DisableLogonUISuppressionForSmartCardPublishedApps

  Typ: DWORD

  Wert: 1 [LC9059]

Systemausnahmen

- Auf Servern kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 (FILE_SYSTEM) kommen. [LC7726]

- Bei Servern mit aktiviertem EDT (Enlightened Data Transport) kann bei tdica.sys eine schwerwiegende Ausnahme mit Bluescreen und dem Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLE (7e)** auftreten. [LC8794]
- Auf Servern kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x000000D1 (DRIVER_IRQL_NOT_LESS_OR_EQUAL) kommen. [LC8830]
- Auf VDAs kann es bei wdica.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [LC9695]
- Der Prozess wfshell.exe wird beim Starten einer veröffentlichten Anwendung möglicherweise unerwartet beendet. Das Problem tritt auf, wenn die Richtlinie "Bidirektionale Inhaltsumleitung"aktiviert ist und keine URLs bereitgestellt werden. [LC9705]
- Der Prozess wfshell.exe wird möglicherweise unerwartet beendet, wenn Sie eine veröffentlichte Anwendung starten. Das Problem tritt aufgrund des fehlerhaften Moduls icaendpoint.dll auf. [LC9737]
- Bei Microsoft Windows Server 2008 R2 kann eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)** auftreten. Das Problem tritt auf, wenn XenApp und XenDesktop 7.15 LTSR CU2 auf dem Computer mit Microsoft Windows Server installiert ist. [LC9849]
- Bei Servern kann bei picavc.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)** auftreten. [LD0006]

Benutzererfahrung

- Wenn Sie versuchen, einen Hyperlink von bestimmten, auf einem Serverbetriebssystem-VDA ausgeführten Drittanbieteranwendungen (z. B. Aurion) zu öffnen, wird dem Anfang der URL möglicherweise die Zeichenfolge "%1"hinzugefügt. [LC8952]
- Wenn Sie die Größe einer veröffentlichten Anwendung ändern und versuchen, sie von einem Bildschirm auf einen anderen zu verschieben, wird möglicherweise ein weißer Rand um die Anwendung angezeigt. [LC9570]
- Sie konfigurieren einen VDA mit der **Unicode-Tastaturlayoutzuordnung** und richten eine HDX-Sitzung von Citrix Receiver mit aktiviertem lokalen IME ein. Wenn Sie ein beliebiges Zeichen eingeben und dann einige oder alle Ausgabezeichen in einer veröffentlichten Anwendung auswählen, werden die neuen Zeichen vor den ausgewählten Zeichen eingefügt, anstatt sie zu ersetzen. [LC9591]

Benutzeroberfläche

- Ein Rechtshinweis erscheint am Anfang des Anmeldebildschirms in einer Benutzersitzung. Wenn Sie bei aktiviertem lokalem App-Zugriff auf dem Anmeldebildschirm auf **OK** klicken, um fortzufahren, wird der Hinweis möglicherweise noch einige Sekunden lang angezeigt, bevor der Anmeldevorgang fortgesetzt wird. [LC9408]
- Wenn ein Anwendungsfenster in einer Seamless-Sitzung nicht mehr reagiert, wird das Taskleistensymbol des Anwendungsfensters möglicherweise entfernt und erneut erstellt. [LC9807]
- Wenn Sie eine veröffentlichte Anwendung starten, wird möglicherweise das Citrix Receiver für Windows-Fenster in der Ecke rechts unten angezeigt. [LC9817]

Virtual Desktop-Komponenten –Sonstiges

- Versuche, die Veröffentlichung von App-V-Paketen aufzuheben und die Pakete vom VDA zu entfernen, schlagen möglicherweise fehl. [LC9161]
- Der Cacheüberlauf in MCSIO (Machine Creation Services Storage Optimization) kann bei virtuellen XenServer-Maschinen zu einer schlechten Leistung führen. [LC9351]
- Auf dem VDA ausgeführte WMI-Abfragen reagieren möglicherweise auf unbestimmte Zeit nicht mehr. [LC9510]
- Die Ausführung mehrerer Instanzen derselben App-V-Anwendung in einer Sitzung kann fehlschlagen. Das Problem tritt auf, wenn der ausgeführte Prozess sich von dem in der Manifestdatei festgelegten Prozess unterscheidet. [LC9652]
- Wird der Microsoft Edge-Browser auf dem VDA ausgeführt, werden im **Aktivitätsmanager** von Citrix Director möglicherweise mehrere Anwendungseinträge angezeigt, während Sie den Benutzer suchen. [LC9673]

Cumulative Update 2 (CU2)

September 16, 2021

Releasedatum: 17. April 2018

Info zu diesem Release

Das kumulative Update 2 (CU2) für XenApp und XenDesktop 7.15 LTSR behebt mehr als 150 Probleme, die seit dem Release von 7.15 LTSR CU1 gemeldet wurden.

Downloads

Download von 7.15 LTSR CU2

Neue Bereitstellungen

Wie stelle ich das CU2 von Grund auf bereit?

Mit dem CU2-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf CU2 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU2 umfasst Updates für Basiskomponenten von 7.15 LTSR. Citrix empfiehlt die Aktualisierung aller LTSR-Komponenten Ihrer Bereitstellung auf CU2. Beispiel: Wenn Provisioning Services zur LTSR-Bereitstellung gehört, aktualisieren Sie die Provisioning Services-Komponenten auf die CU2-Version. Wenn Provisioning Services nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU2

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.2000	
VDA für Serverbetriebssystem	7.15.2000	

7.15 LTSR-Basiskomponente	Version	Hinweise
Delivery Controller	7.15.2000	
Citrix Studio	7.15.2000	
Citrix Director	7.15.2000	
Gruppenrichtlinienverwaltung	3.1.2000	
StoreFront	3.12.2000	
Provisioning Services	7.15.3	
Universeller Druckserver	7.15.2000	
Sitzungsaufzeichnung	7.15.2000	nur Platinum Edition
Linux VDA	7.15.2000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15.2000	
Verbundauthentifizierungsdienst	7.15.2000	

XenApp und XenDesktop 7.15 LTSR CU2-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR CU2 kompatible Komponenten und Plattformen	Version
App Layering	4.10.0
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2,4

Mit 7.15 LTSR CU2 kompatible Komponenten und Plattformen	Version
Lizenzserver	11.14.0.1 Build 23101
Self-Service-Kennwortzurücksetzung	1.1.10.0
Workspace Environment Management	4.6

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen; Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten)
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonyme Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren/aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp LTSR 7.15 CU2. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der Kernkomponenten von XenApp 7.15 LTSR CU2 und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU2-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen VDA (Virtual Delivery Agent) für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU2-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU2-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

May 9, 2022

Citrix Director

- Wenn Sie Maschinen nach DNS-Namen filtern, zeigt Citrix Director möglicherweise keine Maschinen oder aber doppelte Einträge der Maschinen an. Das Problem tritt auf, wenn die Maschine von zwei Delivery Controllern gleichzeitig zur Überwachungsdatenbank hinzugefügt wird. Dies führt dazu, dass zwei Maschineneinträge erstellt werden. [LC4905]
- Eine Ausnahme kann auftreten, wenn Sie als benutzerdefinierter Administrator nicht die Remote PC-Einstellung aus dem Maschinenkatalog abrufen können. Das Problem tritt auf, wenn Sie zwar berechtigt sind, den Maschinenkatalog zu verwalten, der Bereich jedoch nicht den betreffenden Katalog enthält. [LC8170]
- Wenn Sie zu **Filter** > **Sitzungen** in Citrix Director navigieren und versuchen, die Größe des Browsers zu ändern, wird möglicherweise die gesamte Tabelle falsch ausgerichtet. [LC8624]
- Die CSV-Datei wird unbrauchbar, wenn Sie Daten aus Citrix Director exportieren. Dieses Problem kann auftreten, wenn Sie eine nicht englische Windows-Version als Anzeigesprache von Director festlegen, da dann Kommas möglicherweise sowohl als Wert- als auch als Dezimaltrennzeichen verwendet werden. [LC8625]
- Beim Start von Citrix Director wird auf der Registerkarte **Infrastruktur** folgende Fehlermeldung angezeigt:

  Daten können nicht abgerufen werden. Verbindung mit dem Webserver verloren. Überprüfen Sie die Netzwerkverbindung und versuchen Sie es erneut. [LC8752]
- Wenn mehrere Sites konfiguriert sind, werden die Citrix Director-Sitenamen abgeschnitten. [LC9258]

Citrix Richtlinie

- Wenn Sie eine zweite Instanz des Gruppenrichtlinien-Editors (gpedit.msc) öffnen, wird der Knoten für Citrix Richtlinien nicht geöffnet und folgende Fehlermeldung kann angezeigt werden:

  Unhandled exception in managed code snap-in. [LC7600]
- Wenn Sie Citrix Richtlinien über die Gruppenrichtlinien-Verwaltungskonsole (GPMC) anwenden, werden die Richtlinien möglicherweise nicht in den GPMC-Richtlinieneinstellungen angezeigt.

Beim Bearbeiten des Gruppenrichtlinienobjekts (Group Policy Object, GPO) werden Richtlinien und Einstellungen jedoch als aktiviert angezeigt. [LC8282]

- Beim Hinzufügen der Einstellung **Druckerzuordnungen** zu einer **Benutzerrichtlinie** in Active Directory mit Citrix Gruppenrichtlinienverwaltung 3.1 kann es zu einem Problem mit der Anpassung der Fenstergröße kommen. Das Fenster verbreitert sich nach dem Öffnen möglicherweise bis zur Ecke des Bildschirms. Die Bearbeitung der Richtlinie ist dann schwierig, da Sie nicht alle Spalten erreichen. [LC8684]
- Wenn Dateien im Cacheordner für lokale Richtlinien (%ProgramData%/CitrixCseCache) auf "Schreibgeschützt"gesetzt sind, werden die Richtlinieneinstellungen möglicherweise nicht erfolgreich angewendet. [LC8750]
- Der Versuch, App-V-Anwendungen im Einzelverwaltungsmodus von VDAs zu starten, kann fehlschlagen. Das Problem tritt auf, wenn kein Wert für den Registrierungsschlüssel **ApplicationStartDetails** eingegeben wurde oder wenn die Anwendungsdetails für den Registrierungsschlüssel fehlen. [LC8798]
- Das Hinzufügen von Maschinen zu einer Bereitstellungsgruppe mit dem NETBIOS-Namen für die Benutzerzuordnung kann fehlschlagen. Stattdessen wird u. U. der Domänenname angezeigt. Das Problem tritt auf, wenn vom NETBIOS-Namen die falsche URL verwendet wird. [LC9393]

Citrix Studio

- Wenn Sie versuchen, eine Anwendung aus dem Linux-VDA manuell hinzuzufügen, kann die folgende Fehlermeldung erscheinen:

  "Value cannot be null while publishing the application."

  Die Anwendung wird jedoch erfolgreich hinzugefügt, wenn Sie in der angezeigten Fehlermeldung auf "OK"klicken. [LC7910]
- Anwendungen können möglicherweise nicht aus einer Bereitstellungsgruppe entfernt werden, wenn sie sich im Unterordner des Knotens **Anwendungen** in Citrix Studio befinden. [LC8705]
- Das Hinzufügen von Maschinen zu einer Bereitstellungsgruppe mit dem NETBIOS-Namen für die Benutzerzuordnung kann fehlschlagen. Stattdessen wird u. U. der Domänenname angezeigt. Das Problem tritt auf, wenn vom NETBIOS-Namen die falsche URL verwendet wird. [LC9393]

Controller

- Am Ende von Anzeigenamen und Beschreibungen bestimmter Citrix Dienste können unter japanischen Betriebssystemen überflüssige Zeichen angezeigt werden. [LC5208]

- Wenn Sie versuchen, Daten für Sitzungen von Citrix Director abzurufen, werden in der Überwachungsdatenbank keine Einträge angezeigt. Bestimmte Daten werden daher nicht in Citrix Director angezeigt und die folgende Fehlermeldung erscheint:

  "Daten konnten nicht abgerufen werden."[LC6273]

- Wenn Sie versuchen, eine Anwendung aus dem Linux-VDA manuell hinzuzufügen, kann die folgende Fehlermeldung erscheinen:

  "Value cannot be null while publishing the application."

  Die Anwendung wird jedoch erfolgreich hinzugefügt, wenn Sie in der angezeigten Fehlermeldung auf "OK"klicken. [LC7910]

- Nach dem Upgrade von Delivery Controller auf Version 7.15 LTSR wird der alte Basisdatenträger, der nach einer Aktualisierung des Maschinenkatalogs erstellt wurde, nicht aus dem Image des Hypervisors entfernt. [LC8637]

- Der Citrix Brokerdienst (Brokerservice.exe) wird möglicherweise unerwartet beendet. Das Problem tritt aufgrund des fehlerhaften Moduls LicPolEng.dll auf. [LC8638]

- Wenn Sie virtuellen Maschinen (VMs) das erforderliche Minimum an VMware-Privilegien über Maschinenerstellungsdienste (MCS) bereitstellen, können die VMs unter Umständen nicht gelöscht werden. Dieser Fehler kann selbst bei der Mindestmenge an erteilten Berechtigungen für VMware auftreten. [LC8868]

- Wenn Sie versuchen, einen Maschinenkatalog zu erstellen, der Premiumspeicher verwendet, ist die Option zum Auswählen der virtuellen Maschinengröße der E-oder L-Serie möglicherweise nicht verfügbar. [LC9052]

- Wenn Sie einen Active Directory-Benutzer löschen, der mit Zonenpräferenz zugewiesen wurde, kann die Brokerkonfiguration unter Umständen nicht in den sekundären Broker importiert werden. Der Importvorgang kann auch fehlschlagen, nachdem XenDesktop auf die neueste Version aktualisiert wurde. [LC9269]

- Das Hinzufügen von Maschinen zu einer Bereitstellungsgruppe mit dem NETBIOS-Namen für die Benutzerzuordnung kann fehlschlagen. Stattdessen wird u. U. der Domänenname angezeigt. Das Problem tritt auf, wenn vom NETBIOS-Namen die falsche URL verwendet wird. [LC9393]

HDX MediaStream Flash-Umleitung

- Wenn Sie bei aktivierter HDX MediaStream Flash-Umleitung eine VDA-Sitzung erneut mit Qumu.com verbinden, wird der Flash-Inhalt möglicherweise nicht in Microsoft Internet Explorer geladen. [LC9193]

Installer

- Versuche, den Installationsverzeichnispfad auf dem Delivery Controller zu ändern, funktionieren möglicherweise nicht für **XaXdProxy.msi**. [LC8691]

Linux VDA

Die Dokumentation zu Linux Virtual Delivery Agent 7.15 LTSR CU2 enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

- Nach dem Neustart des Profilverwaltungsdiensts zeigt Citrix Director möglicherweise nicht die Anmelde- und Personalisierungsinformationen des Benutzers an. [LC6942]

Provisioning Services

Die Dokumentation zu Provisioning Services 7.15 LTSR CU2 enthält Informationen zu den Updates in diesem Release.

StoreFront

- Wenn die Einstellung "Desktop automatisch starten"aktiviert ist, funktioniert das Verhindern mehrfacher Anmeldungen möglicherweise nicht. Infolgedessen schlagen nachfolgende Anforderungen zum Starten derselben Desktopinstanz fehl. [LC7430]
- Nach dem Upgrade von StoreFront 2.6, das auf einem nicht standardmäßigen Laufwerk installiert ist, werden die Anwendungsabonnementdaten der Benutzer möglicherweise nicht beibehalten. [LC8046]
- Nach dem Neustart der StoreFront MMC-Konsole wird der Wert des Kontrollkästchens **Desktop Viewer anzeigen** möglicherweise nicht korrekt angezeigt. [LC8520]
- Wenn Sie den Befehl **Set-STFWebReceiverSiteStyle** an einer PNG-Datei ausführen (Transparenz wird unterstützt), um StoreFront anzupassen, wird die PNG-Datei in eine JPEG-Datei konvertiert. Im JPEG-Dateiformat geht möglicherweise die Unterstützung für Transparenz verloren. [LC8677]
- Wenn Sie den Befehl **Set-STFWebReceiverApplicationShortcuts** ausführen, um die vertrauenswürdigen URLs für Anwendungsverknüpfungen in Citrix Receiver für Web-Sites festzulegen, wird am Ende der URL möglicherweise ein Schrägstrich ("/") hinzugefügt. [LC8761]

- Wenn Sie den Befehl **Set-STFWebReceiverSiteStyle** verwenden, um StoreFront anzupassen, kann die Datei style.css fälschlicherweise im Custom-Ordner geändert werden. Die StoreFront-Konsole kann die Anpassung dann nicht lesen. [LC8776]
- Auf den StoreFront-Servern kann ein Authentifizierungsfehler auftreten. Das Problem tritt auf, wenn die dynamischen TCP-Ports aufgebraucht sind. [LC8795]
- Versuche, das StoreFront-Logo mit dem Befehl **Set-STFWebReceiverSiteStyle** zu ändern, schlagen möglicherweise fehl. [LC8994]
- StoreFront kann möglicherweise nicht aktualisiert werden, wenn im Verzeichnis "Custom"einer beliebigen Instanz von Citrix Receiver für Websites schreibgeschützte Dateien vorhanden sind. [LC9252]

VDA für Desktopbetriebssystem

HDX 3D Pro

- Wenn HDX 3D Pro und eine benutzerdefinierte Auflösung auf einem VDA unter Microsoft Windows 10 aktiviert ist, kann es vorkommen, dass bei der Anmeldung ein grauer Bildschirm angezeigt wird. [LC8417]

HDX MediaStream Flash-Umleitung

- Wenn Sie bei aktivierter HDX MediaStream Flash-Umleitung eine VDA-Sitzung erneut mit Qumu.com verbinden, wird der Flash-Inhalt möglicherweise nicht in Microsoft Internet Explorer geladen. [LC9193]

HDX MediaStream Windows Media-Umleitung

- Wenn die HDX MediaStream Windows Media-Umleitung deaktiviert ist, kann es bei bestimmten Videodateiformaten dazu kommen, dass das Video in Windows Media Player vertikal gespiegelt angezeigt wird. [LC9194]

HDX RealTime

- RealTime Connector ist installiert. Wenn Sie Anwendungen mit umgeleiteter Webcam verwenden (z. B. Skype for Business), wird die Webcam, die auf einem VDA für Desktopbetriebssysteme installiert ist, beim ersten Sitzungsstart möglicherweise umgeleitet und erkannt. Wenn Sie die Verbindung zur Benutzersitzung wiederherstellen, wird die Webcam jedoch nicht mehr erkannt.

Das Problem tritt auf, wenn RealTime Media Engine nicht auf dem Benutzergerät installiert ist. [LC8793]

Tastatur

- Wenn Sie eine Anwendung auf einem Android-Gerät starten und sich im Textfeld befinden, wird die Tastatur möglicherweise nicht automatisch angezeigt. Außerdem müssen Sie zum Öffnen oder Schließen immer die Tastaturtaste berühren. [LC8936]

Drucken

- Der beidseitige Druck unter Verwendung der Druckeinstellungen in Microsoft Word kann fehlschlagen. [LC7501]
- Das Drucken eines Dokuments aus einer veröffentlichten Instanz von Microsoft Internet Explorer kann fehlschlagen. [LC8093]
- Wenn Französisch als Anzeigesprache auf einem VDA installiert ist, kann der Versuch, ein Dokument zu drucken, fehlschlagen. [LC8209]
- Ein von einem Benutzergerät umgeleiteter Drucker wird nach Wiederverbindung der Sitzung möglicherweise nicht mehr umgeleitet. [LC8762]
- Der Neustart des Citrix Druckmanagerdiensts (cpsvc.exe) kann fehlschlagen, wenn Sie den Druckspoolerdienst beim Starten der ersten Sitzung anhalten. [LC9192]

Sitzung/Verbindung

- Beim Lesen einer Datei auf einem zugeordneten Clientlaufwerk wird möglicherweise die Länge der zwischengespeicherten Datei zurückgegeben, wenn die Dateilänge außerhalb der Sitzung geändert wurde. Darüber hinaus werden für gelöschte Zeichen Null-Zeichen eingefügt.

  Zum Aktivieren dieses Fixes legen Sie den folgenden Registrierungsschlüssel auf 0 fest:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters;
  Name: CacheTimeout;
  Typ: REG_DWORD;
  Wert: Der Standardwert ist 60 Sekunden. Wenn CacheTimeOut auf 0 festgelegt ist, findet das Neuladen der Dateilänge sofort statt, andernfalls nach dem vorgegebenen Timeout. [LC6314]
- Eine Sitzung, die auf einem VDA für Desktopbetriebssysteme ausgeführt wird, reagiert im Legacygrafikmodus möglicherweise nicht mehr. Wenn das Problem auftritt, können Sie unter Umständen nichts im Desktop Viewer aktualisieren, obwohl der Desktop Viewer weiterhin reagiert. Die Sitzung wird zudem nach 30 bis 60 Minuten wiederhergestellt. [LC7777]

- Wenn Sie eine Anwendung bei aktiviertem Sitzungsfortbestehen starten, wird die Sitzung möglicherweise abgemeldet, sobald die Anwendung angezeigt wird. [LC8245]
- Wenn Sie einen VDA für Desktopbetriebssysteme starten, verschwindet der gestartete Desktop möglicherweise nach einigen Sekunden. [LC8373]
- Windows Explorer kann in folgenden Fällen unerwartet geschlossen werden:
  - Wenn eine große Anzahl von Dateien ausgewählt wird, deren Namen mehr als 260 Zeichen enthält, und die Option "Senden an > Faxempfänger"ausgewählt wird
  - Wenn versucht wird, Anwendungen von Drittherstellern zu öffnen.
  - Wenn versucht wird, Dateien mit Nitro PDF zu kombinieren [LC8423]
- Änderungen an erweiterten Systemeinstellungen unter "Visuelle Effekte"werden zwar auf die aktuelle Desktopbetriebssystem-VDA-Sitzung angewendet, möglicherweise aber nicht für zukünftige Sitzungen gespeichert. Damit solche Änderungen beibehalten werden, müssen Sie folgenden Registrierungsschlüssel festlegen:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Typ: DWORD;
  Wert: 1 [LC8049, LC8658]
- Nachdem Sie eine Sitzung getrennt haben, wird Monitor1 bei der nächsten lokalen Anmeldung möglicherweise fälschlich als primärer Monitor angezeigt. Dies kann passieren, wenn Sie sich in einer Umgebung mit mehreren Monitoren lokal an einem VDA mit Remote-PC-Zugriff anmelden und Monitor2 als primären Monitor konfigurieren, eine Verbindung über ein Benutzergerät herstellen und eine Sitzung dann über den Desktop Viewer trennen. [LC8675]

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel für Desktop-OS fest:

  Pfad: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

  Name: UseDCForLocalModes

  Typ: REG_DWORD

  Wert: 1
- Beim Versuch, eine veröffentlichte Anwendung zu starten, die unter Microsoft Windows Server 2012 oder 2016 ausgeführt wird, wird Ihr Zugriff möglicherweise gesperrt. [LC8681]
- Wenn Sie eine Anwendung in einer Umgebung mit mehreren Monitoren starten, wird möglicherweise ein Anmeldebanner angezeigt, das beide Monitore umfasst. Bei Verwendung eines einzelnen Monitors wird das Anmeldebannerfenster im Vollbildmodus angezeigt. [LC8741]

- Wenn der lokale App-Zugriff aktiviert ist und Sie Anwendungen auf den veröffentlichten Desktops öffnen, die unter Microsoft Windows 10 ausgeführt werden, können die Anwendungen nicht minimiert werden. [LC8813]
- Die DLP-Software kann möglicherweise keine Dateien mit UNC-Verknüpfung scannen. [LC8893]
- Nach dem Start einer veröffentlichten Anwendung funktioniert die Num-Taste nicht. Das Problem tritt auf, wenn die LED der Num-Taste auf dem Benutzergerät sichtbar ist, Ziffern jedoch nicht in einer Benutzersitzung funktionieren. Das Problem tritt in bestimmten Szenarien auf, wenn das vom Client angeforderte LED-Update eintrifft, bevor der neu erstellte Remotedesktop seinen LED-Status initialisiert hat. In diesem Fall aktualisiert die WinsStation ihren LED-Status möglicherweise nicht, wodurch der LED-Status von Endpunkt und VDA nicht mehr synchron ist. [LC8921]
- Der Versuch, Anwendungen und Desktops zu starten, kann fehlschlagen. Das Problem tritt auf, wenn der VDA für Serverbetriebssysteme nicht mehr reagiert.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard;
  Name: EnableSCardHookVcResponseTimeout;
  Typ: DWORD;
  Wert: 1 [LC8969]
- Das Öffnen von VM-gehosteten Anwendungen kann fehlschlagen. [LC9001]
- Das Wiederherstellen der Verbindung zu einer Sitzung kann fehlschlagen. [LC9040]
- Der Befehl **WFQuerySessionInformation** des WFAPI SDKs zum Abrufen der VDA-Version in einer Sitzung funktioniert möglicherweise nicht. [LC9041]
- Nach dem Upgrade von XenApp und XenDesktop von Version 7.14 auf 7.15 kann es beim Wechsel zwischen den Registerkarten einer veröffentlichten Anwendung dazu kommen, dass die Anwendung nicht mehr reagiert. Wenn Sie zudem das Seamlessfenster verkleinern und anschließend wieder erweitern, dauert es einige Zeit, bis alle Elemente im Fenster wieder angezeigt werden. [LC9078]
- Eine veröffentlichte Anwendung wird unter Umständen unmittelbar nach dem Start beendet. [LC9167]
- Wenn Sie in einer Millennium-Suite die Verbindung zu einer Seamlessanwendung wiederherstellen und dabei eine andere Bildschirmauflösung als bei der ersten Verbindung verwenden, wird die Größe der Anwendung möglicherweise falsch angepasst. Das Fenster wird dann unter Umständen abgeschnitten angezeigt. [LC9214]
- Wenn Sie über ein Benutzergerät eine Verbindung zu einem veröffentlichten Desktop mit Windows 10 Version 1709 herstellen, kann dies zu einem abgeblendeten Bildschirm führen. Wenn

Sie über die Konsole des Hypervisors eine Verbindung zu einem veröffentlichten Desktop herstellen, wird ein schwarzer Bildschirm mit drehendem Rad angezeigt. Über ein RDP funktioniert das Verbinden mit einem veröffentlichten Desktop jedoch fehlerfrei. [LC9215]

- Das Starten von Anwendungen aus Citrix Receiver für Mac schlägt möglicherweise fehl. Das Problem tritt auf, wenn die Clientlizenz (LicenseRequestClientLicense) nicht abgerufen werden kann. [LC9286]
- Wenn HDX 3D Pro aktiviert ist, kann der Start eines XenDesktops gelegentlich fehlschlagen. Das Problem tritt auf, wenn ein GPU-Fehler vorliegt. [LC9343]
- Beim Wechsel von einer Benutzersitzung auf eine nicht verwaltete Remotedesktopsitzung wird die Sitzung beim SmoothRoaming unter Umständen nicht fehlerfrei angezeigt. [LC9471]

Smartcards

- Bei Verwendung einer Smartcard können Anwendungen von Drittanbietern hängenbleiben, anstatt die PIN-Eingabeaufforderung anzuzeigen. [LC8805]

Systemausnahmen

- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei picadm.sys mit einem Bluescreen und mit Bugcheckcode 0x22 kommen. [LC6177]
- Auf Servern kann es in picadm.sys zu einer schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA) kommen. [LC6985]
- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei picadm.sys mit einem Bluescreen und mit Bugcheckcode 0x22 kommen. [LC7574]
- Auf Servern kann es in vdtw30.dll zu einer schwerwiegenden Ausnahme mit Bluescreen und Stoppcode SYSTEM_SERVICE_EXCEPTION (3b) kommen. [LC8087]
- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei pdcrypt2.sys mit einem Bluescreen und mit Bugcheckcode 0x3B kommen. Das Problem tritt auf, wenn ein VDA gestartet wird. [LC8328]
- Wenn HDX 3D Pro und GPU-Hardwarecodierung aktiviert sind und NVIDIA-GPUs verwendet werden, wird der Citrix Softwaregrafikprozess (Ctxgfx.exe) möglicherweise unerwartet beendet. Das Problem tritt bei Verwendung hochauflösender Bildschirme auf. LC8435]
- Auf VDAs für Serverbetriebssysteme kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [LC8708]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 kommen. [LC8749]

- Wenn Sie sich nach dem Neustart des VDA zum ersten Mal anmelden, kann eine unerwartete Zugriffsverletzung auftreten. Der Citrix Softwaregrafikprozess (Ctxgfx.exe) wird unerwartet beendet. Dadurch kann die Qualität von Text und Bildern auf dem VDA beeinträchtigt werden. [LC9005]
- Windows Explorer kann in folgenden Fällen unerwartet geschlossen werden:
  - Wenn eine große Anzahl von Dateien ausgewählt wird, deren Namen mehr als 260 Zeichen enthält, und die Option **Senden an** > **Faxempfänger** ausgewählt wird.
  - Wenn versucht wird, Anwendungen von Drittherstellern zu öffnen.
  - Wenn versucht wird, Dateien mit Nitro PDF zu kombinieren [LC9076]

Benutzererfahrung

- Wenn Sie Inhalt aus einer auf einem Client ausgeführten Anwendung kopieren und in eine Anwendung einer Benutzersitzung einfügen, wird der Inhalt möglicherweise nicht eingefügt. Außerdem kann die Schaltfläche **Einfügen** deaktiviert sein. [LC8516]
- Beim Versuch, sich an einer zuvor gesperrten Sitzung anzumelden, wird möglicherweise keine erneute Anmeldeaufforderung angezeigt. [LC8774]

Benutzeroberfläche

- Der Desktophintergrund wird angezeigt, obwohl die Richtlinie "Desktophintergrund"auf "Nicht zugelassen"gesetzt wurde. [LC8398]

Sonstiges

- Dieser Fix bietet kleinere Leistungs- und Qualitätsverbesserungen für Enlightened Data Transport (EDT). [LC9278]

VDA für Serverbetriebssystem

HDX MediaStream Windows Media-Umleitung

- Wenn die HDX MediaStream Windows Media-Umleitung deaktiviert ist, kann es bei bestimmten Videodateiformaten dazu kommen, dass das Video in Windows Media Player vertikal gespiegelt angezeigt wird. [LC9194]

HDX RealTime

- RealTime Connector ist installiert. Wenn Sie Anwendungen mit umgeleiteter Webcam verwenden (z. B. Skype for Business), wird die Webcam, die auf einem VDA für Desktopbetriebssysteme installiert ist, beim ersten Sitzungsstart möglicherweise umgeleitet und erkannt. Wenn Sie die Verbindung zur Benutzersitzung wiederherstellen, wird die Webcam jedoch nicht mehr erkannt. Das Problem tritt auf, wenn RealTime Media Engine nicht auf dem Benutzergerät installiert ist. [LC8793]

Tastatur

- Wenn Sie eine Anwendung auf einem Android-Gerät starten und sich im Textfeld befinden, wird die Tastatur möglicherweise nicht automatisch angezeigt. Außerdem müssen Sie zum Öffnen oder Schließen immer die Tastaturtaste berühren. [LC8936]

Drucken

- Der beidseitige Druck unter Verwendung der Druckeinstellungen in Microsoft Word kann fehlschlagen. [LC7501]
- Das Drucken eines Dokuments aus einer veröffentlichten Instanz von Microsoft Internet Explorer kann fehlschlagen. [LC8093]
- Wenn Französisch als Anzeigesprache auf einem VDA installiert ist, kann der Versuch, ein Dokument zu drucken, fehlschlagen. [LC8209]
- Der Neustart des Citrix Druckmanagerdiensts (cpsvc.exe) kann fehlschlagen, wenn Sie den Druckspoolerdienst beim Starten der ersten Sitzung anhalten. [LC9192]

Server- /Siteverwaltung

- Der Citrix Stack Control-Dienst (SCService64.exe) wird möglicherweise unerwartet beendet, wenn der VDA die Gruppenmitgliedschaft des Benutzers überprüft und zwei oder mehr Gruppen mit dem gleichen Namen in mehreren Domänen vorliegen. Das Problem tritt auf, wenn die Zeichenfolge "DnsDomainName"in der DS_DOMAIN_TRUSTSW-Struktur leer ist. [LC8484]

Sitzung/Verbindung

- Die folgende Warnmeldung wird u. U. beim Start von XenApp 7.6 Long Term Service Release Cumulative Update 2 für VDA für Serverbetriebssysteme oder bei Vorversionen im Systemereignisprotokoll angezeigt:

"An attempt to connect to the SemsService has failed with error code 0x2."[LC6311]

- Beim Lesen einer Datei auf einem zugeordneten Clientlaufwerk wird möglicherweise die Länge der zwischengespeicherten Datei zurückgegeben, wenn die Dateilänge außerhalb der Sitzung geändert wurde. Darüber hinaus werden für gelöschte Zeichen Null-Zeichen eingefügt.

  Zum Aktivieren dieses Fixes legen Sie den folgenden Registrierungsschlüssel auf 0 fest:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters;
  Name: CacheTimeout;
  Typ: REG_DWORD;
  Wert: Der Standardwert ist 60 Sekunden. Wenn CacheTimeOut auf 0 festgelegt ist, findet das Neuladen der Dateilänge sofort statt, andernfalls nach dem vorgegebenen Timeout. [LC6314]

- Nach dem Abdocken eines Laptops kann die Sitzungsfreigabe fehlschlagen. Das Problem tritt auf, wenn sich der VDA beim Delivery Controller neu registriert und während der automatischen Clientwiederverbindung eine "Außer Betrieb"-Benachrichtigung ausgelöst wird. [LC7450]

- Eine Sitzung, die auf einem VDA für Desktopbetriebssysteme ausgeführt wird, reagiert im Legacygrafikmodus möglicherweise nicht mehr. Wenn das Problem auftritt, können Sie unter Umständen nichts im Desktop Viewer aktualisieren, obwohl der Desktop Viewer weiterhin reagiert. Die Sitzung wird zudem nach 30 bis 60 Minuten wiederhergestellt. [LC7777]

- Auf iOS-Geräten, auf denen die Konfigurationseinstellungen "EnablePublishingRefreshUI"und "Session Lingering"in der Sitzung aktiviert sind, bleibt ein schwarzes Fenster geöffnet, nachdem eine veröffentlichte Anwendung mit einem auf dem VDA installierten App-V-Client geschlossen wird. Das Problem tritt auf, wenn das Sitzungsfortbestehen (Session Lingering) für die Sitzung aktiviert ist. [LC8080]

- Wenn Sie eine Anwendung bei aktiviertem Sitzungsfortbestehen starten, wird die Sitzung möglicherweise abgemeldet, sobald die Anwendung angezeigt wird. [LC8245]

- Server reagieren möglicherweise nicht mehr auf RPM.dll und die folgende Fehlermeldung wird angezeigt:

  Event ID 1009, picadm: Timeout waiting for response message from client [LC8339]

- Windows Explorer kann in folgenden Fällen unerwartet geschlossen werden:

  - Wenn eine große Anzahl von Dateien ausgewählt wird, deren Namen mehr als 260 Zeichen enthält, und die Option "Senden an > Faxempfänger"ausgewählt wird
  - Wenn versucht wird, Anwendungen von Drittherstellern zu öffnen.
  - Wenn versucht wird, Dateien mit Nitro PDF zu kombinieren [LC8423]

- Citrix Director meldet möglicherweise mehrere Verbindungsfehler. Das Problem tritt auf, wenn die Erweiterung von Gruppen, die zur Steuerung der eingeschränkten Sichtbarkeit einer Anwendung zugewiesen werden, für jeden Benutzer verwendet wird. Der Erweiterungsprozess

dauert lange und tritt in großen Netzwerken mit vielen domänenüberspannenden Gruppen auf. [LC8652]

- Die COM-Ports können in Version 7.15 der VDAs möglicherweise nicht zugeordnet werden. [LC8656]
- Beim Versuch, eine veröffentlichte Anwendung zu starten, die unter Microsoft Windows Server 2012 oder 2016 ausgeführt wird, wird Ihr Zugriff möglicherweise gesperrt. [LC8681]
- Wenn Sie eine Anwendung in einer Umgebung mit mehreren Monitoren starten, wird möglicherweise ein Anmeldebanner angezeigt, das beide Monitore umfasst. Bei Verwendung eines einzelnen Monitors wird das Anmeldebannerfenster im Vollbildmodus angezeigt. [LC8741]
- Wenn der lokale App-Zugriff aktiviert ist und Sie Anwendungen auf den veröffentlichten Desktops öffnen, die unter Microsoft Windows 10 ausgeführt werden, können die Anwendungen nicht minimiert werden. [LC8813]
- Beim Verbinden eines Benutzergeräts mit einem VDA wird der Desktop möglicherweise nicht angezeigt. Stattdessen erscheint auf dem Desktop ein grauer Bildschirm. [LC8821]
- Die DLP-Software kann möglicherweise keine Dateien mit UNC-Verknüpfung scannen. [LC8893]
- Nach dem Start einer veröffentlichten Anwendung funktioniert die Num-Taste nicht. Das Problem tritt auf, wenn die LED der Num-Taste auf dem Benutzergerät sichtbar ist, Ziffern jedoch nicht in einer Benutzersitzung funktionieren. Das Problem tritt in bestimmten Szenarien auf, wenn das vom Client angeforderte LED-Update eintrifft, bevor der neu erstellte Remotedesktop seinen LED-Status initialisiert hat. In diesem Fall aktualisiert die WinsStation ihren LED-Status möglicherweise nicht, wodurch der LED-Status von Endpunkt und VDA nicht mehr synchron ist. [LC8921]
- Der Versuch, Anwendungen und Desktops zu starten, kann fehlschlagen. Das Problem tritt auf, wenn der VDA für Serverbetriebssysteme nicht mehr reagiert.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard;
  Name: EnableSCardHookVcResponseTimeout;
  Typ: DWORD;
  Wert: 1 [LC8969]
- Das Öffnen von VM-gehosteten Anwendungen kann fehlschlagen. [LC9001]
- Der Befehl **WFQuerySessionInformation** des WFAPI SDKs zum Abrufen der VDA-Version in einer Sitzung funktioniert möglicherweise nicht. [LC9041]
- Nach dem Upgrade von XenApp und XenDesktop von Version 7.14 auf 7.15 kann es beim Wechsel zwischen den Registerkarten einer veröffentlichten Anwendung dazu kommen, dass die Anwendung nicht mehr reagiert. Wenn Sie zudem das Seamlessfenster verkleinern und anschließend

wieder erweitern, dauert es einige Zeit, bis alle Elemente im Fenster wieder angezeigt werden. [LC9078]

- Eine veröffentlichte Anwendung wird unter Umständen unmittelbar nach dem Start beendet. [LC9167]
- Wenn Sie in einer Millennium-Suite die Verbindung zu einer Seamlessanwendung wiederherstellen und dabei eine andere Bildschirmauflösung als bei der ersten Verbindung verwenden, wird die Größe der Anwendung möglicherweise falsch angepasst. Das Fenster wird dann unter Umständen abgeschnitten angezeigt. [LC9214]
- Das Starten von Anwendungen aus Citrix Receiver für Mac schlägt möglicherweise fehl. Das Problem tritt auf, wenn die Clientlizenz (LicenseRequestClientLicense) nicht abgerufen werden kann. [LC9286]

Smartcards

- Bei Verwendung einer Smartcard können Anwendungen von Drittanbietern hängenbleiben, anstatt die PIN-Eingabeaufforderung anzuzeigen. [LC8805]

Systemausnahmen

- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei picadm.sys mit einem Bluescreen und mit Bugcheckcode 0x22 kommen. [LC6177]
- Auf Servern kann es in picadm.sys zu einer schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA) kommen. [LC6985]
- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei picadm.sys mit einem Bluescreen und mit Bugcheckcode 0x22 kommen. [LC7574]
- In dem Prozess "Service Host"(svchost.exe) kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls icaendpoint.dll auf. [LC7694]
- Auf Servern kann es in vdtw30.dll zu einer schwerwiegenden Ausnahme mit Bluescreen und Stoppcode SYSTEM_SERVICE_EXCEPTION (3b) kommen. [LC8087]
- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei pdcrypt2.sys mit einem Bluescreen und mit Bugcheckcode 0x3B kommen. Das Problem tritt auf, wenn ein VDA gestartet wird. [LC8328]
- Wenn HDX 3D Pro und GPU-Hardwarecodierung aktiviert sind und NVIDIA-GPUs verwendet werden, wird der Citrix Softwaregrafikprozess (Ctxgfx.exe) möglicherweise unerwartet beendet. Das Problem tritt bei Verwendung hochauflösender Bildschirme auf. [LC8435]

- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei icardd.dll mit einem Bluescreen und mit Bugcheckcode 0x0000003B kommen. [LC8492]
- Auf VDAs für Serverbetriebssysteme kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. [LC8708]
- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei icardd.dll mit einem Bluescreen und mit Bugcheckcode 0x0000003B kommen. [LC8732]
- Auf VDAs kann es in picadm.sys zu einer schwerwiegenden Ausnahme mit Bluescreen und Bugcheckcode 0x22 kommen. [LC8749]
- Wenn Sie sich nach dem Neustart des VDA zum ersten Mal anmelden, kann eine unerwartete Zugriffsverletzung auftreten. Der Citrix Softwaregrafikprozess (Ctxgfx.exe) wird unerwartet beendet. Dadurch kann die Qualität von Text und Bildern auf dem VDA beeinträchtigt werden. [LC9005]
- Windows Explorer kann in folgenden Fällen unerwartet geschlossen werden:
  - Wenn eine große Anzahl von Dateien ausgewählt wird, deren Namen mehr als 260 Zeichen enthält, und die Option **Senden an** > **Faxempfänger** ausgewählt wird.
  - Wenn versucht wird, Anwendungen von Drittherstellern zu öffnen.
  - Wenn versucht wird, Dateien mit Nitro PDF zu kombinieren [LC9076]

Benutzererfahrung

- Wenn Sie Inhalt aus einer auf einem Client ausgeführten Anwendung kopieren und in eine Anwendung einer Benutzersitzung einfügen, wird der Inhalt möglicherweise nicht eingefügt. Außerdem kann die Schaltfläche **Einfügen** deaktiviert sein. [LC8516]
- Auf dem VDA für Serverbetriebssysteme verschwindet der Mauszeiger möglicherweise aus der Sitzung. Dieses Problem tritt auf, wenn der Cursor in die **Textauswahl** wechselt und die Hintergrundfarbe der Farbe des Cursors für die **Textauswahl** entspricht. Die Standardhintergrundfarbe für bearbeitbare Bereiche in Microsoft Windows ist weiß, ebenso wie die Standardfarbe des Cursors für die **Textauswahl**. Daher ist der Cursor möglicherweise nicht mehr sichtbar. [LC8807]
- Microsoft Windows behält bei der Sitzungsanmeldung möglicherweise das bearbeitbare Kennwortfeld bei, obwohl die richtigen Anmeldeinformationen bereits eingegeben wurden. [LC9407]

Benutzeroberfläche

- Der Desktophintergrund wird angezeigt, obwohl die Richtlinie "Desktophintergrund"auf "Nicht zugelassen"gesetzt wurde. [LC8398]

Sonstiges

- Bestimmte Anwendungen von Drittanbietern, die zum Überprüfen der Sitzungsanzeige eines Linux VDAs verwendet werden, zeigen möglicherweise nicht alle Pixel an. [LC8419]
- RunOnce-Registrierungsschlüssel sind möglicherweise nicht korrekt implementiert. [LC9260]
- Dieser Fix bietet kleinere Leistungs- und Qualitätsverbesserungen für Enlightened Data Transport (EDT). [LC9278]

Virtual Desktop-Komponenten –Sonstiges

- Das LastPasswordset-Attribut in Active Directory wird möglicherweise nicht korrekt aktualisiert, wenn Sie die VDA-Version 7.15 LTSR verwenden. [lC8387]
- Nachdem der Delivery Controller auf Version 7.15 aktualisiert wurde, zeigen aktive Sitzungen für anonyme Benutzer an, dass eine Anmeldung ausgeführt wird. Diese Situation führt zu einem falschen Lastindex für den VDA. [LC8771]
- Gestartete Anwendungen werden möglicherweise in einem Double-Hop-Szenario nicht im Aktivitätsmanager von Citrix Director angezeigt. [LC8985]
- Der Registrierungsstatus zwischen dem Delivery Controller und dem VDA ist möglicherweise inkonsistent, was zu einer Neuregistrierung beim Starten des VDA führt. [LC9216]

Sonstiges

Wenn der Citrix Telemetriedienst deaktiviert oder angehalten wurde und Sie XenApp und XenDesktop 7.15 LTSR mit einem Metainstaller auf das kumulative Update 1 (CU1) aktualisieren, wird möglicherweise die folgende Warnmeldung angezeigt:

Der Citrix Dienst für die Registrierung in Call Home kann nicht starten. Weitere Informationen finden Sie unter CTX218094.”[LCM-3642]

Cumulative Update 1 (CU1)

September 16, 2021

Releasedatum: 4. Dezember 2017

Info zu diesem Release

Das kumulative Update 1 (CU1) für XenApp und XenDesktop 7.15 LTSR behebt mehr als 80 Probleme, die seit dem Erstrelease von 7.15 LTSR gemeldet wurden.

7.15 LTSR (Allgemeine Informationen)

Seit XenApp und XenDesktop 7.15 LTSR (Erstrelease) behobene Probleme

Bekannte Probleme in diesem Release

Veraltete und entfernte Produkte und Features

Berechtigungsdaten des Citrix-Produkts für Subscription Advantage

Vor dem Upgrade von 7.6 LTSR CU5

Der Hauptvorteil des Upgrades von 7.6 LTSR CU5 auf 7.15 LTSR CU1 besteht darin, dass die Basis 7.15 LTSR wesentlich mehr Features enthält als die Basis 7.6 LTSR. Wenn Sie diese Aktualisierung in Betracht ziehen, beachten Sie jedoch, dass eine kleine Teilmenge der Korrekturen, die in 7.6 LTSR CU5 enthalten sind, in 7.15 LTSR CU1 nicht vorhanden ist. Das liegt daran, dass 7.15 LTSR CU1 vor 7.6 LTSR CU5 veröffentlicht wurde. Eine Liste der Korrekturen, die für 7.15 gelten, aber nicht in 7.15 LTSR CU1 enthalten sind, finden Sie unter Liste der Korrekturen in 7.6 LTSR CU5, aber nicht in 7.15 LTSRCU1. Wenn Ihre Bereitstellung von bestimmten Fixes in 7.6 LTSR CU5 abhängig ist, empfiehlt Citrix, dass Sie diese Liste vor dem Upgrade überprüfen.

Neue Bereitstellungen

Wie stelle ich das CU1 von Grund auf bereit?

Mit dem CU1-Metainstaller können Sie eine neue XenApp und XenDesktop-Umgebung basierend auf dem CU1 einrichten. Bevor Sie das tun, empfehlen wir Ihnen, sich mit dem Produkt vertraut zu machen:

Bevor Sie mit der Planung der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 LTSR (Erstrelease) und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

Das CU1 umfasst Updates für 13 Basiskomponenten von 7.15 LTSR. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf CU1 zu aktualisieren. Beispiel: Wenn Provisioning Services zur LTSR-Bereitstellung gehört, aktualisieren Sie die Provisioning Services-Komponenten auf die CU1-Version. Wenn Provisioning Services nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR CU1

7.15 LTSR CU1-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15.1000	
VDA für Serverbetriebssystem	7.15.1000	
Delivery Controller	7.15.1000	
Citrix Studio	7.15.1000	
Citrix Director	7.15.1000	
Gruppenrichtlinienverwaltung	3.1.1000	
StoreFront	3.12.1000	
Provisioning Services	7.15.1	
Universeller Druckserver	7.15.1000	
Sitzungsaufzeichnung	7.15.1000	nur Platinum Edition
Linux VDA	7.15.1000	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15.1000	
Verbundauthentifizierungsdienst	7.15.1000	

XenApp und XenDesktop 7.15 LTSR CU1-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR kompatible Komponenten und Plattformen	Version
AppDNA	7.16
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19
Citrix SCOM Management Pack für StoreFront	1.13
Citrix SCOM Management Pack für XenApp und XenDesktop	3.14
HDX RealTime Optimization Pack	2.2.100
Lizenzserver	11.14.0.1 Build 22103
Workspace Environment Management	4.4
App Layering	4.6
Self-Service-Kennwortzurücksetzung	1.1

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit XenApp und XenDesktop 7.15 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen •Windows 7-Maschinen: begrenzte LTSR-Unterstützung bis zum 14. Januar 2020 (CU-Anforderungen gelten) AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonyme Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren/aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation. Weitere Informationen finden Sie unter Analysedaten zu Installationen und Upgrades.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp LTSR 7.15 CU1. Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der Kernkomponenten von XenApp 7.15 LTSR CU1 und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15 CU1-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.

- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15 LTSR CU1-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15 CU1-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Liste der Korrekturen in 7.6 LTSR CU5, aber nicht in 7.15 LTSR CU1

Wenn Sie ein Upgrade von 7.6 LTSR CU5 auf 7.15 LTSR CU1 in Betracht ziehen, beachten Sie, dass einige wenige Korrekturen von 7.6 LTSR CU5 nicht in 7.15 LTSR CU1 enthalten sind. Wenn Ihre Bereitstellung von bestimmten Fixes in 7.6 LTSR CU5 abhängig ist, empfiehlt Citrix, dass Sie diese Liste vor dem Upgrade überprüfen.

- LC6311
- LC6985
- LC7430
- LC7450
- LC7574
- LC7600
- LC7777
- LC7911
- LC8046
- LC8080
- LC8130
- LC8170
- LC8281
- LC8339
- LC8492
- LC8732
- LC8750
- LC8774

Behobene Probleme

May 9, 2022

Das kumulative Update 1 (CU1) für XenApp und XenDesktop 7.15 LTSR behebt mehr als 80 Probleme, die seit dem Erstrelease von 7.15 LTSR gemeldet wurden.

Citrix Director

- Wenn Sie die Director-Konsole öffnen und erstmals Benutzer suchen, wird der Ladebalken nicht angezeigt. Bei anschließenden Suchvorgängen wird die Leiste angezeigt. [LC8190]

Citrix Richtlinie

- Versuche, eine neue USB-Umleitungsregel einer Benutzerrichtlinie in Active Directory hinzuzufügen, schlagen möglicherweise fehl. Das Problem tritt auf, wenn die Bildlaufleiste nicht verfügbar ist. [LC8112]
- Bei dem Versuch, die Richtlinie "Druckerzuweisungen"zu verwalten, können die folgenden Probleme auftreten:
  - Die Ausnahme "InvalidCastException"tritt auf, wenn die Richtlinie "Druckerzuweisungen" hinzugefügt oder bearbeitet wird.
  - Die Ausnahme"InvalidOperationException"tritt beim Hinzufügen eines neuen Sitzungsdruckers auf.
  - Versuche, einen Sitzungsdrucker aus der Richtlinie "Druckerzuweisungen"zu entfernen, schlagen fehl. Dieses Problem tritt auf, wenn die Option "Entfernen"deaktiviert ist.
  - Wenn Sie mit dem Eingeben im Suchfeld der Richtlinie "Druckerzuweisung"aufhören, wird die Suchaktion nicht gestartet.
  - Die Kontrollkästchen zum Überschreiben der Sitzungsdruckereinstellung (PrintQuality, PaperSize, Scale und TrueTypeOption) sind immer aktiviert, auch wenn Sie sie zuvor deaktiviert haben. [LC8146]

Citrix Studio

- Wenn Sie versuchen, einer Bereitstellungsgruppe benutzerdefinierte Maschinen hinzuzufügen, werden möglicherweise nicht zugewiesene Maschinen auf der Seite "Maschinenzuteilung" angezeigt. [LC6755]

- Versuche, auf Maschinenkataloge in Citrix Studio zuzugreifen, können dazu führen, dass Citrix Studio unerwartet beendet wird und die folgende Ausnahme auftritt:

  "Fehler-ID: XDDS:ABB14FD9"[LC7961]

- Der Text für die Option "Lokaler Speicher auf dem Hypervisor"im Assistenten "Verbindung und Ressourcen hinzufügen"wird bei Ausführung unter einer nicht-englischen Version von Windows möglicherweise abgeschnitten. [LC8041]
- Nach dem Upgrade von Citrix Studio auf Version 7.14.1 wird die Spalte "Verwendet von"(die sich auf die Bereitstellungsgruppe bezieht, welche die Anwendung verwendet) für vorhandene App-V-Pakete möglicherweise leer angezeigt. [LC8075]
- Wenn Sie in Citrix Studio auf den Hyperlink "Bereitstellungsgruppe"klicken, werden Sie möglicherweise nicht an den ausgewählten Knoten weitergeleitet. [LC8095]
- Bei dem Versuch, die Richtlinie "Druckerzuweisungen"zu verwalten, können die folgenden Probleme auftreten:
  - Die Ausnahme "InvalidCastException"tritt auf, wenn die Richtlinie "Druckerzuweisungen" hinzugefügt oder bearbeitet wird.
  - Die Ausnahme"InvalidOperationException"tritt beim Hinzufügen eines neuen Sitzungsdruckers auf.
  - Versuche, einen Sitzungsdrucker aus der Richtlinie "Druckerzuweisungen"zu entfernen, schlagen fehl. Dieses Problem tritt auf, wenn die Option "Entfernen"deaktiviert ist.
  - Wenn Sie mit dem Eingeben im Suchfeld der Richtlinie "Druckerzuweisung"aufhören, wird die Suchaktion nicht gestartet.
  - Die Kontrollkästchen zum Überschreiben der Sitzungsdruckereinstellung (PrintQuality, PaperSize, Scale und TrueTypeOption) sind immer aktiviert, auch wenn Sie sie zuvor deaktiviert haben. [LC8146]
- Nach dem Upgrade von Delivery Controller auf Version 7.15 schlagen Versuche fehl, Citrix Studio auf dem Delivery Controller zu starten. Folgende Fehlermeldung wird angezeigt:

  "MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand" [LC8396]

- Wenn Sie den Knoten "Bereitstellungsgruppen"in Citrix Studio und anschließend die Registerkarte "Anwendung"auswählen, funktioniert der Hyperlink auf dieser Registerkarte möglicherweise nicht. [LC8555]

Controller

- Enthält eine Bereitstellungsgruppe einen oder mehrere VDAs im Wartungsmodus, können Sie sie möglicherweise nicht auswählen, um veröffentlichte Anwendungen zu starten. [LC6943]

- Nach der Aktualisierung eines mit Maschinenerstellungsdiensten erstellten Maschinenkatalogs können die unter vSAN 6 (oder höher) gehostete virtuellen Maschinen möglicherweise nicht mehr gestartet werden. Die folgende Fehlermeldung wird in der VMware-Konsole angezeigt:

  A general system error occurred: PBM error occurred during PreProcessReconfigureSpec: pbm.fault.PBMFault; Error when trying to run pre-provision validation; Invalid entity. [LC7860]

- Versuche, auf Maschinenkataloge in Citrix Studio zuzugreifen, können dazu führen, dass Citrix Studio unerwartet beendet wird und die folgende Ausnahme auftritt:

  "Fehler-ID: XDDS:ABB14FD9"[LC7961]

- In Citrix Director wird möglicherweise zu jeder vollen Stunde eine falsche Anzahl getrennter Sitzungen angezeigt. [LC8006]

- Die "AllowRestart"-Richtlinie für unter dem Serverbetriebssystem laufende Sitzungen ermöglicht keine Abmeldung von getrennten Sitzungen. Wenn Sie eine getrennte Sitzung neu starten, wird statt einer neuen Sitzung die Verbindung zur vorherigen Sitzung wiederhergestellt. [LC8090]

- Bei dem Versuch, die Richtlinie "Druckerzuweisungen"zu verwalten, können die folgenden Probleme auftreten:

  - Die Ausnahme "InvalidCastException"tritt auf, wenn die Richtlinie "Druckerzuweisungen" hinzugefügt oder bearbeitet wird.
  - Die Ausnahme"InvalidOperationException"tritt beim Hinzufügen eines neuen Sitzungsdruckers auf.
  - Versuche, einen Sitzungsdrucker aus der Richtlinie "Druckerzuweisungen"zu entfernen, schlagen fehl. Dieses Problem tritt auf, wenn die Option "Entfernen"deaktiviert ist.
  - Wenn Sie mit dem Eingeben im Suchfeld der Richtlinie "Druckerzuweisung"aufhören, wird die Suchaktion nicht gestartet.
  - Die Kontrollkästchen zum Überschreiben der Sitzungsdruckereinstellung (PrintQuality, PaperSize, Scale und TrueTypeOption) sind immer aktiviert, auch wenn Sie sie zuvor deaktiviert haben. [LC8146]

- Der Überwachungsdienst kann möglicherweise keine neuen Sitzungsdaten an die Überwachungsdatenbank weitergeben. [LC8191]

- Im Bereich "Anmeldedauer per Benutzersitzung"unter **Director** > **Trends** > **Anmeldungsleistung** werden unter Umständen nur Teile von Anmeldedatensätze angezeigt. [LC8265]

- Nach dem Upgrade von Delivery Controller auf Version 7.15 schlagen Versuche fehl, Citrix Studio auf dem Delivery Controller zu starten. Folgende Fehlermeldung wird angezeigt:

  "MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand" [LC8396]

- In einer großen XenApp und XenDesktop-Umgebung funktioniert die gespeicherte Prozedur zum Überwachen der Datenbankoptimierung nicht ordnungsgemäß, wenn die Überwachungsdatenbank groß ist. [LC8770]

HDX MediaStream Flash-Umleitung

- Wenn die HDX MediaStream Flash-Umleitung aktiviert ist, können Flash-Videos möglicherweise nicht auf MSN.com und News.com wiedergegeben werden. [LC6823]

Linux VDA

Linux Virtual Delivery Agent 7.15 LTSR CU1 Dokumentation enthält spezifische Informationen zu den Updates in diesem Release.

Profilverwaltung

- Die Profilverwaltung kann zur Anzeige eines schwarzen Bildschirms führen, wenn versucht wird, eine Windows 10-Sitzung zu starten. Für diesen Fix müssen Sie die Richtlinie "Zu synchronisierende Verzeichnisse"konfigurieren und den Ordner ""*AppData\Local\Microsoft\Windows\Caches*" hinzufügen. [LC7596]
- Wenn Sie sich von einem VDA unter Microsoft Windows 10 abmelden, wird die Datei "ntuser.dat" möglicherweise verwendet und nicht in den Profilverwaltungsspeicher kopiert. Daher gehen die Änderungen an dem Registrierungsschlüssel "HKEY_CURRENT_USER"verloren. [LC8068]
- Wenn die Richtlinie "Lokal zwischengespeicherte Profile nach Abmeldung löschen"aktiviert und "Verzögerung vor dem Löschen von zwischengespeicherten Profilen"auf zwei Minuten festgelegt ist, wird möglicherweise ein neues lokales Profil erstellt, wenn Sie versuchen, sich innerhalb von zwei Minuten mit demselben Benutzerkonto bei einer Sitzung ab- und wieder anzumelden. [LC8388]

Provisioning Services

Die Dokumentation zu Provisioning Services 7.15 LTSR CU1 enthält Informationen zu den Updates in diesem Release.

StoreFront

- Wenn "TWIMode"für einige Anwendungen auf "Aus"gesetzt ist, werden alle Anwendungen im Fenstermodus gestartet, wenn Sie Citrix Receiver für Chrome verwenden. [LC7558]

- Wenn zwei oder mehr Stores in StoreFront vorhanden sind, kann durch Klicken auf "Remotezugriffseinstellungen konfigurieren"im ersten oder zweiten Store der Storename des zuletzt hinzugefügten Stores dupliziert werden. [LC8089]
- Wenn Sie Stores mit gemeinsamer Authentifizierung in StoreFront konfigurieren, können bei dem Versuch, ein neues NetScaler Gateway-Gerät mit einem Store zu verbinden, vorhandene, bereits verbundene NetScaler Gateway-Geräte entfernt werden. Wenn Sie versuchen, sich an den Stores anzumelden, wird die folgende Fehlermeldung angezeigt:

  "Der Anmeldung ist abgelaufen. Melden Sie sich erneut an, um fortzufahren."

  Darüber hinaus zeigt die StoreFront-Konsole doppelte Storenamen an. [LC8219]
- Beim Importieren eines Stores mit HTML5-Konfiguration über den PowerShell-Befehl "Import-STFConfiguration"wird der Import möglicherweise erfolgreich abgeschlossen. Allerdings scheitern Versuche, eine Anwendung mit Citrix Receiver für HTML5 zu starten. [LC8290]
- Der StoreFront-Server zeigt möglicherweise NULL-Einträge für Receiver für Web-Sites in der Konsole an. Das Problem tritt auf, wenn der Name des Stores mit dem Text "discovery"in der URL beginnt. [LC8320]
- Wenn der W3C-Protokollierungsdienst aktiviert ist, schlagen möglicherweise Versuche fehl, die StoreFront-Konfiguration zu ändern, und die folgende Fehlermeldung wird angezeigt:

  "Ein Fehler ist beim Speichern der Änderungen aufgetreten."[LC8370]
- Wenn das Socketpooling aktiviert und die Sitedatenbankkonnektivität inkonsistent ist, werden die Sockets in StoreFront möglicherweise erschöpft, wenn Sie sich dauernd anmelden und abmelden. [LC8514]

VDA für Desktopbetriebssystem

HDX MediaStream Flash-Umleitung

- Wenn die HDX MediaStream Flash-Umleitung aktiviert ist, können Flash-Videos möglicherweise nicht auf MSN.com und News.com wiedergegeben werden. [LC6823]
- Versuche, Microsoft Office-Dateien (z. B. Excel-Kalkulationstabellen) zu speichern, die in einer Sitzung mit aktivierten HDX-Seamless-Apps ausgeführt werden, können dazu führen, dass die Dateien unerwartet geschlossen werden. [LC8572]

HDX Plug-n-Play

- USB-Geräte, die dieselbe Seriennummer für mehrere Geräte melden, wie Syn-Tech ProKee V2, werden möglicherweise nicht an eine VDA-Sitzung weitergeleitet. CDF-Trace zeigt Folgendes:

Failed to assign the instance ID, error 0xc000000d. [LC8264]

Drucken

- Versuche, eine veröffentlichte Anwendung zu starten, schlagen möglicherweise fehl, wenn die Anwendung auf ein Mutex-Objekt im Citrix Druck-Manager-Dienst (cpsvc.exe) wartet. [LC6829]
- Der Citrix Druckmanagerdienst (cpsvc.exe) wird möglicherweise sporadisch beendet. [LC7535]
- Sitzungsdrucker können beim Sitzungsroaming zwischen Clients nicht gelöscht werden. Wenn Sie beispielsweise die Richtlinie "Druckerzuweisungen"mit Drucker A für Client A und Drucker B für Client B konfigurieren, kann Drucker A nicht gelöscht werden, wenn Sie von Client A zu Client B wechseln. [LC8077]

Server- /Siteverwaltung

- VDA 7.12 oder höher: Wenn Sie versuchen, die Anzeige der Sprachenleiste in einer Seamlesssitzung zu unterdrücken, indem Sie das Seamlessflag von Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI auf "0x00040000"setzen (deaktiviert den Sprachenleistenagent), wird die Sprache nicht länger ausgeblendet. [LC8349]

Sitzung/Verbindung

- Ist der lokale App-Zugriff aktiviert, wird bei Verwendung der Haftungsausschlussrichtlinie für die interaktive Anmeldung 45 Sekunden lang ein schwarzer oder grauer Bildschirm angezeigt. [LC6518]
- Der Versuch einer erneuten Verbindung mit einer Anwendung kann fehlschlagen. Das Problem tritt auf, wenn eine der getrennten Anwendungen beim ersten Trennen abstürzt. [LC6550]
- Wenn Sie eine Sitzung mit zwei Bildschirmen und HDX 3D Pro sperren, wird nur der primäre Bildschirm gesperrt. [LC7767]
- Wenn Sie einen Skype for Business-Videoanruf starten, kann bei Überschneiden mit dem Fenster einer anderen Anwendung ein blauer Fensterrand erscheinen. [LC7773]
- Ist der lokale App-Zugriff aktiviert, wird bei Verwendung der Haftungsausschlussrichtlinie für die interaktive Anmeldung ein schwarzer oder grauer Bildschirm angezeigt. [LC7798]
- Manche veröffentlichte Anwendungen füllen bei Maximierung nicht den gesamten Bildschirm aus. [LC7854]

- Beim Kopieren und Einfügen zwischen zwei Microsoft Excel 2010-Arbeitsblättern auf einem VDA der Version 7.9 kann das Excel-Fenster aufhören zu reagieren. [LC7912]
- In bestimmten Szenarien werden Seamlessanwendungen möglicherweise nicht im Seamless-modus angezeigt oder bestimmte Features funktionieren nicht. [LC8030]
- Wenn HDX 3D Pro auf einem VDA aktiviert ist und die Richtlinie "Nachricht für Benutzer, die sich anmelden wollen"aktiviert ist, kann der Versuch, nach der Anmeldung einen veröffentlichten Desktop zu starten, fehlschlagen und ein grauer Bildschirm erscheint.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\BitmapRemotingConfig;
  Name: HKLM_DisableMontereyFBCOnInit;
  Typ: DWORD;
  Wert: 1 zum Aktivieren [LC8082]
- Ist der lokale App-Zugriff aktiviert, wird bei Verwendung der Haftungsausschlussrichtlinie für die interaktive Anmeldung möglicherweise ein schwarzer oder grauer Bildschirm angezeigt. [LC8136]
- Wenn Sie Anwendungen verwenden, die eine umgeleitete Webcam einsetzen, z. B. Skype for Business oder einen VLC-Medienplayer, wird die Webcam möglicherweise beim ersten Sitzungsstart umgeleitet und erkannt. Wenn Sie die Verbindung zur Benutzersitzung wiederherstellen, wird die Webcam jedoch nicht mehr erkannt. Es wird ein grauer Bildschirm statt der Videovorschau angezeigt. [LC8588]

Smartcards

- Wenn Sie sich mit einer Smartcard bei einer Sitzung anmelden, reagiert die Sitzung möglicherweise nicht mehr, bis Sie sie trennen und wieder verbinden. [#LC8036]

Systemausnahmen

- Der Prozess wfshell.exe wird möglicherweise unerwartet beendet und verweist auf das Modul für die Taskleistengruppierung. [LC6968]
- Wenn die Richtlinie für die USB-Umleitung aktiviert ist, kann bei VDAs eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e) auftreten. [LC7999]
- Auf VDAs kann es zu einer schwerwiegenden Ausnahme mit einem Bluescreen und mit Bugcheckcode 0x7E kommen. Das Problem tritt auf, wenn Sie die VDA-Sitzung für einige Zeit inaktiv lassen. [LC8045]

- Bei Servern kann bei picavc.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e) auftreten. [LC8063]

Benutzererfahrung

- Beim Wiederverbinden mit einer Sitzung einer Seamlessanwendung werden die Anwendungsfenster auf der Clientseite möglicherweise nicht richtig angezeigt. Stattdessen sind die Sitzungsgrafiken in einem kleinen Rechteck zu sehen. [LC7857]
- In Windows Media Player können Dateien im Microsoft-AVI-Format (.avi) ggf. vertikal gespiegelt angezeigt werden. [LC8308]
- Wenn eine veröffentlichte Anwendung auf dem Bildschirm des dritten Monitors maximiert ist, deckt die Anwendung möglicherweise nicht den gesamten Bildschirm ab. Stattdessen wird ein schwarzer Rahmen angezeigt. [LC8472]
- Die Seamlessanwendungen, die in VDA 7.15 gehostet werden, zeigen beim Verschieben des Anwendungsfensters möglicherweise einen grauen oder schwarzen Rahmen im Hintergrund. [LC8551]

Benutzeroberfläche

- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC7557]

VDA für Serverbetriebssystem

HDX MediaStream Flash-Umleitung

- Versuche, Microsoft Office-Dateien (z. B. Excel-Kalkulationstabellen) zu speichern, die in einer Sitzung mit aktivierten HDX-Seamless-Apps ausgeführt werden, können dazu führen, dass die Dateien unerwartet geschlossen werden. [LC8572]

HDX Plug-n-Play

- USB-Geräte, die dieselbe Seriennummer für mehrere Geräte melden, wie Syn-Tech ProKee V2, werden möglicherweise nicht an eine VDA-Sitzung weitergeleitet. CDF-Trace zeigt Folgendes:

  Failed to assign the instance ID, error 0xc000000d. [LC8264]

Drucken

- Versuche, eine veröffentlichte Anwendung zu starten, schlagen möglicherweise fehl, wenn die Anwendung auf ein Mutex-Objekt im Citrix Druck-Manager-Dienst (cpsvc.exe) wartet. [LC6829]
- Der Citrix Druckmanagerdienst (cpsvc.exe) wird möglicherweise sporadisch beendet. [LC7535]
- Sitzungsdrucker können beim Sitzungsroaming zwischen Clients nicht gelöscht werden. Wenn Sie beispielsweise die Richtlinie "Druckerzuweisungen"mit Drucker A für Client A und Drucker B für Client B konfigurieren, kann Drucker A nicht gelöscht werden, wenn Sie von Client A zu Client B wechseln. [LC8077]

Server- /Siteverwaltung

- Für VDA 7.12 oder höhere Versionen: Wenn Sie versuchen, die Anzeige der Sprachenleiste in einer Seamlesssitzung zu unterdrücken, indem Sie das Seamlessflag unter Registrierungsschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI auf "0x00040000"setzen (deaktiviert den Sprachenleistenagenten), ist die Sprache nicht länger ausgeblendet. [#LC8349]

Sitzung/Verbindung

- Der Versuch einer erneuten Verbindung mit einer Anwendung kann fehlschlagen. Das Problem tritt auf, wenn eine der getrennten Anwendungen beim ersten Trennen abstürzt. [LC6550]
- Wenn Sie in der Statusleiste eines Sitzungsstarts auf "Abbrechen"klicken, können falsche Sitzungsinformationen auf dem Delivery Controller verbleiben. Die aktuelle Sitzung wird dann nicht auf dem VDA erstellt und Sie können möglicherweise keine neue Sitzung starten. [LC6779]
- Das Mikrofon kann bei Benutzersitzungen zeitweise umgeleitet werden, obwohl die Richtlinie "Clientmikrofonumleitung"auf "Nicht zulässig"gesetzt wurde.

  Das Problem wird durch diesen Fix behoben. Tritt es weiterhin auf, wenden Sie auf dem Gerät mit dem Mikrofon folgenden Registrierungsschlüssel an:

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    Name: MaxPolicyAge
    Typ: DWORD;
    Wert: maximale Zeit (in Sekunden) zwischen der letzten Richtlinienauswertung und dem Zeitpunkt der Endpunktaktivierung. Die Standardeinstellung ist 30 Sekunden.

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig;
    Name: PolicyTimeout;
    Typ: DWORD;
    Wert: maximale Zeit (in Millisekunden), die das System auf Richtlinien wartet, nachdem festgestellt wurde, dass die Richtlinien nicht aktuell sind. Der Standardwert ist 4000 Millisekunden. Wenn das Timeout auftritt, liest das System die Richtlinien und fährt mit der Initialisierung fort. Wenn Sie den Wert auf 0 setzen, wird die Prüfung der Active Directory-Richtlinien umgangen und Richtlinien werden sofort verarbeitet. [LC7495]

- Wenn Sie einen Skype for Business-Videoanruf starten, kann bei Überschneiden mit dem Fenster einer anderen Anwendung ein blauer Fensterrand erscheinen. [LC7773]
- Manche veröffentlichte Anwendungen füllen bei Maximierung nicht den gesamten Bildschirm aus. [LC7854]
- Nach dem Upgrade eines VDAs auf Version 7.13, 7.14 oder 7.15 kann bei Verwendung von vGPU in veröffentlichten Anwendungen oder Desktops unter Windows Server ein schwarzer Bereich angezeigt werden. [LC7875]
- Beim Kopieren und Einfügen zwischen zwei Microsoft Excel 2010-Arbeitsblättern auf einem VDA der Version 7.9 kann das Excel-Fenster aufhören zu reagieren. [LC7912]
- In bestimmten Szenarien werden Seamlessanwendungen möglicherweise nicht im Seamlessmodus angezeigt oder bestimmte Features funktionieren nicht. [LC8030]
- Ist der lokale App-Zugriff aktiviert, wird bei Verwendung der Haftungsausschlussrichtlinie für die interaktive Anmeldung möglicherweise ein schwarzer oder grauer Bildschirm angezeigt. [LC8136]
- Serverbetriebssystem-VDAs können sporadisch neu registriert werden, wenn eine "Außer Betrieb"-Benachrichtigung an die Delivery Controller gesendet wird. [LC8228]
- Wenn Sie Anwendungen verwenden, die eine umgeleitete Webcam einsetzen, z. B. Skype for Business oder einen VLC-Medienplayer, wird die Webcam möglicherweise beim ersten Sitzungsstart umgeleitet und erkannt. Wenn Sie die Verbindung zur Benutzersitzung wiederherstellen, wird die Webcam jedoch nicht mehr erkannt. Es wird ein grauer Bildschirm statt der Videovorschau angezeigt. [LC8588]

Smartcards

- Wenn Sie sich mit einer Smartcard bei einer Sitzung anmelden, reagiert die Sitzung möglicherweise nicht mehr, bis Sie sie trennen und wieder verbinden. [LC8036]

Systemausnahmen

- Der Prozess wfshell.exe wird möglicherweise unerwartet beendet und verweist auf das Modul für die Taskleistengruppierung. [LC6968]
- Windows Shell Experience Host kann unerwartet beendet werden, wenn Sie auf den Lautstärkeregler auf der Taskleiste klicken. [LC7000]
- In dem Prozess "Service Host"(svchost.exe) kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls icaendpoint.dll auf. [LC7900]
- Wenn die Richtlinie für die USB-Umleitung aktiviert ist, kann bei VDAs eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e) auftreten. [LC7999]
- Bei Servern kann bei picavc.sys eine schwerwiegende Ausnahme mit Bluescreen und Bugcheckcode SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e) auftreten. [LC8063]

Benutzererfahrung

- Beim Wiederverbinden mit einer Sitzung einer Seamlessanwendung werden die Anwendungsfenster auf der Clientseite möglicherweise nicht richtig angezeigt. Stattdessen sind die Sitzungsgrafiken in einem kleinen Rechteck zu sehen. [LC7857]
- In Windows Media Player können Dateien im Microsoft-AVI-Format (.avi) ggf. vertikal gespiegelt angezeigt werden. [LC8308]
- Wenn eine veröffentlichte Anwendung auf dem Bildschirm des dritten Monitors maximiert ist, deckt die Anwendung möglicherweise nicht den gesamten Bildschirm ab. Stattdessen wird ein schwarzer Rahmen angezeigt. [LC8472]
- Die Seamlessanwendungen, die in VDA 7.15 gehostet werden, zeigen beim Verschieben des Anwendungsfensters möglicherweise einen grauen oder schwarzen Rahmen im Hintergrund. [LC8551]

Benutzeroberfläche

- Beim Abmelden von einer Seamlesssitzung mit nicht gespeicherten Daten über das Connection Center wird ein schwarzes Fenster angezeigt.

  Die darin enthaltene Meldung weist darauf hin, dass Programme noch geschlossen werden müssen, und es werden die Optionen "Abmelden erzwingen"und "Abbrechen"angeboten. Die Option "Abbrechen"funktioniert nicht.

Nach der Installation dieses Fixes funktioniert die Option "Abbrechen"einwandfrei. [LC6075]

- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC7557]
- Der Abmeldebildschirm wird möglicherweise nicht angezeigt, wenn Sie versuchen, sich von einer Microsoft Windows Server 2008 R2-Desktopsitzung abzumelden. Sie können sich möglicherweise von der Sitzung abmelden, die Sitzung wird jedoch so angezeigt, als ob sie unerwartet getrennt wurde. [LC8016]

Virtual Desktop-Komponenten –Sonstiges

- In Citrix Director wird möglicherweise zu jeder vollen Stunde eine falsche Anzahl getrennter Sitzungen angezeigt. [LC8006]
- Der Überwachungsdienst kann möglicherweise keine neuen Sitzungsdaten an die Überwachungsdatenbank weitergeben. [LC8191]
- Im Bereich "Anmeldedauer per Benutzersitzung"unter **Director** > **Trends** > **Anmeldungsleistung** werden unter Umständen nur Teile von Anmeldedatensätze angezeigt. [LC8265]
- Der Client für System Center Configuration Manager (SCCM) wird möglicherweise nach dem Update von Microsoft Windows 10 von Build 1511 auf Build 1703 unerwartet beendet, wenn ein VDA darauf installiert. [LC8632]
- Zurücksetzen von Microsoft Office 2016 ist funktioniert möglicherweise unter Microsoft Windows 10 nicht, wenn Sie Maschinenerstellungsdienste (MCS) verwenden. [LC8680]
- In einer großen XenApp und XenDesktop-Umgebung funktioniert die gespeicherte Prozedur zum Überwachen der Datenbankoptimierung nicht ordnungsgemäß, wenn die Überwachungsdatenbank groß ist. [LC8770]

7.15 LTSR (Erstrelease)

January 21, 2022

Releasedatum: 04. April 2017

Info zu diesem Release

XenApp und XenDesktop Long Term Service Release (LTSR) 7.15 enthält neue Versionen der Windows-VDAs und einiger XenApp- und XenDesktop-Kernkomponenten.
Sie haben folgende Möglichkeiten:

- **Installieren oder Aktualisieren einer XenApp- oder XenDesktop-Site**

Installieren oder aktualisieren Sie alle Kernkomponenten und Virtual Delivery Agents (VDAs) mit der ISO-Datei. Nach der Installation bzw. dem Aktualisieren auf die neueste Version können Sie alle neuen Features nutzen.

- **Installieren oder Aktualisieren von VDAs in einer vorhandenen Site**

Wenn Sie eine XenApp- oder XenDesktop-Bereitstellung haben und noch kein Upgrade der Kernkomponenten durchführen können, können Sie durch eine Installation eines VDAs bzw. ein Upgrade auf den aktuellen VDA die aktuellen HDX-Features verwenden. Ein bloßes Upgrade der VDAs ist beispielsweise nützlich, wenn Sie die Erweiterungen in einer Testumgebung testen möchten.

Weitere Informationen finden Sie unter Vorbereiten der Installation bzw. Upgrade einer Bereitstellung.

Die XenApp- und XenDesktop-Downloadseiten für dieses Release enthalten auch aktualisierte Versionen der nachfolgend aufgeführten Software. Weitere Informationen zu Features und Installationsanweisungen finden Sie in der Dokumentation der jeweiligen Komponente.

StoreFront

AppDNA

Citrix SCOM Management Pack für XenApp und XenDesktop

Eine Übersicht über die Features, die seit XenApp and XenDesktop 7.6 LTSR hinzugefügt wurden, finden Sie unter XenApp und XenDesktop 7.15 LTSR - Featuresübersicht im Vergleich.

Das Produktrelease enthält außerdem die folgenden, seit XenApp und XenDesktop 7.14.1, neuen, geänderten oder erweiterten Features.

VDA-Installation auf Maschinen ohne Microsoft Media Foundation

Bei den meisten unterstützten Windows-Editionen ist Microsoft Media Foundation bereits installiert. Wenn Media Foundation auf der Maschine, auf der Sie einen VDA installieren, nicht installiert ist (z. B. N-Editionen), werden mehrere Multimediafeatures nicht installiert und sind nicht funktionsfähig. Sie können diese Einschränkung bestätigen oder die VDA-Installation beenden und später, nach der Installation von Media Foundation neu beginnen. Diese Auswahl wird bei der grafischen Oberfläche per Meldung angeboten. In der Befehlszeile können Sie zum Bestätigen der Einschränkung die Option "/no_mediafoundation_ack"verwenden.

Upgrade eines XenApp 6.5-Workers auf einen neuen VDA

Nach der Migration einer XenApp 6.5-Farm können Sie ein Upgrade eines XenApp 6.5-Workers auf einen neuen VDA durchführen. Zuvor wurde bei Ausführung des Installationsprogramms für XenApp

und XenDesktop auf dem Workerserver die XenApp 6.5-Software automatisch entfernt und dann der neue VDA installiert. Jetzt entfernen Sie in separaten Verfahren zuerst HRP7 und die XenApp 6.5-Software vom Server. Dann installieren Sie den neuen VDA. Informationen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA.

MCS unterstützt VMs der zweiten Generation

Wenn Sie VMs mit Microsoft System Center Virtual Machine Manager bereitstellen, können Sie jetzt Maschinenerstellungsdienste (MCS) zum Bereitstellen von VMs der zweiten Generation verwenden.

Lokaler Hostcache

Bei einer Neuinstallation von XenApp und XenDesktop ist der lokale Hostcache standardmäßig aktiviert. Das Verbindungsleasing ist standardmäßig deaktiviert.

Nach einem Upgrade bleibt die Einstellung für den lokalen Hostcache erhalten. War der lokale Hostcache beispielsweise in der Vorgängerversion aktiviert, ist er auch in der aktualisierten Version aktiviert. Wenn der lokale Hostcache in der früheren Version nicht aktiviert war (oder nicht unterstützt wurde), bleibt er in der aktualisierten Version deaktiviert.

Director

Überwachen von Anwendungsstörungen In Director wird die Ansicht "Trends"durch die Registerkarte **Anwendungsstörungen** erweitert, auf der historische Fehler bei veröffentlichten Anwendungen angezeigt werden. Es werden Störungen und Fehler beim Starten oder Ausführen der ausgewählten Anwendung bzw. des ausgewählten Prozesses während des ausgewählten Zeitraums angezeigt. Diese Informationen helfen bei Analyse und Behebung anwendungsspezifischer Probleme. Weitere Informationen finden Sie im Abschnitt "Problembehandlung bei Anwendungen"unter Überwachen historischer Anwendungsstörungen.

Standardmäßig werden auf Serverbetriebssystem-VDAs gehostete Anwendungen auf Fehler überwacht. Sie können die Überwachungseinstellungen über die Überwachungsgruppenrichtlinien ändern: "Überwachung von Anwendungsausfällen aktivieren", "Überwachung von Ausfällen auf Desktop-OS-VDAs"und "Von der Fehlerüberwachung ausgeschlossene Anwendungen". Weitere Informationen finden Sie unter Richtlinien für die Überwachung auf Anwendungsfehler im Artikel "Einstellungen der Überwachungsrichtlinie".

Für dieses Feature sind Delivery Controller und VDAs ab Version 7.15 erforderlich. Desktopbetriebssystem-VDAs ab Windows Vista und Serverbetriebssystem-VDAs ab Windows Server 2008 werden unterstützt.

Virtual Delivery Agents (VDAs) 7.15

Nach dem Upgrade von VDAs von Version 7.9, 7.11, 7.12, 7.13 oder 7.14 ist keine Aktualisierung der Funktionsebene des Maschinenkatalogs erforderlich. Die Standardebene (7.9 oder höher) ist weiterhin die aktuelle Funktionsebene. Weitere Informationen finden Sie unter VDA-Versionen und Funktionsebenen.

Sitzungsaufzeichnung 7.15

Lastausgleich für die Sitzungsaufzeichnung: Dieses experimentelle Feature aus XenApp und XenDesktop 7.14 ist nicht in diesem Release enthalten.

Neue Bereitstellungen

Wie stelle ich 7.15 LTSR von Grund auf bereit?

Mit dem 7.15-LTSR-Metainstaller* können Sie eine neue XenApp- oder XenDesktop-Umgebung einrichten. Wir empfehlen, dass Sie sich vorher mit dem Produkt vertraut machen:

Bevor Sie mit dem Planen der Bereitstellung beginnen, lesen Sie die Dokumentation zu XenApp und XenDesktop 7.15 Long Term Service Release und besonders die Abschnitte Technische Übersicht, Installation und Konfiguration und Sicherheit. Stellen Sie sicher, dass die Systemanforderungen für alle Komponenten erfüllt sind. Der Abschnitt Installation und Konfiguration enthält Bereitstellungsanweisungen.

*Hinweis: Provisioning Services und Sitzungsaufzeichnung sind als separate Downloads und Installationsprogramme verfügbar.

Vorhandene Bereitstellungen

Wie funktioniert das Aktualisieren

XenApp und XenDesktop 7.15 LTSR umfasst Updates für alle 7.6 LTSR-Basiskomponenten. Nicht vergessen: Citrix empfiehlt, alle LTSR-Komponenten in Ihrer Bereitstellung auf 7.15 LTSR zu aktualisieren. Beispiel: Wenn Provisioning Services zur LTSR-Bereitstellung gehört, aktualisieren Sie die Provisioning Services-Komponente. Wenn Provisioning Services nicht zu Ihrer Bereitstellung gehört, brauchen Sie es nicht zu installieren oder zu aktualisieren.

Seit 7.6 LTSR wurde ein Metainstaller hinzugefügt, mit dem Sie die vorhandenen Komponenten der LTSR-Umgebung über eine einheitliche Benutzeroberfläche aktualisieren können. Aktualisieren Sie anhand der Upgradeanweisungen mit dem Metainstaller die LTSR-Komponenten Ihrer Bereitstellung.

Basiskomponenten von XenApp und XenDesktop 7.15 LTSR

7.15 LTSR-Basiskomponente	Version	Hinweise
VDA für Desktopbetriebssystem	7.15	
VDA für Serverbetriebssystem	7.15	
Delivery Controller	7.15	
Citrix Studio	7.15	
Citrix Director	7.15	
Gruppenrichtlinienverwaltung	3.1	
StoreFront	3.12	
Provisioning Services	7.15	
Universeller Druckserver	7.15	
Sitzungsaufzeichnung	7.15	nur Platinum Edition
Linux VDA	7.15	Informationen zu den unterstützten Plattformen finden Sie in der Linux VDA-Dokumentation.
Profilverwaltung	7.15	
Verbundauthentifizierungsdienst	7.15	

XenApp und XenDesktop 7.15 LTSR-kompatible Komponenten

Die folgenden Komponenten sind in der angegebenen Version kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden. Citrix fordert Sie u. U. auf, ein Upgrade auf eine neuere Version der folgenden Komponenten in Ihrer 7.15 LTSR-Umgebung durchzuführen.

Mit 7.15 LTSR kompatible Komponenten und Plattformen	Version
AppDNA	7.15
Citrix SCOM Management Pack for License Server	1.2
Citrix SCOM Management Pack für Provisioning Services	1.19

Mit 7.15 LTSR kompatible Komponenten und Plattformen	Version
Citrix SCOM Management Pack für StoreFront	1.12
Citrix SCOM Management Pack für XenApp und XenDesktop	3.13
HDX RealTime Optimization Pack	2.3
Lizenzserver	11.14.0 Build 21103
Workspace Environment Management	4.4
App Layering	4.3
Self-Service-Kennwortzurücksetzung	1.1

Kompatible Versionen der Citrix Workspace-App

Alle derzeit unterstützten Versionen der Citrix Workspace-App sind mit Citrix Virtual Apps and Desktops 1912 LTSR kompatibel. Informationen zum Lebenszyklus der Citrix Workspace-App finden Sie unter Lifecycle Milestones for Citrix Workspace app & Citrix Receiver.

Wenn Sie den RSS-Feed der Citrix Workspace-App abonnieren, erhalten Sie eine Benachrichtigung, wenn eine neue Version der Citrix Workspace-App zur Verfügung steht.

XenApp und XenDesktop 7.15 LTSR –wichtige Ausschlüsse

Für die folgenden Features, Komponenten und Plattformen können die 7.15-LTSR-Lebenszyklusmeilensteine und Vorteile nicht in Anspruch genommen werden. Insbesondere sind kumulative Updates und die mit dem erweiterten Lebenszyklus verbundenen Vorteile ausgeschlossen. Updates für ausgeschlossene Features und Komponenten sind durch regelmäßige aktuelle Releases verfügbar.

Ausgeschlossene Features
Framehawk
StoreFront/Citrix Online-Integration

Ausgeschlossene Komponenten
Personal vDisk: für Windows 10-Maschinen ausgeschlossen

Ausgeschlossene Komponenten
AppDisks

Ausgeschlossene Windows Plattformen *
Windows 2008 32 Bit (für den universellen Druckserver)

*Citrix behält sich das Recht vor, die Plattformunterstützung basierend auf den Lebenszyklusmeilensteinen von Drittanbietern zu aktualisieren.

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonyme Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren/aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation.

XenApp 6.5-Migration

Der XenApp 6.5-Migrationsprozess ermöglicht eine effiziente und schnelle Migration von einer XenApp 6.5-Farm auf eine Site mit XenApp 7.15 LTSR (oder ein neueres unterstütztes Release). Dies ist nützlich bei Bereitstellungen mit vielen Anwendungen und Citrix Gruppenrichtlinien, da das Fehlerrisiko beim manuellen Verschieben von Anwendungen und Citrix Gruppenrichtlinien in die neue XenApp-Site verringert wird.

Nach der Installation der XenApp 7.15-LTSR-Kernkomponenten und dem Erstellen einer Site wird der Migrationsprozess in der folgenden Reihenfolge ausgeführt:

- Führen Sie das XenApp 7.15-Installationsprogramm auf jedem XenApp 6.5-Worker aus. Damit wird dieser automatisch auf einen neuen Virtual Delivery Agent für Serverbetriebssysteme zur Verwendung in der neuen Site aktualisiert.
- Führen Sie PowerShell-Export-Cmdlets auf einem XenApp 6.5-Controller aus, um die Anwendung und Citrix Richtlinieneinstellungen in XML-Dateien zu exportieren.
- Bearbeiten Sie ggf. die XML-Dateien, um genau zu bestimmen, welche Elemente Sie in die neue Site importieren möchten. Durch Anpassen der Dateien können Sie Richtlinien- und Anwendungseinstellungen phasenweise (d. h. einige sofort, andere später) in die XenApp 7.15-LTSR-Site importieren.
- Führen Sie PowerShell-Import-Cmdlets auf dem neuen XenApp 7.15-Controller aus, um die Einstellungen aus den XML-Dateien in die neue XenApp-Site zu importieren.

Konfigurieren Sie die neue Site nach Bedarf um und testen Sie sie.

Weitere Informationen finden Sie unter Migrieren von XenApp 6.x

Behobene Probleme

May 9, 2022

Die folgenden Probleme wurden seit Version 7.14.1 behoben:

Behobene Probleme gegenüber Version 7.14.1

Seit Version 7.6 LTSR CU4 behobene Probleme

Behobene Probleme gegenüber Version 7.14.1

Citrix Director

- Wenn Sie in Citrix Director zur Registerkarte **Trends** > **Fehler** > **Verbindung** navigieren, wird möglicherweise die folgende Fehlermeldung angezeigt:

  Unerwarteter Fehler. Überprüfen Sie die Netzwerkverbindung oder suchen Sie im Director-Serverereignisprotokoll nach weiteren Informationen. [LC7755]

- Versuche, Richtlinieninformationen für bestimmte Sitzungen in Citrix Director anzuzeigen, können fehlschlagen und die folgende Fehlermeldung wird angezeigt:

  Daten können nicht abgerufen werden. [LC8207]

Citrix Richtlinie

- Gruppenrichtlinienobjekte, die Einstellungen für Citrix und Microsoft enthalten, werden u. U. nicht erzwungen. Dieses Problem tritt auf, wenn die Erweiterungseinheit in der Liste mehr als zwei GUIDs enthält. [LC7533]

Citrix Studio

- Das Hinzufügen von Computerkonten zu neuen oder vorhandenen Maschinenkatalogen schlägt möglicherweise fehl, wenn anstelle von PowerShell-Befehlen die GUI verwendet wird. Das Problem tritt auf, wenn das Verzeichnissuchtool beim Ermitteln des NetBIOS-Namens nicht das richtige Objekt bindet.

  Lautet beispielsweise der Name der Domäne “xyz.ad.airxyz.aa”und der NetBIOS-Name “xyz-Ad”, wird bei Verwendung der GUI der NetBIOS-Name “xyz”statt “xyz-Ad”akzeptiert. Das Maschinenkonto kann dann für vorhandene und neue Computerkonten nicht hinzugefügt werden. [LC6679]

- Nach dem Upgrade des Citrix Delivery Controllers auf Version 7.12 kann das Hinzufügen von Maschinen aus Citrix Provisioning Services (PVS) zu einem Katalog in einer Umgebung mit mehreren Domänen fehlschlagen. Das Problem tritt auf, wenn PVS den Domänennamen nicht zusammen mit dem Gerätenamen zurückgibt. Wenn Citrix Studio den Kontonamen in der lokalen Domäne sucht, wird das Konto nicht gefunden. [LC6818]
- Die Veröffentlichung von App-V-Anwendungen kann fehlschlagen. [LC7421]
- Wenn ein Administrator versucht, einer Bereitstellungsgruppe eine App-V-Anwendung aus einer Isolationsgruppe hinzuzufügen oder eine Isolationsgruppe zu erstellen, wird in Citrix Studio möglicherweise die folgende Fehlermeldung angezeigt:

  Ein unbekannter Fehler ist aufgetreten. [LC7594]
- Das Hinzufügen von Maschinen zu einer Bereitstellungsgruppe unter Verwendung des NETBIOS-Namens für die Benutzerzuordnung kann fehlschlagen. Stattdessen wird u. U. der Domänenname angezeigt. Das Problem tritt auf, wenn vom NETBIOS-Namen die falsche URL verwendet wird. [LC7830]

Controller

- Nach dem Upgrade des Citrix Delivery Controllers auf Version 7.12 kann das Hinzufügen von Maschinen aus Citrix Provisioning Services (PVS) zu einem Katalog in einer Umgebung mit mehreren Domänen fehlschlagen. Das Problem tritt auf, wenn PVS den Domänennamen nicht zusammen mit dem Gerätenamen zurückgibt. Wenn Citrix Studio den Kontonamen in der lokalen Domäne sucht, wird das Konto nicht gefunden. [LC6818]
- Beim Hinzufügen von Maschinen zu einem MCS-Katalog wird möglicherweise nicht das Roundrobinverfahren für mehrere Speicher angewendet, die die neuen Maschinen aufnehmen könnten. [LC7456]
- Die Erstellung von Isolationsgruppen durch benutzerdefinierte Administratoren kann unter Anzeige der folgenden Fehlermeldung fehlschlagen:

  Sie haben nicht die erforderlichen Berechtigungen, um diese Anforderung abzuschließen. Weitere Informationen erhalten Sie von Ihrem XenDesktop-Siteadministrator. [LC7563]
- Wenn ein Administrator versucht, einer Bereitstellungsgruppe eine App-V-Anwendung aus einer Isolationsgruppe hinzuzufügen oder eine Isolationsgruppe zu erstellen, wird in Citrix Studio möglicherweise die folgende Fehlermeldung angezeigt:

  Ein unbekannter Fehler ist aufgetreten. [LC7594]
- Wird versucht, TLSv1.0 auf einem Citrix Delivery Controller zu deaktivieren, kann dies zum Verlust der Kommunikation mit dem VMware vCenter-Hypervisor führen. [LC7686]

- Das Hinzufügen von Maschinen zu einer Bereitstellungsgruppe unter Verwendung des NETBIOS-Namens für die Benutzerzuordnung kann fehlschlagen. Stattdessen wird u. U. der Domänenname angezeigt. Das Problem tritt auf, wenn vom NETBIOS-Namen die falsche URL verwendet wird. [LC7830]

Profilverwaltung

- Beim Öffnen von Dateien in einem Profil, für das Profilstreaming aktiviert ist, wird die Datei nach dem Anmelden möglicherweise leer angezeigt. [LC6996]
- Auf Servern kann es zu einer schwerwiegenden Ausnahme bei upmjit.sys mit einem Bluescreen und mit Bugcheckcode 0x135 kommen. [LC7841]
- UserProfileManager.exe wird möglicherweise unerwartet beendet, wenn Sie sich bei einem VDA anmelden. [LC7952]

StoreFront

- In Bereitstellungen mit Multisiteaggregation kann der Versuch, die Verbindung für getrennte Sitzungen wiederherzustellen, fehlschlagen. Dies kann zum Erhalt einer zweiten Instanz derselben Ressource führen. [LC7453]
- Wenn ein Teil der Quelle einer aggregierten Anwendung deaktiviert wird, wird die Anwendung für den Endbenutzer möglicherweise unerwartet ausgeblendet. [LC7675]
- Ein Deaktivieren der Option "Konto-Self-Service"in StoreFront wird möglicherweise nicht wirksam, selbst wenn die Option als deaktiviert angezeigt wird. [LC7744]
- Beim Versuch, die freigegebene Authentifizierung für Stores in StoreFront zu entfernen, kann beim Speichern der Änderungen die folgende Fehlermeldung angezeigt werden:

  "Ein Fehler ist beim Speichern der Änderungen aufgetreten."[LC7781]

Universeller Druckserver

Client

- Der Druckspoolerdienst kann aufhören, zu reagieren, sodass Universal Printing nicht funktioniert. Das Problem wird durch ein Timeout beim Warten auf eine Transaktionsantwort vom Spoolerdienst verursacht. [LC5209]
- Wenn Sie die Profilverwaltung verwenden, werden Änderungen an Citrix Universeller Druckserver-Druckern (Hinzufügen, Entfernen, Umbenennen), die in einer Sitzung auf

einem Server gemacht werden, möglicherweise nicht korrekt in anschließenden Sitzungen auf einem anderen Server widergespiegelt. [LC7645]

Server

- Das Drucken eines Dokuments kann unter Anzeige der folgenden Fehlermeldung fehlschlagen:

  Aufgrund eines Problems mit der Druckereinrichtung kann von Windows nicht gedruckt werden. [LC6825]

- Beim Verwenden bestimmter Drucker wird in Microsoft Editor möglicherweise die Meldung "Handle ist ungültig"angezeigt und der Druck schlägt fehl. Das Problem tritt auf, wenn in der Citrix Richtlinie "Verwendung universeller Druckertreiber"die Einstellung "Nur druckermodellspezifische Treiber verwenden"und in der Citrix Richtlinie "Universellen Druckserver aktivieren"die Einstellung "Aktiviert ohne Fallback auf systemeigenen Windows-Remotedruck" konfiguriert ist. [LC7623]

VDA für Desktopbetriebssystem

Installation, Deinstallation, Upgrade

- Nach einem Upgrade des VDAs von Version 5.6.400 auf Version 7.9 kann das Neustarten des VDAs dazu führen, dass die Spiegelungstreiber der vorherigen Version zurückbleiben. [LC6295]
- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7555]
- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7587]

Drucken

- Der Citrix Druckmanagerdienst (cpsvc.exe) kann aufhören zu reagieren und unerwartet beendet werden, wenn sich neue Benutzer anmelden. [LC6933]
- Nach einem Upgrade des VDAs von Version 7.9 auf Version 7.12 oder höher werden beim Drucken aus Microsoft Internet Explorer mit dem Citrix universellen Druckertreiber die Drucke nicht im ausgewählten Ausgabefach sondern immer in Fach 1 ausgegeben. [LC7463]

Sitzung/Verbindung

- Wenn mehrere Webcams des gleichen Modells auf einem Desktopbetriebssystem-VDA installiert sind, wird möglicherweise nur die letzte Webcam in einer Sitzung erkannt und zugeordnet. [LC5008]
- Ein Wechselclientlaufwerk wird möglicherweise vom WFAPI SDK auf einem Desktopbetriebssystem-VDA nicht zurückgegeben. [LC6877]
- Die Fensterpositionen werden möglicherweise nicht beibehalten, wenn Sie die Verbindung mit einer veröffentlichten Desktopsitzung wiederherstellen und mehrere Monitore verwenden. [LC7644]
- Beim Wechseln von Sitzungen zwischen mehreren Monitoren im Vollbildmodus mit aktiviertem Legacygrafikmodus und ohne dass Desktop Viewer konfiguriert ist, wird die Sitzung u. U. nur auf einem Monitor ausgeführt. [LC7907]

Smartcards

- Durch das Entfernen eines Smartcardlesers wird die Benutzersitzung eventuell nicht gesperrt, selbst wenn eine Sperrung für diesen Fall konfiguriert ist. [LC7411]

Systemausnahmen

- Auf VDAs kann es zu einer schwerwiegenden Ausnahme bei vd3dk.sys mit einem Bluescreen und mit Bugcheckcode 0X00000050 kommen. [LC6833]
- Auf VDAs kann es beim Herunterfahren von Sitzungen zu einer schwerwiegenden Ausnahme bei picadm.sys mit einem Bluescreen und mit Bugcheckcode 0x7E kommen. [LC7545]
- In dem Prozess "Service Host"(svchost.exe) kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls scardhook64.dll auf. [LC7580]
- Auf Servern kann es zu einem schwerwiegenden Fehler mit vdtw30.dll kommen, ein Bluescreen wird angezeigt (Stoppcode 0xc0000006). [LC7608]
- Auf VDAs kann es zu einer schwerwiegenden Ausnahme bei tdica.sys mit einem Bluescreen und Bugcheckcode kommen. [LC7632]
- Mit diesem Fix wird ein Speicherproblem mit der Datei wdica.sys behoben, durch das Server ggf. unerwartet beendet wurden. [LC7666]

Benutzererfahrung

- Dieser Fix bietet verbesserte Unterstützung für Töne, die nur kurz wiedergegeben werden, wenn hohe Clientaudioqualität verwendet wird.

  Hinweis:

  - Der Fix wird nicht in Sitzungen unter Windows Server 2008 R2 nicht wirksam.
  - Der Fix funktioniert nur unter Citrix Receiver 4.4 für Windows Long Term Service Release (LTSR) CU5 oder höher und XenApp-/XenDesktop-VDA-Version 7.6 LTSR CU4 oder höher. [LC5842]

- Beim Kopieren und Einfügen zwischen zwei Microsoft Excel 2010-Arbeitsblättern auf einem VDA der Version 7.9 kann das Excel-Fenster aufhören zu reagieren. [LC7481]
- Definieren Sie in einer Umgebung mit mehreren Monitoren den externen Monitor in Windows als Hauptanzeige und platzieren Sie ihn rechts neben dem Monitor des sekundären Laptops oder Tablets in den Anzeigeeinstellungen der Systemsteuerung. Wenn Sie eine veröffentlichte Anwendung starten, die auf dem externen Monitor angezeigt wird, und diese Anwendung auf den an den externen Monitor angeschlossenen Tablet- bzw. Laptop-Monitor verschieben, wird bei Öffnen oder Schließen des Tablet-/Laptop-Deckels die veröffentlichte Anwendung schwarz angezeigt.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel auf dem VDA fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire; Name: EnableDrvTw2NotifyMonitorOrigin; Typ: REG_DWORD; Wert: 1 (aktivieren) oder 0 (deaktivieren; 0 = Standardwert). Standardmäßig fehlt der Registrierungswert. [LC7760]

Benutzeroberfläche

- URL-Verknüpfungssymbole werden bei Verwendung eines touchoptimierten Desktops möglicherweise leer angezeigt. [LC6663]
- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC7557]

VDA für Serverbetriebssystem

Installation, Deinstallation, Upgrade

- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7555]

- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7587]

Drucken

- Der Citrix Druckmanagerdienst (cpsvc.exe) kann aufhören zu reagieren und unerwartet beendet werden, wenn sich neue Benutzer anmelden. [LC6933]
- Nach einem Upgrade des VDAs von Version 7.9 auf Version 7.12 oder höher werden beim Drucken aus Microsoft Internet Explorer mit dem Citrix universellen Druckertreiber die Drucke nicht im ausgewählten Ausgabefach sondern immer in Fach 1 ausgegeben. [LC7463]

Server- /Siteverwaltung

- Die folgende Fehlermeldung wird Benutzern einer untergeordneten Domäne möglicherweise beim Starten einer Anwendung über das Webinterface oder StoreFront angezeigt:

  Sie haben keine Zugriffsrechte auf diese veröffentlichte Anwendung. [LC7566]

Sitzung/Verbindung

- Wenn mehrere Webcams des gleichen Modells auf einem Desktopbetriebssystem-VDA installiert sind, wird möglicherweise nur die letzte Webcam in einer Sitzung erkannt und zugeordnet. [LC5008]
- Wiederverbindungsversuche mit einer Sitzung schlagen manchmal fehl und führen dazu, dass die VDAs für Serverbetriebssysteme in den Initialisierungszustand versetzt werden. Das Problem tritt auf, wenn der VDA bei einem Delivery Controller erneut registriert wird. [LC6647]
- Aktive Sitzungen werden möglicherweise auf den XenApp-Servern getrennt, wenn die Delivery Controller-Verbindung verloren geht. Das Problem tritt auf, wenn VDAs den Status von Sitzungen beim Übergang von "Vor Start"zu "Aktiv"nicht richtig verfolgen. Aus diesem Grund versucht der Delivery Controller beim Neustart, die Ressourcen aus den VDAs zu löschen. Sitzungen im Status "Vor Start"werden dann getrennt oder abgemeldet, während Anwendungen aktiv genutzt werden. [LC6819]
- Wenn Sie eine veröffentlichte Anwendung auf Microsoft Windows Server 2016 starten, wird möglicherweise einige Sekunden lang ein schwarzer Bildschirm angezeigt, bevor die Anwendung sichtbar wird. [LC7947]

Systemausnahmen

- Auf VDAs kann es beim Herunterfahren von Sitzungen zu einer schwerwiegenden Ausnahme bei picadm.sys mit einem Bluescreen und mit Bugcheckcode 0x7E kommen. [LC7545]
- In dem Prozess "Service Host"(svchost.exe) kann eine Zugriffsverletzung auftreten, worauf der Prozess unerwartet beendet wird. Das Problem tritt aufgrund des fehlerhaften Moduls scardhook64.dll auf. [LC7580]
- Auf Servern kann es zu einem schwerwiegenden Fehler mit vdtw30.dll kommen, ein Bluescreen wird angezeigt (Stoppcode 0xc0000006). [LC7608]
- Auf VDAs kann es zu einer schwerwiegenden Ausnahme bei tdica.sys mit einem Bluescreen und Bugcheckcode kommen. [LC7632]
- Mit diesem Fix wird ein Speicherproblem mit der Datei wdica.sys behoben, durch das Server ggf. unerwartet beendet wurden. [LC7666]

Benutzererfahrung

- Dieser Fix bietet verbesserte Unterstützung für Töne, die nur kurz wiedergegeben werden, wenn hohe Clientaudioqualität verwendet wird.

  Hinweis:

  - Der Fix wird nicht in Sitzungen unter Windows Server 2008 R2 nicht wirksam.
  - Der Fix funktioniert nur unter Citrix Receiver 4.4 für Windows Long Term Service Release (LTSR) CU5 oder höher und XenApp-/XenDesktop-VDA-Version 7.6 LTSR CU4 oder höher. [LC5842]

- Beim Kopieren und Einfügen zwischen zwei Microsoft Excel 2010-Arbeitsblättern auf einem VDA der Version 7.9 kann das Excel-Fenster aufhören zu reagieren. [LC7481]
- Definieren Sie in einer Umgebung mit mehreren Monitoren den externen Monitor in Windows als Hauptanzeige und platzieren Sie ihn rechts neben dem Monitor des sekundären Laptops oder Tablets in den Anzeigeeinstellungen der Systemsteuerung. Wenn Sie eine veröffentlichte Anwendung starten, die auf dem externen Monitor angezeigt wird, und diese Anwendung auf den an den externen Monitor angeschlossenen Tablet- bzw. Laptop-Monitor verschieben, wird bei Öffnen oder Schließen des Tablet-/Laptop-Deckels die veröffentlichte Anwendung schwarz angezeigt.

  Zum Implementieren dieses Fixes legen Sie folgenden Registrierungsschlüssel auf dem VDA fest:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire; Name: EnableDrvTw2NotifyMonitorOrigin; Typ: REG_DWORD; Wert: 1 (aktivieren) oder 0 (deaktivieren; 0 = Standardwert). Standardmäßig fehlt der Registrierungswert. [LC7760]

Benutzeroberfläche

- URL-Verknüpfungssymbole werden bei Verwendung eines touchoptimierten Desktops möglicherweise leer angezeigt. [LC6663]
- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC7557]

Virtual Desktop-Komponenten –Sonstiges

- Die Veröffentlichung von App-V-Anwendungen kann fehlschlagen. [LC7421]
- Der Versuch, App-V-Anwendungen im Einzelverwaltungsmodus zu starten, kann fehlschlagen. Das Problem tritt auf, wenn der Anwendungsname Sonderzeichen enthält. [LC7897]

Seit Version 7.6 LTSR CU4 behobene Probleme

Citrix Director

- Citrix Director mit integrierter Windows-Authentifizierung (WIA) funktioniert eventuell nicht mit eingeschränkter Kerberos-Delegierung. [LC5196]
- Beim Anmelden bei Citrix Director tritt der Fehler "System nicht verfügbar"auf. [LC5385]
- In Citrix Director werden Sitzungsdetails möglicherweise nicht angezeigt. Das Problem tritt auf, wenn Sie als Anwendungstyp "Veröffentlicht"verwenden. [LC6577]

Citrix Richtlinie

- Die Citrix Richtlinienverarbeitung reagiert möglicherweise nicht mehr, was dazu führt, dass Benutzersitzungen nicht mehr reagieren. Verbindungsanfragen an Receiver und Remotedesktop (RDP) schlagen dann fehl. [LA4969]
- Bei Systemen mit Fix LC1987 (GPCSExt170W2K8R2X64006 oder dessen Ersatz) werden Active Directory-Richtlinien, die Einstellungen für Citrix und Microsoft enthalten, möglicherweise nicht erzwungen.

  Hinweis: Dieser Fix behebt das Problem für Active Directory-Richtlinien, die Sie nach der Installation dieses Updates erstellen. Es behebt das Problem außerdem für *bestehende* Richtlinien, sofern die Citrix Einstellungen vor den Microsoft-Einstellungen konfiguriert wurden. Es behebt das Problem nicht für bestehende Richtlinien, wenn die Citrix Einstellungen *nach* den Microsoft-Einstellungen konfiguriert wurden. Bei solchen Active Directory-Richtlinien müssen Sie diese öffnen und die Citrix Einstellungen speichern. [LC2121]

- Mit dieser Featureerweiterung generiert die Citrix Gruppenrichtlinienengine zusätzliche Ereignisprotokollmeldungen bei der Verarbeitung von Citrix Richtlinien. [LC3664]
- Nach einem Upgrade von Version 7.6 auf Version 7.8 oder 7.9 sind bestimmte Farbschemas in Citrix Studio möglicherweise zu dunkel für die einwandfreie Anzeige von Text. [LC5690]
- Nach der Installation des Citrix Verbundauthentifizierungsdiensts kann der Versuch einer Konfiguration der Option **Security Access Control Lists** auf dem StoreFront-Server unter **User Rules** dazu führen, dass das Konfigurationsfenster aufhört zu reagieren. [LC5788]
- Der CPU- und RAM-Verbrauch von Microsoft Excel kann beim Öffnen einer XLSM-Datei mit Makros extrem ansteigen. Das Öffnen der Datei schlägt dann fehl. [LC6142]
- Gruppenrichtlinienobjekte, die Einstellungen für Citrix und Microsoft enthalten, werden u. U. nicht erzwungen. Dieses Problem tritt auf, wenn die Erweiterungseinheit in der Liste mehr als zwei GUIDs enthält. [LC7533]

Citrix Studio

- Wenn mehrere Benutzer in zeitgleichen Studio-Sitzungen Richtlinien erstellen, überschreibt die zuletzt erstellte Richtlinie die älteren, wenn Citrix Studio aktualisiert wird. [LA5533]
- Citrix Studio erkennt möglicherweise die XenDesktop App Edition-Lizenz nicht und folgende Fehlermeldung wird angezeigt:

  Keine gültige Lizenz gefunden
  Es sind keine geeigneten Lizenzen verfügbar. Überprüfen Sie die Lizenzserveradresse und dass Produktedition und -modell richtig angegeben sind. [LC0822]
- Beim domänenübergreifenden Hinzufügen von Benutzern zu einer Bereitstellungsgruppe löst Citrix Studio deren tatsächliche Domäne in das lokale Domänenkonto auf. [LC1886
- Beim Veröffentlichen einer Anwendung in Citrix Studio 7.7 mit Befehlszeilenargumenten mit Anführungszeichen (“) wird möglicherweise eine Fehlermeldung angezeigt. [LC4525]
- Citrix Studio bietet möglicherweise eine Rollbackoption für einen Katalog an, selbst wenn keine Katalogaktualisierung erfolgt ist. Bei Verwendung der Rollbackoption kommt es zu einer Ausnahme. [LC4791]
- Das Hinzufügen von Maschinen zu einem Maschinenkatalog in Citrix Studio kann fehlschlagen und zur Anzeige einer Fehlermeldung führen. Das Problem tritt nicht auf, wenn Sie Maschinen mit dem XenDesktop-Setupassistenten hinzufügen. [LC5030]
- Wenn zwei Anwendungen die gleiche ApplicationID haben, führt das Aktualisieren von App-V-Anwendungen u. U. dazu, dass Citrix Studio den App-V-Paketnamen falsch festlegt. [LC5261]

- Wenn ein Delivery Controller offline geht oder aus anderen Gründen nicht verfügbar ist, wird Citrix Studio möglicherweise langsam ausgeführt. [LC5335]
- Nach dem Upgrade von XenApp bzw. XenDesktop von 7.6 auf 7.7 wird in Citrix Studio ab und zu möglicherweise eine Aufforderung zum Upgrade angezeigt. [LC5478]
- Wenn Sie eine Instanz von Citrix Studio Version 7.9, die mit App-V-Servern mit vielen Paketen konfiguriert ist, schließen und versuchen, sie dann wieder zu öffnen, verbleibt Studio im Erweiterungszustand und wird nicht geöffnet. [LC5643]
- Mit Citrix Studio kann einer Site nur ein App-V-Server hinzugefügt werden. Um zusätzliche App-V-Server hinzuzufügen, muss PowerShell verwendet werden. [LC5767]
- Wenn Sie nach dem Upgrade von Citrix Studio von 7.8 auf 7.9 Anwendungen hinzufügen, werden diese ohne Paketnamen oder Version angezeigt. [LC5958]
- Wenn Sie eine Anwendung über den Knoten "Anwendungen"in Citrix Studio hinzufügen, tritt möglicherweise ein Fehler auf und die Anwendung wird nicht hinzugefügt. Verwenden Sie als Workaround den Knoten "Bereitstellungsgruppen"zum Hinzufügen von Anwendungen. [LC5975]
- Beim Erstellen einer XenDesktop-Site über Citrix Studio und Verweisen auf den SQL AlwaysOn-Listener kann folgender Fehler auftreten:

  "Kontakt zur Replikatserver <Servername> konnte nicht hergestellt werden. Überprüfen Sie den Status der Datenbank auf dem SQL-Server. Stellen Sie sicher, dass der Datenbankserver Remoteverbindungen zulässt und die Firewall die Verbindungen nicht blockiert. [LC6010]
- Wenn Sie ein veröffentlichtes App-V Paket aus Citrix Studio entfernen und versuchen, der Bereitstellungsgruppe eine andere Version des gleichen App-V-Pakets mit demselben Namen und Veröffentlichungsort hinzuzufügen, wird das Paket möglicherweise mit einem roten Ausrufezeichen aufgeführt und folgende Fehlermeldung angezeigt:

  Fehler beim Laden der Anwendungsdaten für die Anwendung "ANWENDUNGSNAME". [LC6254]
- Der Versuch, einen Delivery Controller in einer Umgebung mit gespiegelter Datenbank mit der Option zum Hinzufügen eines zusätzlichen Controllers über Citrix Studio und dem PowerShell-Befehl „Add-XDController"hinzuzufügen, kann fehlschlagen. [LC6563]
- Das Hinzufügen von Computerkonten zu neuen oder vorhandenen Maschinenkatalogen schlägt möglicherweise fehl, wenn anstelle von PowerShell-Befehlen die GUI verwendet wird. Das Problem tritt auf, wenn das Verzeichnissuchtool beim Ermitteln des NetBIOS-Namens nicht das richtige Objekt bindet.

  Lautet beispielsweise der Name der Domäne "xyz.ad.airxyz.aa"und der NetBIOS-Name "xyz-Ad", wird bei Verwendung der GUI der NetBIOS-Name "xyz"statt "xyz-Ad"akzeptiert. Das Maschinenkonto kann dann für vorhandene und neue Computerkonten nicht hinzugefügt werden. [LC6679]

- Nach dem Upgrade des Citrix Delivery Controllers auf Version 7.12 kann das Hinzufügen von Maschinen aus Citrix Provisioning Services (PVS) zu einem Katalog in einer Umgebung mit mehreren Domänen fehlschlagen. Das Problem tritt auf, wenn PVS den Domänennamen nicht zusammen mit dem Gerätenamen zurückgibt. Wenn Citrix Studio den Kontonamen in der lokalen Domäne sucht, wird das Konto nicht gefunden. [LC6818]
- Beim Upgrade einer XenApp-Site kann das Lizenzmodell unerwartet von XenApp in XenDesktop wechseln. [LC6981]
- Der Befehl "Start-Transcript"kann für "Get-XDSite"und andere PowerShell-Verwaltungsbefehle hoher Ebene für XenDesktop bei Verwendung von PowerShell 5 fehlgeschlagen. [LC7006]
- Wenn ein Administrator versucht, einer Bereitstellungsgruppe eine App-V-Anwendung aus einer Isolationsgruppe hinzuzufügen oder eine Isolationsgruppe zu erstellen, wird in Citrix Studio möglicherweise die folgende Fehlermeldung angezeigt:

  Ein unbekannter Fehler ist aufgetreten. [LC7594]
- Das Hinzufügen von Maschinen zu einer Bereitstellungsgruppe unter Verwendung des NETBIOS-Namens für die Benutzerzuordnung kann fehlschlagen. Stattdessen wird u. U. der Domänenname angezeigt. Das Problem tritt auf, wenn vom NETBIOS-Namen die falsche URL verwendet wird. [LC7830]

Controller

- Das Bereitstellen virtueller Maschinen mit Maschinenerstellungsdiensten in Citrix Studio schlägt fehl und folgende Fehlermeldung wird angezeigt:

  Fehler-ID: XDDS:0F7CB924. [LC4930]
- Wenn Benutzer versuchen, den gepoolten Katalog unter XenServer zu löschen und dann den Katalog aktualisieren, werden die Basisdatenträger nicht aus dem Speicher entfernt und die Anzahl der Basisdatenträger kann steigen. [LC0577]
- Die Sitzungszuverlässigkeit kann weder über das Active Directory-Gruppenrichtlinienobjekt noch über Citrix Studio in VDA 7.x-Sitzungen, die mit XenDesktop 5.6-Desktop Delivery Controllern (DDCs) starten, deaktiviert werden. [LC0878]
- Wird mit den Maschinenerstellungsdiensten eine gepoolte Maschine von einem Masterimage mit benutzerdefinierten VMX- und NVRAM-Einstellungen erstellt, werden diese Einstellungen nicht auf die neuen virtuellen Maschinen kopiert. [LC0967]
- Bei dem Brokerdienst-Task "PrepareSession"tritt in XenDesktop 5.6-Umgebungen möglicherweise ein Timeout auf, wodurch StoreFront fehlschlägt. [LC1055]

- Dieser Fix behebt ein Timingproblem, das auftreten kann, wenn der Hypervisor beim Formatieren eines PvD-Datenträgervolumes während der anfänglichen Maschinenerstellung stark ausgelastet ist. [LC3275]
- Das Erstellen virtueller Maschinen mit den Maschinenerstellungsdiensten mit VMware vSphere 6.0 und vSAN 6-Speicher kann fehlschlagen. [LC4563]
- Die WaitForTask-Antwort verursacht die Ausnahme VimApi.MissingProperty, die das Aktualisieren von Maschinenkatalogen nicht zulässt. [LC4573]
- Das Hinzufügen von Maschinen zu einem Maschinenkatalog in Citrix Studio kann fehlschlagen und zur Anzeige einer Fehlermeldung führen. Das Problem tritt nicht auf, wenn Sie Maschinen mit dem XenDesktop-Setupassistenten hinzufügen. [LC5030]
- Nach dem Upgrade der VDAs auf Version 7.8 kann bei dem Versuch, den Bestand zu aktualisieren, die folgende Fehlermeldung angezeigt werden:

  Das Aktualisieren des Bestands schlug unter Anzeige der Meldung "Ein interner Fehler ist aufgetreten. Fehlercode: 0x2"fehl. [LC5051]
- Am Ende von Anzeigenamen und Beschreibungen bestimmter Citrix Dienste können unter japanischen Betriebssystemen überflüssige Zeichen angezeigt werden. [LC5208]
- Wenn zwei Anwendungen die gleiche ApplicationID haben, führt das Aktualisieren von App-V-Anwendungen u. U. dazu, dass Citrix Studio den App-V-Paketnamen falsch festlegt. [LC5261]
- Nach dem Upgrade von XenApp bzw. XenDesktop von 7.6 auf 7.7 wird in Citrix Studio ab und zu möglicherweise eine Aufforderung zum Upgrade angezeigt. [LC5478]
- Ein kaufmännisches Und-Zeichen (&) im Titel einer Anwendung kann zur Beschädigung des StoreFront-XML-Codes führen, sodass keine Anwendungen oder Symbole angezeigt werden. [LC5505]
- Wenn Sie eine Instanz von Citrix Studio Version 7.9, die mit App-V-Servern mit vielen Paketen konfiguriert ist, schließen und versuchen, sie dann wieder zu öffnen, verbleibt Studio im Erweiterungszustand und wird nicht geöffnet. [LC5643]
- Nach dem Upgrade auf XenDesktop 7.9 schlägt die Anmeldung gelegentlich fehl, weil der NetScaler-Broker Anmeldeinformationen nicht richtig sendet. [LC5753]
- Mit Citrix Studio kann einer Site nur ein App-V-Server hinzugefügt werden. Um zusätzliche App-V-Server hinzuzufügen, muss PowerShell verwendet werden. [LC5767]
- Nach der Installation des Citrix Verbundauthentifizierungsdiensts kann der Versuch einer Konfiguration der Option **Security Access Control Lists** auf dem StoreFront-Server unter **User Rules** dazu führen, dass das Konfigurationsfenster aufhört zu reagieren. [LC5788]
- Das Ändern des SDK-Ports von Flexcast Management Architecture-Diensten wie Analytics, Broker, Log usw. führt dazu, dass Citrix Studio keine einwandfreie Verbindung herstellen kann.

[LC6005]

- Beim Erstellen einer XenDesktop-Site über Citrix Studio und Verweisen auf den SQL AlwaysOn-Listener kann folgender Fehler auftreten:

  "Kontakt zur Replikatserver <Servername> konnte nicht hergestellt werden. Überprüfen Sie den Status der Datenbank auf dem SQL-Server. Stellen Sie sicher, dass der Datenbankserver Remoteverbindungen zulässt und die Firewall die Verbindungen nicht blockiert. [LC6010]

- In Citrix Director wird im Dashboard möglicherweise eine Zahl nicht registrierter Maschinen angezeigt, die nicht mit dem Bericht auf der Seite "Trends"übereinstimmt. [LC6184]

- Der Überwachungsdienst kann keine neuen Sitzungsdaten an die Überwachungsdatenbank weitergeben, wenn die Lastauswertungsprogrammindex-Richtlinie aktiviert ist. Als Folge kann Citrix Director u. U. keine aktuellen Informationen für Sitzungen, wie Anmeldedauer, aktuelle Anzahl aktiver Sitzungen, usw., anzeigen. Das Problem wird zwar in Citrix Director angezeigt, verursacht wird es jedoch durch ein Problem im Delivery Controller. In der aktuellen Version des Controllers wurde das Problem behoben. [LC6241]

- Bei dem Versuch, eine Hosteinheit zu entfernen, kann die Replikation von AppDisks auf anderen Hostingeinheiten fehlschlagen. Infolgedessen können Maschinen in der Bereitstellungsgruppe mit AppDisks nicht gestartet werden. [LC6433]

- Nach dem Neustart des Citrix Überwachungsdiensts oder des Citrix Delivery Controllers kann Ereignis-ID 1013 auftreten:

  "Anfängliche Datenbankpflege fehlgeschlagen: System.NullReferenceException: Objekt verweist nicht auf eine Instanz eines Objekts."

  Das Problem tritt beim Beenden des Citrix Überwachungsdiensts auf. [LC6438]

- Der Versuch der Verwendung bestimmter Anwendungen von Drittanbietern (z. B. RayStation) auf einem Citrix Delivery Controller kann unter Anzeige folgender Fehlermeldung fehlschlagen:

  ""The communication object, System.ServiceModel.Channels.ServiceChannel, cannot be used for communication because it is in the Faulted state. [LC6552]

- Der Versuch, einen Delivery Controller in einer Umgebung mit gespiegelter Datenbank mit der Option zum Hinzufügen eines zusätzlichen Controllers über Citrix Studio und dem PowerShell-Befehl „Add-XDController"hinzuzufügen, kann fehlschlagen. [LC6563]

- Das Löschen von MCS-Katalogen auf VMware-VSANs kann fehlschlagen. [LC6691]

- Der Speicherverbrauch des Überwachungsdiensts kann plötzlich rasant ansteigen und dazu führen, das Server nicht mehr reagieren. [LC6705]

- Nach einem Upgrade von Citrix Studio von einer älteren Version oder nach einer neuen Installation von Citrix Studio Version 7.12 kann der Delivery Controller bei Citrix Studio zu einer Schleife mit einem obligatorischen Upgrade führen. [LC6737]

- Wenn Sie VMs mit Version 7.12 von MCS erstellen, wird XenTools nicht installiert, sodass ein ordnungsgemäßes Herunterfahren der VMs nicht möglich ist. [LC6769]
- Nach dem Upgrade des Citrix Delivery Controllers auf Version 7.12 kann das Hinzufügen von Maschinen aus Citrix Provisioning Services (PVS) zu einem Katalog in einer Umgebung mit mehreren Domänen fehlschlagen. Das Problem tritt auf, wenn PVS den Domänennamen nicht zusammen mit dem Gerätenamen zurückgibt. Wenn Citrix Studio den Kontonamen in der lokalen Domäne sucht, wird das Konto nicht gefunden. [#LC6818]
- Berechtigungen zum Veröffentlichen von App-V-Paketen können Administratoren ohne Vollzugriff verweigert werden. Es wird folgende Ausnahme angezeigt:

  "Citrix.Console.Models.Exceptions.PermissionDeniedException: Sie haben nicht die erforderlichen Berechtigungen, um diesen Vorgang auszuführen."[LC6897]
- Der Prozess HighAvailabilityService.exe verbraucht möglicherweise viel Arbeitsspeicher. [LC6918]
- Beim Upgrade einer XenApp-Site kann das Lizenzmodell unerwartet von XenApp in XenDesktop wechseln. [LC6981]
- Der Befehl "Start-Transcript"kann für "Get-XDSite"und andere PowerShell-Verwaltungsbefehle hoher Ebene für XenDesktop bei Verwendung von PowerShell 5 fehlgeschlagen. [LC7006]
- Dieser Fix behebt ein Speicherproblem im Citrix Hostdienst. [LC7516]
- Die Erstellung von Isolationsgruppen durch benutzerdefinierte Administratoren kann unter Anzeige der folgenden Fehlermeldung fehlschlagen:

  Sie haben nicht die erforderlichen Berechtigungen, um diese Anforderung abzuschließen. Weitere Informationen erhalten Sie von Ihrem XenDesktop-Siteadministrator. [LC7563]
- Wenn ein Administrator versucht, einer Bereitstellungsgruppe eine App-V-Anwendung aus einer Isolationsgruppe hinzuzufügen oder eine Isolationsgruppe zu erstellen, wird in Citrix Studio möglicherweise die folgende Fehlermeldung angezeigt:

  Ein unbekannter Fehler ist aufgetreten. [LC7594]
- Die Installation eines VDAs unter Microsoft Windows Server kann fehlschlagen, wenn der Rollendienst "Microsoft Remotedesktop-Sitzungshost"bereits installiert ist. [LC7680]
- Wird versucht, TLSv1.0 auf einem Citrix Delivery Controller zu deaktivieren, kann dies zum Verlust der Kommunikation mit dem VMware vCenter-Hypervisor führen. [LC7686]
- Das Hinzufügen von Maschinen zu einer Bereitstellungsgruppe unter Verwendung des NETBIOS-Namens für die Benutzerzuordnung kann fehlschlagen. Stattdessen wird u. U. der Domänenname angezeigt. Das Problem tritt auf, wenn vom NETBIOS-Namen die falsche URL verwendet wird. [LC7830]

Lizenzierung

- Der Lizenzserver besteht unter Umständen nicht den Payment Card Industry-Konformitätstest für Clickjacking, weil der Headertyp "X-Frame-Options"nicht festgelegt ist. [LC1983]
- Das Hinzufügen von Domänengruppen, deren Name mehr als 32 Zeichen enthält, kann fehlschlagen. [LC1986]
- Enthält der NetBIOS-Domänenname ein kaufmännisches Und (&), kann die Registerkarte "Lizenzierung"in Citrix Studio möglicherweise nicht geöffnet werden und es wird folgende Fehlermeldung angezeigt:

  Citrix Lizenzserver ist nicht verfügbar. [LC2728]

Profilverwaltung

- Versuche von bestimmten Drittanbieteranwendungen, während des An- oder Abmeldens Dateien umzubenennen oder zu verschieben, schlagen möglicherweise fehl. Wenn es beispielsweise die Dateien file0, file1 und file2 im lokalen Profil gibt, schlägt während des Anmeldevorgangs der Versuch fehl file2 in file3, file1 in file2 und file0 in file1 umzubenennen, wenn file2 bereits im Bereich für ausstehende Aktionen oder Benutzerspeicher vorhanden ist. [LC0465]
- Wenn sich Benutzer abmelden, schlägt der Profilverwaltungsdienst (UserProfileManager.exe) gelegentlich fehl. [LC0625]
- Im Bereich "Anmeldedauer"im Zähler des Systemmonitors (Perfmon) werden u. U. Daten für Benutzeranmeldungen aufgezeichnet, die nicht von der Profilverwaltung verwaltet werden. [LC0779]
- Nach einer bestimmten Zeit synchronisiert die Profilverwaltung möglicherweise nicht die Dateien mit dem Benutzerspeicher. [LC1338]
- Nach dem Aktivieren der folgenden Protokollierungsoptionen werden in der Protokolldatei keine Debuginformationen aufgezeichnet:
  - Richtlinie: Active Directory-Aktionen
  - Richtlinie: Richtlinienwerte bei Anmeldung und Abmeldung
  - Richtlinie: Registrierungsunterschiede bei der Abmeldung [LC2003]
- Wenn ein Benutzer die Profilversionsverwaltung aktiviert (Anweisungen siehe https://support.microsoft.com us/kb/2890783), kann die Profilverwaltung aus folgenden Gründen u. U. nicht migriert werden:
  - Das Microsoft-Roamingprofil wird mit der Erweiterung "V4"erstellt.
  - Das Profil der Profilverwaltung wurde nicht migriert und auch nicht mit der Vorlage für Standardbenutzer erstellt. [LC2427]

- Wenn Benutzer sich nach dem Zurücksetzen des Benutzerprofils in Desktop Director zum ersten Mal anmelden, funktioniert die Ordnerumleitung nicht. Die Ordnerumleitung funktioniert bei nachfolgenden Anmeldungen. [LC2602]
- Der Profilverwaltungsdienst (UserProfileManager.exe) wird u. U. unerwartet beendet. [LC2979]
- Nach der Anwendung von Fix LC0625 wird der Profilverwaltungsdienst (UserProfileManager.exe) u. U. unerwartet beendet. [LC3058]
- Unter Windows 8.1 schlagen Versuche, Dateien unter Verwendung von Internet Explorer 11 herunterzuladen, fehl, wenn der erweiterte geschützte Modus aktiviert ist. [LC3464]
- Dateisperren können in der Profilverwaltung während des Abmeldevorgangs mit einer Fehlermeldung ähnlich der Folgenden fehlschlagen:

  "Der Prozess kann nicht auf die Datei zugreifen, weil sie von einem anderen Prozess gesperrt ist."

  Erst wenn die Sperre aufgehoben wird, schlagen Versuche, die von der Profilverwaltung gesperrten Dateien zu löschen, nicht mehr fehl. [LC3532]
- Während das Benutzergerät herunterfährt, wird die Profilverwaltung u. U. unerwartet beendet. [LC3626]
- Die XenApp-Server der Farm reagieren möglicherweise nicht mehr und der Server muss neu gestartet werden. [LC4318]
- Beim Anmeldeversuch an einem XenApp 7.7-Server per RDP reagiert der Server möglicherweise nicht mehr, wenn der Begrüßungsbildschirm offen ist. [LC5169]
- Nach dem Aktualisieren eines VDAs von Version 7.6.1000 oder früher auf Version 7.7 oder höher schlagen Versuche, die Profilverwaltung oder den VDA zu löschen, zu reparieren oder neu zu installieren, möglicherweise fehl. [LC5207]
- Bei der Abmeldung kann es vorkommen, dass Dateien/Ordner auf dem Server von der Profilverwaltung gesperrt werden und Anwendungen nicht mehr gestartet werden können. Lokal gespeicherte Profile können auch nicht gelöscht werden. [LC5266]
- Es kann vorkommen, dass Dateien in Benutzerprofilen von der Profilverwaltung gesperrt werden. Wenn dieser Fall eintritt, erhalten Benutzer beim Versuch eines Verbindungsaufbaus so lange ein temporäres Profil, bis die Sperre für ihr Profil aufgehoben wird. [LC5278]
- Lokal zwischengespeicherte Profile können möglicherweise nicht gelöscht werden, wenn Benutzer sich abmelden. [LC5470]
- Wenn der Lizenzserver offline ist, gehen Dateien, die den Benutzerumleitungsordner auf dem Server verwenden, verloren. [LC5595]
- Die Dateien von Benutzern gehen verloren, wenn die Lizenztestphase ohne Lizenzerneuerung endet. [LC5775]

- Die Profilverwaltung setzt u. U. fälschlicherweise das Flag "NetworkDetection", das darauf hinweist, dass das Netzwerk verloren wurde. Durch diesen Fix wird eine zusätzliche Prüfung eingeführt, die sicherstellt, dass das Netzwerk nicht nur vorübergehend nicht verfügbar ist. [LC5943]
- Gelegentlich hört die Anmeldeseite für Benutzer unter Windows Server 2012 R2 auf zu reagieren. [LC6149]
- Die Migration von Roamingprofilen in die Profilverwaltung kann fehlschlagen. Das Problem tritt auf, wenn einem Profil eine falsche Versionsnummer hinzugefügt wird. [LC6150]
- Die Anwendungssymbole können ausgegraut sein, wenn Sie versuchen, die Symbole aus dem Benutzerprofilspeicher der Profilverwaltung über eine WAN-Verbindung zu kopieren. [LC6152]
- Das Roaming von Dateitypzuordnungen funktioniert in Sitzungen mit aktivierter Profilverwaltung, die unter Microsoft Windows 10 oder Windows Server 2016 ausgeführt werden, möglicherweise nicht. [LC6736]
- Wenn die Richtlinie "Lokalen Cache nach Abmeldung löschen"unter Microsoft Windows 10 oder Windows Server 2016 aktiviert ist, wird die Datei NTUSER.DAT bei der Abmeldung u. U. nicht gelöscht, sodass ein weiteres lokales Profile bei der nächsten Anmeldung erstellt wird. [LC6765]
- Bei Verwendung der Profilverwaltung unter Microsoft Windows Server 2016 unter Einschluss von usrclass.dat funktioniert das Startmenü möglicherweise nicht. [LC6914]
- Beim Öffnen von Dateien in einem Profil, für das Profilstreaming aktiviert ist, wird die Datei nach dem Anmelden möglicherweise leer angezeigt. [LC6996]
- Die Profilverwaltung kann zur Anzeige eines schwarzen Bildschirms führen, wenn versucht wird, eine Windows 10-Sitzung zu starten. Für diesen Fix müssen Sie die Richtlinie "Zu synchronisierende Verzeichnisse"konfigurieren und den Ordner "*AppData\Local\Microsoft\Windows\Caches*" hinzufügen. [LC7596]

Provisioning Services

Probleme mit der Konsole

- Mit diesem Fix sind die Optionen "Schedule the next vDisk update to occur on"und "Apply vDisk updates as soon as they are directed by the server"nicht mehr für Provisioning Services verfügbar. [LA4166]
- Das Erstellen von virtuellen Maschinen mit dem XenDesktop-Setupassistenten schlägt möglicherweise in einer nicht-englischen Microsoft System Center Virtual Machine Manager (SCVMM)-Umgebung fehl. [LC5451]
- Das Erstellen einer ISO-Datei mit dem PowerShell-Skript New-BootDeviceManager schlägt möglicherweise mit der folgenden Fehlermeldung fehl: "ISOFileName must be called with the

name of the new ISO file to create."[LC5559]

- Beim Verwenden von geclustertem Volumespeicher behält der Setupassistent für gestreamte VMs die Volumeauswahl nicht bei und erstellt Zielgeräte u. U. in zufälligen Volumes. [LC5890]
- Versuche, die Provisioning Services Console zu schließen, nachdem sie den XenDesktop-Setupassistenten oder den Setupassistenten für gestreamte VMs ausgeführt haben, können zu einer Ausnahme führen. [LC6048]
- Nach dem Upgrade von PVS-Version 7.6 auf PVS 7.11 können sich Benutzer in anderen Domänen möglicherweise nicht an der Konsole anmelden. [LC6216]
- Serverkommunikationstimeout. In manchen Fällen kann die Anmeldung übermäßig lange dauern (z. B. mehr als 2 Minuten). Dies kann zu Timeouts zwischen PVS-Konsole und SoapServer führen. Das Standardtimeout für solche Verbindungen ist 2 Minuten. Sie können diesen Wert über den Registrierungswert "HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout = <Timeout in Sekunden>"erhöhen. Wenn die Anmeldung länger als ca. 4 Minuten dauert, kommt es außerdem zu Timeouts bei der Microsoft-MMC mit der PVS-Konsole (diese Timeoutmeldungen können geschlossen werden).

  Eine Ursache sind nicht erreichbare Domänen in Active Directory, wo bei jedem Verbindungsversuch mit einer nicht erreichbaren Domäne ein Timeout von 30 Sekunden angewendet wird. So kommen schnell mehrere Minuten zusammen, wenn mehrere Domänen nicht erreichbar sind. Nicht erreichbare Domänen entstehen generell, wenn Active Directory Testdomänen hinzugefügt und später wieder entfernt werden. Eine solche entfernte Domäne wird von Active Directory weiterhin unter den Domänen bzw. Autorisierungsgruppen aufgelistet.

  Nicht erreichbare Domänen können auch entstehen, wenn ein Domänencontroller vorübergehend heruntergefahren und vom Netzwerk getrennt wird. Daher sollten nicht alle nicht erreichbaren Domänen auf die Sperrliste gesetzt werden.

  Die beste Methode herauszufinden, ob es nicht erreichbare Domänen gibt, ist die Prüfung der CDF-Trace auf Fehlermeldungen über nicht erreichbare Domänen oder Serverweiterleitungen für das Modul "PVS_DLL_ADSUPPORT". Wenn Sie einen solchen Fehler finden, vergewissern Sie sich, dass die Domänen nicht mehr verwendet werden, und setzen Sie deren Namen auf die Sperrliste.

  Die Sperrliste ist eine JSON-Datei mit dem Namen "%ProgramData\Citrix\Provisioning Services\blacklist.json". Beispiel:

```
{


"Domains":

[

```



```
 8   "sub.xs.local",
 9
10   "sb.xs.local"
11
12   ]
13
14    }
15
16   <!--NeedCopy-->
```

Wobei die beiden Domänen **sub.xs.local** und **sb.xs.local** aus der Domänen- und Gruppenauflistung ausgenommen werden. Nachdem die Datei aktualisiert wurde, müssen Sie den SoapServer und alle laufenden Konsolen neu starten, um die aktualisierten Werte zu laden. [LC6249]

- Nach dem Konfigurieren der Provisioning Services Console fehlen u. U. die Bezeichnungen in den Eigenschaften des Zielgeräts. [LC6864]

Serverprobleme

- In VMware ESX-Bereitstellungen kann es beim XenDesktop-Setupassistenten zu einer Ausnahme kommen, die verhindert, dass Benutzer Vorlagen und Maschinen richtig einrichten können. [LA2499]
- Zwei PVS-Server können möglicherweise nicht den Replikationsstatus einer vDisk auf dem jeweils anderen Server sehen, sie zeigen jedoch den Status der jeweils eigenen vDisks richtig an. [LC4317]
- Die Citrix PXE- Dienst ignoriert möglicherweise die Einträge in der Datei BOOTPTAB. [#LC4600]
- Bei Verwendung einer BDM-Partition versuchen auf VMware ausgeführte Zielgeräte nicht, sich auf allen Servern in der Liste anzumelden, wenn der oberste Server nicht erreichbar ist. [LC4736]
- Das Erstellen von virtuellen Maschinen mit dem XenDesktop-Setupassistenten schlägt möglicherweise in einer nicht-englischen Microsoft System Center Virtual Machine Manager (SCVMM)-Umgebung fehl. [LC5451]
- Wenn beim Klonen einer Festplatte nicht alle Partitionen geklont werden, schlägt das Klonen der letzten Partitionen möglicherweise fehl. [LC5452]
- Beim Ausführen des Replikationsstatus für zwei PVS-Server von der PVS-Konsole aus wird der Status für beide Server als unvollständig angezeigt. [LC5700]
- Beim Verwenden von geclustertem Volumespeicher behält der Setupassistent für gestreamte VMs die Volumeauswahl nicht bei und erstellt Zielgeräte u. U. in zufälligen Volumes. [LC5890]

- Nach dem Upgrade von PVS-Version 7.6 auf PVS 7.11 können sich Benutzer in anderen Domänen möglicherweise nicht an der Konsole anmelden. [LC6216]
- Serverkommunikationstimeout. In manchen Fällen kann die Anmeldung übermäßig lange dauern (z. B. mehr als 2 Minuten). Dies kann zu Timeouts zwischen PVS-Konsole und SoapServer führen. Das Standardtimeout für solche Verbindungen ist 2 Minuten. Sie können diesen Wert über den Registrierungswert "HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout = <Timeout in Sekunden>"erhöhen. Wenn die Anmeldung länger als ca. 4 Minuten dauert, kommt es außerdem zu Timeouts bei der Microsoft-MMC mit der PVS-Konsole (diese Timeoutmeldungen können geschlossen werden).

  Eine Ursache sind nicht erreichbare Domänen in Active Directory, wo bei jedem Verbindungsversuch mit einer nicht erreichbaren Domäne ein Timeout von 30 Sekunden angewendet wird. So kommen schnell mehrere Minuten zusammen, wenn mehrere Domänen nicht erreichbar sind. Nicht erreichbare Domänen entstehen generell, wenn Active Directory Testdomänen hinzugefügt und später wieder entfernt werden. Eine solche entfernte Domäne wird von Active Directory weiterhin unter den Domänen bzw. Autorisierungsgruppen aufgelistet.

  Nicht erreichbare Domänen können auch entstehen, wenn ein Domänencontroller vorübergehend heruntergefahren und vom Netzwerk getrennt wird. Daher sollten nicht alle nicht erreichbaren Domänen auf die Sperrliste gesetzt werden.

  Die beste Methode herauszufinden, ob es nicht erreichbare Domänen gibt, ist die Prüfung der CDF-Trace auf Fehlermeldungen über nicht erreichbare Domänen oder Serverweiterleitungen für das Modul "PVS_DLL_ADSUPPORT". Wenn Sie einen solchen Fehler finden, vergewissern Sie sich, dass die Domänen nicht mehr verwendet werden, und setzen Sie deren Namen auf die Sperrliste.

  Die Sperrliste ist eine JSON-Datei mit dem Namen "%ProgramData\Citrix\Provisioning Services\blacklist.json". Beispiel:

```
{


"Domains":

[

"sub.xs.local",

"sb.xs.local"

]

 }

<!--NeedCopy-->
```


Wobei die beiden Domänen **sub.xs.local** und **sb.xs.local** aus der Domänen- und Gruppenauflistung ausgenommen werden. Nachdem die Datei aktualisiert wurde, müssen Sie den SoapServer und alle laufenden Konsolen neu starten, um die aktualisierten Werte zu laden. [LC6249]

Probleme bei Zielgeräten

- Das Feature zur automatischen Aktualisierung des Provisioning Services-Zielgeräts generiert folgende Anwendungsfehlermeldung (Ereignis-ID: 0) in der Ereignisanzeige des Zielgeräts, wenn die Aktualisierung nicht verfügbar ist.
  "No update server found. Stopping client service."[LC0450]
- Die Zielgerätesoftware erkennt das AppDisk-Laufwerk nicht und verwendet das AppDisk-Laufwerk für den Schreibcache, was zu Konflikten führen kann. [LC5409]
- Wenn Sie eine vDisk mit "Write Cache on RAM"konfigurieren und die Größe des RAM-Cache auf 4.096 MB oder 4.097 MB festlegen, kann das Starten einer Hyper-V-VM der zweiten Generation bei Zielgeräten zu einer schwerwiegenden Ausnahme mit Anzeige eines Bluescreen führen. [LC6707]

StoreFront

- Wenn der Administrator die Gruppenrichtlinieneinstellung "MaxPasswordAge"ändert, wird der neue Wert im StoreFront-Standarddomänendienst nicht geladen. In StoreFront wird Benutzern dann evtl. eine falsche Anzahl Tage bis zum Kennwortablauf angezeigt.

  Hinweis: Dieser Fehler wurde behoben, es kann jedoch bis zu einer Stunde dauern, bis der neue Wert geladen wird. [DNA-41380]
- In StoreFront 3.5 wird für die Ordnerfarbe in der Kategorienansicht möglicherweise nicht mehr die benutzerdefinierte Farbe verwendet, die in der StoreFront-Verwaltungskonsole definiert wurde. Die Standardfarbe wird wiederhergestellt. [LC5001]
- StoreFront wird beim Verwalten von Citrix Receiver für Web-Sites u. U. unerwartet beendet. Das Problem tritt auf, wenn die style.css für Citrix Receiver für Web angepasst wurde. [LC5589]
- Das Aktivieren des Verbundauthentifizierungsdiensts für StoreFront kann zu Fehlern bei der Anmeldung führen. [LC5708]
- Selbst wenn Citrix Receiver für HTML5 in Citrix StoreFront aktiviert ist, zeigt die StoreFront-Konsole möglicherweise "Nicht verwendet"statt der HTML-Version an. [LC6626]
- Wenn Sie während der Einrichtung von XenDesktop eine konfigurierte Site auswählen, wird möglicherweise ein Standardstore in StoreFront erstellt, der den Standardauthentifizierungs-

dienst verwendet. Wenn Sie diesen Store entfernen, können Benutzer von Citrix Receiver für Windows keine anderen Stores hinzufügen und die folgende Fehlermeldung wird angezeigt:

"Ein Protokollfehler ist bei der Kommunikation mit dem Authentifizierungsdienst aufgetreten." [LC6664]

- Bei der Konfiguration von Self-Service-Kennwortzurücksetzung (SSPR) für einen bestimmten Store in der StoreFront-Verwaltungskonsole gilt die Konfiguration für alle Stores, nicht nur für den spezifischen Store, den Sie ausgewählt haben. [LC6987]
- In Bereitstellungen mit Multisiteaggregation kann der Versuch, die Verbindung für getrennte Sitzungen wiederherzustellen, fehlschlagen. Dies kann zum Erhalt einer zweiten Instanz derselben Ressource führen. [LC7453]
- Wenn eine der Quellen einer aggregierten Anwendung deaktiviert wird, wird die Anwendung für den Endbenutzer möglicherweise unerwartet ausgeblendet. [LC7675]
- Ein Deaktivieren der Option "Konto-Self-Service"in StoreFront wird möglicherweise nicht wirksam, selbst wenn die Option als deaktiviert angezeigt wird. [LC7744]
- Beim Versuch, die freigegebene Authentifizierung für Stores in StoreFront zu entfernen, kann beim Speichern der Änderungen die folgende Fehlermeldung angezeigt werden:

  "Ein Fehler ist beim Speichern der Änderungen aufgetreten."[LC7781]

Universeller Druckserver

Client

- Wenn Sie die Profilverwaltung verwenden, werden Änderungen an Citrix Universeller Druckserver-Druckern (Hinzufügen, Entfernen, Umbenennen), die in einer Sitzung auf einem Server gemacht werden, möglicherweise nicht korrekt in anschließenden Sitzungen auf einem anderen Server widergespiegelt. [LC7645]

Server

- Das Drucken aus Microsoft Internet Explorer mit dem universellen Citrix Druckertreiber kann unter Anzeige der folgenden Fehlermeldung fehlschlagen:

  Internet Explorer konnte das Dokument aufgrund eines internen Fehlers nicht drucken. [LC4735]

- Das Drucken eines Dokuments kann unter Anzeige der folgenden Fehlermeldung fehlschlagen:

  Aufgrund eines Problems mit der Druckereinrichtung kann von Windows nicht gedruckt werden. [LC6825]

- Beim Verwenden bestimmter Drucker wird in Microsoft Editor möglicherweise die Meldung "Handle ist ungültig"angezeigt und der Druck schlägt fehl. Das Problem tritt auf, wenn in der Citrix Richtlinie "Verwendung universeller Druckertreiber"die Einstellung "Nur druckermodellspezifische Treiber verwenden"und in der Citrix Richtlinie "Universellen Druckserver aktivieren"die Einstellung "Aktiviert ohne Fallback auf systemeigenen Windows-Remotedruck" konfiguriert ist. [LC7623]

VDA für Desktopbetriebssystem

Inhaltsumleitung

- Die Erfassung von Images mit DirectShow schlägt fehl und die Anwendung wird unerwartet beendet. [LC6667]

HDX Broadcast

- HDX-Audiogeräte können beim Start einer Sitzung wahllos deaktiviert werden. [LC5281]

Installation, Deinstallation, Upgrade

- Nach einem Upgrade des VDAs von Version 5.6.400 auf Version 7.9 kann das Neustarten des VDAs dazu führen, dass die Spiegelungstreiber der vorherigen Version zurückbleiben. [LC6295]
- Beim Upgrade von VDA-Version 5.6 auf 7.x kann ein falscher Legacy-Videotreiber installiert werden. [LC6363]
- Wenn Sie VMs mit Version 7.12 von MCS erstellen, wird XenTools nicht installiert, sodass ein ordnungsgemäßes Herunterfahren der VMs nicht möglich ist. [LC6769]
- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7555]
- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7587

Tastatur

- Citrix Receiver für Linux unterstützt möglicherweise keine spanischen DNIe-Ausweise. [LC6547]
- Wenn HDX 3D Pro auf einem VDA aktiviert ist, funktionieren die Tastenkombinationen Alt+P und Alt+S möglicherweise nicht. [LC6826]

Drucken

- Wenn Sie versuchen, zwei Exemplare eines Dokuments zu drucken, wird möglicherweise nur eines gedruckt. Das Problem tritt auf, wenn in der Citrix Richtlinie "Verwendung universeller Druckertreiber"die Einstellung "Nur druckermodellspezifische Treiber verwenden"und in der Citrix Richtlinie "Universellen Druckserver aktivieren"die Einstellung "Aktiviert ohne Fallback auf systemeigenen Windows-Remotedruck"konfiguriert ist. [LC6023]
- Der Citrix Druckmanagerdienst (cpsvc.exe) kann aufhören zu reagieren und unerwartet beendet werden, wenn sich neue Benutzer anmelden. [LC6933]
- Nach einem Upgrade des VDAs von Version 7.9 auf Version 7.12 oder höher werden beim Drucken aus Microsoft Internet Explorer mit dem Citrix universellen Druckertreiber die Drucke nicht im ausgewählten Ausgabefach sondern immer in Fach 1 ausgegeben. [LC7463]

Server- /Siteverwaltung

- Änderungen an erweiterten Systemeinstellungen unter "Visuelle Effekte"werden zwar auf die aktuelle Desktopbetriebssystem-VDA-Sitzung angewendet, möglicherweise aber nicht für zukünftige Sitzungen gespeichert. Damit solche Änderungen beibehalten werden, müssen Sie folgenden Registrierungsschlüssel festlegen:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Typ: DWORD;
  Wert: 1 [LC8049]

Sitzung/Verbindung

- Die Richtlinie "Regeln für die Client-USB-Geräteumleitung"wird u. U. nicht angewendet. Das Problem tritt auf, wenn die Anzahl der vom Benutzer eingegebenen Zeichen in der Richtlinie 1002 überschreitet. [LC1144]
- Nach einer Netzwerkunterbrechung schlagen Wiederverbindungsversuche mit einem VDA möglicherweise fehl. Das Problem tritt nach einem Upgrade des VDAs auf Version 7.8 auf. [LC5040]
- Wenn Framehawk aktiviert ist, wird bei Verwendung der Mausrolltaste in XenDesktop-7.8-VDA-Sitzungen möglicherweise keine Aktion ausgeführt. Der entsprechende VDA-seitige Fix ist in XenDesktop 7.9 verfügbar. [LC5302]
- Bei VDAs kann es zu einer schwerwiegenden Ausnahme vom Typ 0x50 (Page_Fault_In_NonPaged_Area) beim Citrix Anzeigetreiber vdodk.sys kommen. [LC5074]

- Wenn AppDisk einer virtuellen Maschine mit einer Windows-Version in einer anderen Sprache als Englisch angefügt ist, wird u. U. zu einem sofortigen oder späteren Neustart aufgefordert. Die Aufforderung verschwindet durch diesen Fix. [LC5403]
- Nach der Wiederverbindung einer getrennten Sitzung mit mehreren Monitoren erscheint der Anzeigebildschirm schwarz und benutzerdefinierte Einstellungen werden auf die Standardwerte zurückgesetzt. [LC5556]
- Nach dem Upgrade eines VDAs von Version 7.6.300 auf Version 7.8 funktioniert die Zwischenablagen-Synchronisierung möglicherweise nicht mehr. [LC5699]
- Wenn Framehawk aktiviert ist, wird bei Verwendung der Mausrolltaste in XenDesktop 7.9-VDA-Sitzungen möglicherweise keine Aktion ausgeführt. [LC5779]
- Ein für den Verbundauthentifizierungsdienst konfigurierter VDA nimmt möglicherweise keine Verbindungen mehr an und bleibt beim Begrüßungsbildschirm hängen, bis er neu gestartet wird. [LC5978]
- Citrix Receiver kann beim Starten von Anwendungen in der Phase "Connection Established. Negotiate Capabilities"hängen. [LC6021]
- Änderungen an erweiterten Systemeinstellungen unter "Visuelle Effekte"werden zwar auf die aktuelle VDA-Sitzung angewendet, möglicherweise aber nicht für zukünftige Sitzungen gespeichert. Damit solche Änderungen beibehalten werden, müssen Sie folgenden Registrierungsschlüssel festlegen:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Type: DWORD;
  Value: 0 [LC6163]
- Versuche, eine Remote-PC-Sitzung auf einem touchfähigen Gerät zu trennen, können zu einem schwarzen Bildschirm führen, bei dem keine Wiederherstellung möglich ist. [LC6384]
- Citrix Receiver für Linux unterstützt möglicherweise keine spanischen DNIe-Ausweise. [LC6547]
- Beim Sperren einer Remote-PC-Sitzung mit installiertem SecureDoc unter Windows 10 wird der Sperrbildschirm bis zu zwei Minuten lang angezeigt. Während dieser Zeit ist keine Interaktion mit der Sitzung möglich. [LC6668]
- Wenn Sie die Verbindung mit einer Citrix Receiver für Mac-Sitzung während der Wiedergabe mehrmals trennen und wiederherstellen, funktioniert das Audio möglicherweise nicht. [LC6678]
- Ein Wechselclientlaufwerk wird möglicherweise vom WFAPI SDK auf einem Desktopbetriebssystem-VDA nicht zurückgegeben. [LC6877]

- Bei Verwendung des Legacygrafikmodus auf einem Windows 7-VDA für XenDesktop 7.13 wird möglicherweise ein grauer Bildschirm angezeigt. [LC7477]
- Beim Wechseln von Sitzungen zwischen mehreren Monitoren im Vollbildmodus mit aktiviertem Legacygrafikmodus und ohne dass Desktop Viewer konfiguriert ist, wird die Sitzung u. U. nur auf einem Monitor ausgeführt. [LC7907]

Systemausnahmen

- Es kommt auf Serverbetriebssystem-VDAs möglicherweise zu einer schwerwiegenden Ausnahme mit Bluescreen bei TDICA.sys. [LC6898]
- Auf Servern kann es zu einem schwerwiegenden Fehler mit vdtw30.dll kommen, ein Bluescreen wird angezeigt (Stoppcode 0xc0000006). [LC7608]
- Auf VDAs kann es zu einer schwerwiegenden Ausnahme bei tdica.sys mit einem Bluescreen und Bugcheckcode kommen. [LC7632]
- Mit diesem Fix wird ein Speicherproblem mit der Datei wdica.sys behoben, durch das Server ggf. unerwartet beendet wurden. [LC7666]

Smartcards

- Beim Wechsel zwischen Benutzersitzungen und Microsoft Remotedesktop-Sitzungen können sitzungsinterne, smartcardfähige Anwendungen wie Microsoft Outlook und Microsoft Word möglicherweise keine Smartcards verwenden. Es werden dann diverse Fehlermeldungen angezeigt. Außerdem wird beim Testen der sitzungsinternen Unterstützung von Smartcards mit "CertUtil /scinfo"in einem Befehlsfenster möglicherweise folgende Fehlermeldung angezeigt:

  Die Microsoft Smartcard-Ressourcenverwaltung wird nicht ausgeführt. [LC5839]
- Smartcard-Passthrough kann zeitweilig fehlschlagen. [LC6147]

Benutzererfahrung

- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC5370]
- Bei Verwendung des Legacygrafikmodus auf einem Windows 7-VDA der Version XenDesktop 7.11 wird nur die obere, linke Bildschirmecke angezeigt. [LC6532]
- Beim Kopieren und Einfügen zwischen zwei Microsoft Excel 2010-Arbeitsblättern auf einem VDA der Version 7.9 kann das Excel-Fenster aufhören zu reagieren. [LC7481]

Benutzeroberfläche

- Beim Abmelden von einer Seamlesssitzung mit nicht gespeicherten Daten über das Connection Center wird ein schwarzes Fenster angezeigt.

  Die darin enthaltene Meldung weist darauf hin, dass Programme noch geschlossen werden müssen, und es werden die Optionen "Abmelden erzwingen"und "Abbrechen"angeboten. Die Option "Abbrechen"funktioniert nicht.

  Nach der Installation dieses Fixes funktioniert die Option "Abbrechen"einwandfrei. [LC6075]

- Wenn die Richtlinie "Automatische Anzeige der Tastatur"aktiviert und die Richtlinie "Touchoptimierten Desktop starten"auf "Nicht zugelassen"festgelegt ist, wird beim Starten eines veröffentlichten Desktops auf einem iPad der Dokumentviewer im Zoomverhältnis 80 % angezeigt. Wenn Sie bestimmte Anwendungen auf dem Desktop schließen, kann der Dokumentviewer mit 100 % angezeigt werden. [LC6460]
- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC7557]

VDA für Serverbetriebssystem

Inhaltsumleitung

- Die Erfassung von Images mit DirectShow schlägt fehl und die Anwendung wird unerwartet beendet. [LC6667]

Installation, Deinstallation, Upgrade

- Nach dem Upgrade von VDA 7.11 für Desktopbetriebssysteme auf VDA 7.12 für Desktopbetriebssysteme wird beim Starten bestimmter Anwendungen möglicherweise folgende Fehlermeldung angezeigt:

  "wfapi.dll is missing"[LC6874]

- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7555]
- Nach der Installation von Version 7.12 oder 7.13 des VDA unter Microsoft Windows einer anderen Sprachversion als Englisch werden bestimmte WMI-Klassen möglicherweise umbenannt. [LC7587]

Drucken

- Bei dem Versuch, einen Netzwerkdrucker mit dem Befehl "CreateClientPrinter"zuzuordnen, wird Citrix Print Manager unerwartet beendet. [LC4685]
- Wenn Sie versuchen, zwei Exemplare eines Dokuments zu drucken, wird möglicherweise nur eines gedruckt. Das Problem tritt auf, wenn in der Citrix Richtlinie "Verwendung universeller Druckertreiber"die Einstellung "Nur druckermodellspezifische Treiber verwenden"und in der Citrix Richtlinie "Universellen Druckserver aktivieren"die Einstellung "Aktiviert ohne Fallback auf systemeigenen Windows-Remotedruck"konfiguriert ist. [LC6023]
- Der Citrix Druckmanagerdienst (cpsvc.exe) kann aufhören zu reagieren und unerwartet beendet werden, wenn sich neue Benutzer anmelden. [LC6933]
- Nach einem Upgrade des VDAs von Version 7.9 auf Version 7.12 oder höher werden beim Drucken aus Microsoft Internet Explorer mit dem Citrix universellen Druckertreiber die Drucke nicht im ausgewählten Ausgabefach sondern immer in Fach 1 ausgegeben. [LC7463]

Server- /Siteverwaltung

- Wenn Benutzer zwischen Sitzungen wechseln, die in einem Netzwerk in verschiedenen Subnetzen sind, enthält die Druckerliste Drucker beider Subnetze statt der Drucker des Subnetzes, bei dem Benutzer zurzeit angemeldet sind. [LC2308]
- Die folgende Fehlermeldung wird Benutzern einer untergeordneten Domäne möglicherweise beim Starten einer Anwendung über das Webinterface angezeigt:

  Sie haben keine Zugriffsrechte auf diese veröffentlichte Anwendung. [LC7566]
- Änderungen an erweiterten Systemeinstellungen unter "Visuelle Effekte"werden zwar auf die aktuelle Desktopbetriebssystem-VDA-Sitzung angewendet, möglicherweise aber nicht für zukünftige Sitzungen gespeichert. Damit solche Änderungen beibehalten werden, müssen Sie folgenden Registrierungsschlüssel festlegen:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
  Name: EnableVisualEffect;
  Typ: DWORD;
  Wert: 1 [LC8049]

Sitzung/Verbindung

- Bei Systemen mit Fix LC2702 (im Hotfix Rollup Pack 6 enthalten) werden Anwendungen u. U. nicht auf zugeordneten Clientlaufwerken gespeichert und stattdessen werden beschädigte Dateien generiert. [LC3976]

- Das Starten eines Prozesses mit WinDbg.exe schlägt möglicherweise fehl, wenn Streaming Profiler oder das Offline-Plug-In installiert sind. Dieses Problem tritt auf, weil RadeAPHook einen Hook für die Einstellung für HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*processname*> und HKEY_LOCAL_MACHINE\SOFTWARE\W NT\CurrentVersion\Image File Execution Options\<*processname*> aufruft.

  Zum Implementieren dieses Fixes erstellen Sie folgenden Registrierungsschlüssel:

- *32-Bit Windows:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook;
  Name: EnableReadImageFileExecOptionsExclusionList;
  Typ: Reg_SZ;
  Wert: <*Durch Kommas getrennte Liste (ohne Leerstellen) der ausführbaren Dateien, die vom Hooking in Bezug auf die Einstellung ''Image File Execution Options''ausgenommen werden. Beispiel: windbg.exe,anwendung_1.exe.*>

- *64-Bit-Windows-Version für 32-Bit-Anwendungen:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
  Name: EnableReadImageFileExecOptionsExclusionList
  Typ: Reg_SZ
  Wert: <*Durch Kommas getrennte Liste (ohne Leerstellen) der ausführbaren Dateien, die vom Hooking in Bezug auf die Einstellung ''Image File Execution Options''ausgenommen werden. Beispiel: windbg.exe,anwendung_1.exe.*>

  *[LC4750]

- Beim Starten einer neuen Sitzung kann der Versuch des Citrix Audioumleitungsdiensts, eine Verbindung mit einer virtuellen Kanalsitzung herzustellen, die ungültige Informationen enthält, fehlschlagen. [LC5024]

- Wenn Framehawk aktiviert ist, wird bei Verwendung der Mausrolltaste in XenDesktop-7.8-VDA-Sitzungen möglicherweise keine Aktion ausgeführt. Der entsprechende VDA-seitige Fix ist in XenDesktop 7.9 verfügbar. [LC5302]

- Nach dem Upgrade eines VDAs von Version 7.6.300 auf Version 7.8 funktioniert die Zwischenablagen-Synchronisierung möglicherweise nicht mehr. [LC5699]

- Wenn Framehawk aktiviert ist, wird bei Verwendung der Mausrolltaste in XenDesktop 7.9-VDA-Sitzungen möglicherweise keine Aktion ausgeführt. [LC5779]

- Ein für den Verbundauthentifizierungsdienst konfigurierter VDA nimmt möglicherweise keine Verbindungen mehr an und bleibt beim Begrüßungsbildschirm hängen, bis er neu gestartet wird. [LC5978]

- Änderungen an erweiterten Systemeinstellungen unter "Visuelle Effekte"werden zwar auf die aktuelle VDA-Sitzung angewendet, möglicherweise aber nicht für zukünftige Sitzungen gespe-

ichert. Damit solche Änderungen beibehalten werden, müssen Sie folgenden Registrierungsschlüssel festlegen:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix;
Name: EnableVisualEffect;
Type: DWORD;
Value: 0 [LC6163]

- Die folgende Warnmeldung wird u. U. beim Start von XenApp 7.6 Long Term Service Release Cumulative Update 2 für VDA für Serverbetriebssysteme oder bei Vorversionen im Systemereignisprotokoll angezeigt:

  "An attempt to connect to the SemsService has failed with error code 0x2."[LC6311]

- Wenn eine Remotedesktopsitzung eine Konsolensitzung auf einem VDA für Serverbetriebssysteme übernimmt, wird möglicherweise eine nicht betriebsbereite XenApp-Sitzung erstellt. [LC6617]

- Wiederverbindungsversuche mit einer Sitzung schlagen manchmal fehl und führen dazu, dass die VDAs für Serverbetriebssysteme in den Initialisierungszustand versetzt werden. Das Problem tritt auf, wenn der VDA bei einem Delivery Controller erneut registriert wird. [LC6647]

- Beim Sperren einer Remote-PC-Sitzung mit installiertem SecureDoc unter Windows 10 wird der Sperrbildschirm bis zu zwei Minuten lang angezeigt. Während dieser Zeit ist keine Interaktion mit der Sitzung möglich. [LC6668]

- Wenn Sie die Verbindung mit einer Citrix Receiver für Mac-Sitzung während der Wiedergabe mehrmals trennen und wiederherstellen, funktioniert das Audio möglicherweise nicht. [LC6678]

- Wenn Sie eine veröffentlichte Anwendung auf Microsoft Windows Server 2016 starten, wird möglicherweise einige Sekunden lang ein schwarzer Bildschirm angezeigt, bevor die Anwendung sichtbar wird. [LC7947]

Smartcards

- Beim Wechsel zwischen Benutzersitzungen und Microsoft Remotedesktop-Sitzungen können sitzungsinterne, smartcardfähige Anwendungen wie Microsoft Outlook und Microsoft Word möglicherweise keine Smartcards verwenden. Es werden dann diverse Fehlermeldungen angezeigt. Außerdem wird beim Testen der sitzungsinternen Unterstützung von Smartcards mit "CertUtil /scinfo"in einem Befehlsfenster möglicherweise folgende Fehlermeldung angezeigt:

  Die Microsoft Smartcard-Ressourcenverwaltung wird nicht ausgeführt. [LC5839]

Systemausnahmen

- Es kommt auf Serverbetriebssystem-VDAs möglicherweise zu einer schwerwiegenden Ausnahme mit Bluescreen bei TDICA.sys. [LC6898]
- Auf Servern kann es zu einem schwerwiegenden Fehler mit vdtw30.dll kommen, ein Bluescreen wird angezeigt (Stoppcode 0xc0000006). [LC7608]
- Auf VDAs kann es zu einer schwerwiegenden Ausnahme bei tdica.sys mit einem Bluescreen und Bugcheckcode kommen. [LC7632]
- Mit diesem Fix wird ein Speicherproblem mit der Datei wdica.sys behoben, durch das Server ggf. unerwartet beendet wurden. [LC7666]

Benutzererfahrung

- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC5370]
- Beim Kopieren und Einfügen zwischen zwei Microsoft Excel 2010-Arbeitsblättern auf einem VDA der Version 7.9 kann das Excel-Fenster aufhören zu reagieren. [LC7481]

Benutzeroberfläche

- Beim Abmelden von einer Seamlesssitzung mit nicht gespeicherten Daten über das Connection Center wird ein schwarzes Fenster angezeigt.

  Die darin enthaltene Meldung weist darauf hin, dass Programme noch geschlossen werden müssen, und es werden die Optionen "Abmelden erzwingen"und "Abbrechen"angeboten. Die Option "Abbrechen"funktioniert nicht.

  Nach der Installation dieses Fixes funktioniert die Option "Abbrechen"einwandfrei. [LC6075]
- Wenn die Richtlinie "Automatische Anzeige der Tastatur"aktiviert und die Richtlinie "Touchoptimierten Desktop starten"auf "Nicht zugelassen"festgelegt ist, wird beim Starten eines veröffentlichten Desktops auf einem iPad der Dokumentviewer im Zoomverhältnis 80 % angezeigt. Wenn Sie bestimmte Anwendungen auf dem Desktop schließen, kann der Dokumentviewer mit 100 % angezeigt werden. [LC6460]
- Wenn Sie eine Tabellenkalkulation mit mehreren Arbeitsmappen in Excel 2010 öffnen, wird auf der Taskleiste nur die aktuelle Arbeitsmappe angezeigt. [LC7557]

Virtual Desktop-Komponenten –Sonstiges

- Der Sitzungstyp einer auf einer virtuellen Maschine gehosteten Anwendungssitzung kann unerwartet von "Anwendung"in "Desktop"wechseln. Der Versuch einer erneuten Verbindung mit der Anwendung schlägt dann fehl. [LC5461]
- Beim Starten eines App-V-Pakets unter Verwendung der in XenDesktop integrierten Microsoft App-V 5.0-Infrastruktur wird das App-V-Paket möglicherweise nicht synchronisiert und die folgenden Ausnahme tritt auf:

  <Anwendungsname> kann nicht gestartet werden. [LC5483]
- Beim Laden einer App-V-Anwendung über das Netzwerk wird möglicherweise folgende Fehlermeldung angezeigt:

  Index ist außerhalb des gültigen Bereichs. Muss eine positive Zahl kleiner als die Größe der Sammlung sein. [LC5828]
- Nach dem XenApp-Upgrade von Version 7.7 auf 7.8 kann der Start von App-V-Anwendungen fehlschlagen. Das Problem tritt auf, wenn der boolesche targetIn-Wert auf 0 anstelle von 1 festgelegt ist. Die manuelle Einstellung des Werts hat möglicherweise keine Wirkung. Beim Aktualisieren der Anwendung wird er möglicherweise wiederhergestellt. [LC5861]
- Beim Hinzufügen eines App-V-Pakets mit mehreren Anwendungen in Citrix Studio und Veröffentlichen aller Anwendungen in dem Paket wird möglicherweise nur die erste Anwendung in Benutzersitzungen gestartet. [LC5863]
- Die App-V-Anwendung kann nur von einem einzelnen Benutzer gestartet werden. Der Versuch eines weiteren Benutzers, dieselbe Anwendung auf demselben Server zu starten, kann fehlschlagen. [LC6414]
- App-V-sequenzierte Anwendungen sind möglicherweise nicht im App-V-Paket enthalten, selbst wenn sie von dem Paket referenziert werden (InTarget=False.) Infolgedessen wird der Anwendungsstart nicht auf abhängige Verbindungsgruppen angewendet, die für die einwandfreie Funktion der Anwendung erforderlich sind. [LC6534]
- Nach dem Upgrade von XenApp/XenDesktop 7.11 auf Version 7.12 werden vorhandene Zeitpläne für Bereitstellungsgruppenneustarts nicht angewendet. [LC6766]
- Der Versuch, eine App-V-Anwendung von einem zugeordneten Laufwerk aus zu starten, kann fehlschlagen. [LC6961]
- Die Veröffentlichung von App-V-Anwendungen kann fehlschlagen.

  [LC7421]
- Wenn Microsoft Message Queuing auf dem VDA-Masterimage installiert ist, kann das Erstellen von Maschinenkatalogen unter Anzeige der folgenden Fehlermeldung in Citrix Studio fehlschlagen:

Imagevorbereitung wurde nicht abgeschlossen. Status ‘NotSet”[LC7528]

- Der Versuch, App-V-Anwendungen im Einzelverwaltungsmodus zu starten, kann fehlschlagen. Das Problem tritt auf, wenn der Anwendungsname Sonderzeichen enthält. [LC7897]

Weitere behobene Probleme

- Gruppenrichtlinien fehlen in Citrix Studio, wenn die Richtlinie UPM - Software\Microsoft\Speech_OneCore unter Profilverwaltung > Registrierung > Standardausschlüsse vor dem Upgrade des Delivery Controllers von Version 7.11 auf 7.14, 7.12 auf 7.14 oder 7.13 auf 7.14 konfiguriert wurde. [UPM-538]
- Die Installation von bzw. das Upgrade auf Version 7.14 der Sitzungsaufzeichnung mit dem XenApp- und XenDesktop-Produktinstallationsprogramm unter Windows Server 2008 schlägt unter Meldung eines Fehlers bei Microsoft Message Queuing fehl. [SRT-1782]
- Nach dem Upgrade der Controller wird der Energiezustand eines VDAS möglicherweise mit “Unbekannt”angeben. [DNA-37756]

Bekannte Probleme

July 11, 2022

Bekannte Probleme, die in den Abschnitten 7.15-Basiskomponenten,CU1, CU2, CU3, CU4, CU5, CU6, CU7 und CU8 dieses Artikels beschrieben werden, sind auch in CU9 vorhanden, sofern sie nicht in der Liste der behobenen Problem enthalten sind.

Bekannte Probleme in Cumulative Update 9

Es gibt keine neuen bekannten Probleme in CU9.

Bekannte Probleme in Cumulative Update 8

- Wenn Sie diese Version des VDAs verwenden, schlagen die von der Organisationseinheit auf eine Maschine angewendeten Citrix-Richtlinien manchmal fehl. [CVADHELP-19826]
- Wenn die sicheren XML-Schlüssel nicht in der Registrierung erstellt werden, fehlt möglicherweise die lokale Hostcachedatenbank oder ist beschädigt. Informationen zum Neuerstellen der lokalen Hostcachedatenbanken finden Sie unter CTX228758. [LCM-9660]

- Wenn StoreFront auf demselben Server wie der Delivery Controller installiert ist, schlagen Versuche, Storefront nach dem Upgrade des Delivery Controllers zu aktualisieren, fehl. Das Upgrade von StoreFront kann jedoch einwandfrei vor dem des Delivery Controllers ausgeführt werden.

  Wenn Sie StoreFront nach dem Delivery Controller aktualisieren müssen, beenden Sie als Workaround den Citrix Telemetriedienst, bevor Sie das StoreFront-Upgrade ausführen. [LCM-9706]

- Versuche, in Citrix Studio eine Hostingverbindung zu Azure herzustellen, schlagen möglicherweise mit einer Ausnahme fehl. Das Problem tritt aufgrund der von Microsoft in Azure vorgenommenen Änderungen auf. Ein privater Fix ist unter CTX457802 verfügbar. [CVADHELP-18741]

Bekannte Probleme in Cumulative Update 7

- Die Aktualisierung der CEIP-Option für die Lizenzierung mit dem Cmdlet `Set-LicCEIPOption` schlägt mit einem `CommunicationError` fehl. Als Workaround kann die CEIP-Option über Citrix Licensing Manager aktiviert werden. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX220679.

Bekannte Probleme in Cumulative Update 6

- Die Citrix Workspace-App 1912 und höher unterstützt HDX-Flash-Umleitung (Teil von XenApp und XenDesktop 7.15 LTSR CU6) nicht. HDX-Flash-Umleitung ist nur bis einschließlich Citrix Workspace-App 1911 verfügbar. Sie können auch Citrix Receiver 4.9 LTSR mit 7.15 LTSR CU6 verwenden. [LCM-8140]

- Das CU6-Relase enthält eine neuere Version der Self-Service-Kennwortzurücksetzung. Die neuere Version erkennt die Sicherheitskonfigurationen des zentralen Speichers. Wenn Sie den zentralen Speicher oder den Dienst unter Windows Server 2008 R2 erstellen, wird eine Warnung angezeigt. Das Problem tritt auf, weil Windows Server 2008 R2 keine SMB-Verschlüsselung unterstützt und daher die Sicherheitsprüfung nicht besteht. Durch das Problem werden weitere Aktionen nicht verhindert. Erstellen Sie als Workaround den zentralen Speicher und den Dienst unter Windows Server 2012 oder höher, sodass SMB-Verschlüsselung unterstützt wird. [LCM-8179]

- In Citrix Director werden Richtlinieninformationen möglicherweise nicht aufgelistet, wenn Sie mit einem VDA der Version 7.15 LTSR CU6 verknüpfte Sitzungsdetails anzeigen. Das Problem tritt bei Citrix Director-Versionen auf, die älter als die VDA-Version 7.15 LTSR CU6 sind. Verwenden Sie als Workaround Citrix Director Version 7.15 LTSR CU6. Alternativ können Sie die folgenden Registrierungseinträge auf dem VDA ändern und diesen dann neu starten.

- Registrierungspfad: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

  Name: SaveRsopToFile

  Typ: REG_DWORD

  Wert: 1
- Registrierungspfad: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

  Name: SaveRsopToMemory

  Typ: REG_DWORD

  Wert: 0
- Registrierungspfad: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy

  Name: SaveRsopToRegistry

  Typ: REG_DWORD

  Wert: 0

[LCM-8201]

Bekannte Probleme in Cumulative Update 5

- Beim Upgrade eines Windows 7-VDA von 7.6 LTSR CU8 auf diesen Release kann es zu einer schwerwiegenden Ausnahme mit Bluescreen kommen. Es gibt keinen Workaround.

  Führen Sie einen der folgenden Workarounds aus, wenn Sie einen Windows 7-VDA von 7.6 LTSR CU8 auf diese Version aktualisieren:

  - Deinstallieren Sie 7.6 LTSR CU8 und installieren Sie 7.15 LTSR CU5.
  - Deaktivieren Sie manuell den Citrix WDDM-Treiber auf Windows 7-Maschinen und führen Sie dann das Upgrade auf diese Version aus. Zum Deaktivieren des Citrix WDDM-Treibers gehen Sie folgendermaßen vor:
    * Öffnen Sie `Device Manager`.
    * Klicken Sie auf `Display adapters` und erweitern Sie die Auswahl.
    * Klicken Sie mit der rechten Maustaste auf `Citrix Display Driver (Citrix Systems - WDDM)` und wählen Sie `Disable`. [LCM-6798]
- Auf VDAs mit Windows 7 oder Windows Server 2008 R2 kann ein VC++-Fehler auftreten, wenn Sie eine App-V Anwendung starten. Das Problem tritt auf, weil der App-V Client eine bestimmte Version von VC++ 2013 benötigt.

  Wenden Sie als Workaround den Microsoft-Hotfix https://support.microsoft.com/en-in/help/4014009/march-2017-servicing-release-for-microsoft-desktop-optimization-pack an. Alternativ können Sie zuerst den App-V Client installieren und dann das CU5-Update des VDA. [LCM-6809]

- Citrix Scout führt auf Delivery Controllern mit Windows 2008 R2 möglicherweise keine Systemintegritätsprüfungen aus. Es wird dann gemeldet, dass die Prüfung fehlgeschlagen ist. Das Problem tritt auf, wenn der Delivery Controller keine Internetverbindung hat. Laden Sie als Workaround die Prüfskripts herunter und führen Sie sie manuell aus. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX263240. [LCM-6837]

Bekannte Probleme in Cumulative Update 4

- Benutzerdefinierte Adminskripts des Citrix XenDesktop Admin-Moduls, die auf PowerShell 2.0 abzielen, schlagen möglicherweise fehl. Das Problem tritt auf, weil das Modul PowerShell 2.0 nicht mehr unterstützt.
- Unter der spanischen Version von Microsoft Windows schlägt die Komponenteninitialisierung möglicherweise fehl. Das Problem tritt auf, wenn die Sitetests zur Vorbereitung beim Upgrade des Delivery Controllers von einer beliebigen CU-Version der Version 7.6 auf Version 7.15 CU4 ausgeführt werden.
- Citrix Director zeigt möglicherweise nicht alle Datensätze in den Tabellen "Trends"an. Director zeigt eine begrenzte Anzahl von Datensätzen an, gefolgt von einem zusätzlichen leeren Bereich. Sie können jedoch nach unten scrollen, um die restlichen Datensätze zu finden. [LCM-5841]

Bekannte Probleme in Cumulative Update 3

- Eine Liste der Citrix bekannten Probleme mit dem Windows-Update vom 10. Oktober 2018 (v1809) finden Sie im Knowledge Center-Artikel CTX234973.
- In einer AWS-Umgebung kann ein Server-VDA-Rollback auf ein Image bzw. einen Snapshot der Version XenApp und XenDesktop 7.15 LTSR CU2 fehlschlagen. Verlängern Sie als Workaround das Rollbacktimeout mit dem folgenden PowerShell-Cmdlet auf 30 Minuten:

  Set-ProvServiceConfigurationData –Name ImageManagemntPrep_preparationTimeout –Value 30 [LCM-4364]
- Nach dem Upgrade auf XenApp und XenDesktop 7.15 LTSR CU3 kann ein Siteupgrade fehlschlagen, wenn der Lizenzserver der Site nicht auf die die im Rahmen von CU3 veröffentlichte Version aktualisiert wird. Während des Upgrades werden keine Benachrichtigungen angezeigt. [LCM-5467]
- Nach dem Abschluss des XenDesktop-Assistenten ist der Maschinenkatalog in Studio leer und die Streaming-IP-Adresse wird fälschlicherweise statt der Management-IP-Adresse angezeigt. Legen Sie den folgenden Registrierungsschlüssel fest, damit die Management-IP-Adresse verwendet wird:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices
Name: UseManagementIpInCatalog
Typ: DWORD
Wert: 1

[LD0125]

Bekannte Probleme in Cumulative Update 2

- Auf einem VDA mit Windows 2016 können Benutzer, die sich mit Smartcards anmelden, möglicherweise nicht alle verfügbaren Benutzer bei der Anmeldung sehen. Das Problem basiert auf der Standardgröße des Anmeldefensters (600 x 520). Weitere Informationen und ein Workaround finden Sie im Knowledge Center-Artikel CTX204070. [LCM-3951]
- Eine Liste bekannter Probleme mit Windows 10 Redstone 4 (Insider Preview Builds) finden Sie im Knowledge Center-Artikel CTX231942.
- Nach einem Upgrade von Citrix Studio auf Version 7.15 CU 2 sind die Richtlinien möglicherweise nicht lokalisiert. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX234711. [LC9613]
- 7.15 LTSR CU2-Sitzungen werden möglicherweise als schwarzer Bildschirm gestartet. Das Problem tritt bei Sitzungen auf, die auf XenApp und XenDesktop 7.15 LTSR CU2 und 7.17 VDAs ausgeführt werden, wenn die Profilverwaltung aktiviert ist. Weitere Informationen und ein Workaround finden Sie im Knowledge Center-Artikel CTX235100. [LC9648]

Bekannte Probleme in Cumulative Update 1

- Konfigurierbare Registrierungsschlüssel wie "picadm" und "MultiStreamIca" unter HKEY_LOCAL_MACHINE werden beim Installieren von Cumulative Updates möglicherweise gelöscht oder durch den Standardwert überschrieben. [CVADHELP-16481]
- Die StoreFront-Verwaltungskonsole wird nach einem Upgrade von StoreFront 3.12 (XenApp und XenDesktop 7.15 LTSR) auf StoreFront 3.12.1000 (XenApp und XenDesktop 7.15 LTSR CU1) oder nach der Installation von StoreFront 3.12.1000 nicht geöffnet. Auf der StoreFront-Verwaltungskonsole wird folgender Fehler angezeigt: "MMC could not create the snap-in. The snap-in might not have been installed correctly."Führen Sie als Workaround die in CTX233206 beschriebenen Schritte aus. [LC8935]
- Wenn Sie einen Treiber installieren, der mit einem SHA-256-Zertifikat auf einer Windows 7- oder Windows Server 2008 R2-Maschine signiert ist, wird möglicherweise eine Microsoft WHQL-Meldung (Windows Hardware Quality Labs) angezeigt. Installieren Sie die folgenden Microsoft-Hotfixes auf der Maschine, um das Problem zu beheben:

  - Windows 7 (ein Hotfix): Microsoft-Hotfix
  - Windows Server 2008 R2 (zwei Hotfixes): Hotfix 1 und Hotfix 2 [LCM-2836]

- Wenn der Citrix Telemetriedienst deaktiviert oder angehalten wurde und Sie XenApp und XenDesktop 7.15 LTSR mit einem Metainstaller auf Cumulative Update 1 (CU1) aktualisieren, wird möglicherweise die folgende Warnmeldung angezeigt:
  "Der Citrix Dienst für die Registrierung in Call Home kann nicht starten. Weitere Informationen finden Sie unter CTX218094."[LCM-3642]
- Die Profilverwaltung kann zur Anzeige eines schwarzen Bildschirms führen, wenn versucht wird, eine Windows 10-Sitzung zu starten. Für diesen Fix müssen Sie die Richtlinie "Zu synchronisierende Verzeichnisse"konfigurieren und den Ordner "*AppData\Local\Microsoft\Windows\Caches*" hinzufügen. Weitere Informationen und einen Workaround finden Sie im Knowledge Center-Artikel CTX234144. [LC9030]

Bekannte Probleme in 7.15 LTSR (Erstrelease)

Bei Version 7.15 LTSR von XenApp und XenDesktop gibt es folgende Probleme:

VDA

- Wenn die SAS-Benachrichtigung* aktiviert ist, beobachten Benutzer mit mehreren Monitoren, die eine Verbindung zu einer vorhandenen Sitzung in der Konsole herstellen, dass das Monitorlayout nicht korrekt wiederhergestellt wird. Wenn beispielsweise rechts Monitor 1 ist, der als Hauptmonitor ausgewählt wurde, und links Monitor 2, beobachten Benutzer, dass die Positionen beim Wiederverbinden ausgetauscht sind. Dieses Problem betrifft nur RemotePC-Benutzer mit einem physischen Desktop. Dies ist auf eine Inkompatibilität zwischen zwei Features zurückzuführen. [CVADHELP-14249]

  * SAS-Benachrichtigung ist die Funktion, die einem Konsolenbenutzer in RemotePC ankündigt, dass ein anderer Benutzer versucht, eine Verbindung herzustellen.

App-V

- Wenn Sie in Studio eine oder mehrere App-V-Anwendungen aus dem Knoten "Anwendungen" oder einer Bereitstellungsgruppe löschen, wird ein unbekannter Fehler gemeldet. Sie können diese Meldung ignorieren. Die Anwendungen werden einwandfrei gelöscht. [DNA-29702]
- App-V-Anwendungen können nicht aus einer Bereitstellungsgruppe entfernt werden, wenn ein untergeordneter Prozess für eine Anwendung gestartet wurde beim Schließen der Anwendung

jedoch nicht geschlossen werden konnte. Es wird gemeldet, dass die Anwendung verwendet wird. Um den Namen des Prozesses zu ermitteln, führen Sie "Get-AppVVirtualProcess" aus. Beenden Sie den Prozess dann im Task-Manager oder über "Stop AppVClientPackage". [DNA-23624]

- Beim Entfernen eines App-V-Pakets aus der Anwendungsbibliothek wird es aus der Studio-Anzeige, jedoch nicht vom VDA entfernt. Führen Sie als Workaround die folgenden Cmdlets über den VDA mit erhöhten Administratorrechten aus:

  Import-Module AppvClient
  Get-AppVClientPackage -all
  #Paket-ID und Versions-ID des zu entfernenden Pakets ermitteln
  Remove-AppVClientPackage -PackageId <*packageid*> -VersionId <*versionid*> [DNA-47379]

- Aufgrund der Funktionsweise von Microsoft App-V kann bei der Veröffentlichung mehrerer sequenzierter Versionen derselben App über die Einzelverwaltung oder die duale Verwaltung jeweils nur eine Version der App pro Benutzer auf dem VDA gestartet werden. Die von einem Benutzer zuerst gestartete Version bestimmt, welche Version später ausgeführt wird. Das gleiche Verhalten tritt auf, wenn keine Citrix Komponenten beteiligt sind und der Benutzer die sequenzierten Apps über Desktop-Verknüpfungen startet, die auf unterschiedliche Pfade verweisen. Bisher hat Citrix dieses Verhalten bei verschiedenen Versionen der Browser Mozilla Firefox und Google Chrome festgestellt. [APPV-60]

Citrix Director

- Wenn Sie in einer Umgebung mit mehreren Sitzungen **Filter** > **Sitzungen** > **Alle** aufrufen und sich von einer Sitzung abmelden, wird die Sitzung abgemeldet. Wenn Sie eine weitere Sitzung mit demselben Benutzernamen auswählen und eine Abmeldung versuchen, wird folgende Fehlermeldung angezeigt:

  Die Datenquelle reagiert nicht oder hat einen Fehler gemeldet. Weitere Informationen finden Sie in den Ereignisprotokollen des Director-Servers. [LC8826]

Installation und Upgrade

- Wenn Sie ein Upgrade von VDA 7.14 auf VDA 7.15 durchführen, werden die unter dem Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\Policies\Citrix erstellten Schlüssel für Citrix Richtlinieneinstellungen, die unter **Administrative Vorlagen** angewendet werden, möglicherweise vom VDA gelöscht. [LCM-3876]
- Bei der Installation von Komponenten unter Verwendung der AutoSelect-Anwendung auf dem Installationsmedium enthält die Datei autorun.log möglicherweise Fehler und Ausnahmen

bezüglich unzureichender Rechte. Wenn die Installation erfolgreich abgeschlossen wurde, können Sie diese Fehler ignorieren. Um sie zu vermeiden, starten AutoSelect unter Auswahl der Option **Als Administrator ausführen**. [DNA-45937]

- Beim Upgrade einer XenDesktop 5.6-Bereitstellung auf XenDesktop 7.15 LTSR fehlt die Gruppenrichtlinie. Führen Sie als Workaround zunächst ein Upgrade von XenDesktop 5.6 auf XenDesktop 7.13 durch. Führen Sie anschließend das Upgrade von 7.13 auf 7.15 LTSR durch. [DNA-44818]
- Wenn Sie bei der Installation eines Controllers auf der Seite **Smart Tools** des Installationsassistenten **Mit Smart Tools und Call Home Verbindung herstellen** auswählen, wird Call Home möglicherweise nicht aktiviert. Verwenden Sie als Workaround entweder den Zeitplan in Citrix Scout oder aktivieren Sie Call Home über die PowerShell. [CAM-9907]
- Wenn Sie bei der Installation eines Delivery Controllers unter Windows Server 2012 R2 oder Windows Server 2016 die Verbindung mit Smart Tools auswählen und mit Ihrem Citrix Cloud-Konto mehrere Organisationen verknüpft sind, wird die Anmeldung nach der Eingabe Ihrer Citrix Cloud-Anmeldeinformationen möglicherweise nicht abgeschlossen. Führen Sie als Workaround einen der folgenden Schritte aus:
  - Sicherstellen, dass für Windows Server und Internet Explorer die neuesten Updates installiert sind.
  - Deaktivieren Sie in Internet Explorer folgende Option: Internetoptionen > Sicherheit > Lokales Intranet > Sites > Alle Sites, die den Proxyserver umgehen, einbeziehen. [CAM-9816]
- Wenn StoreFront ursprünglich über die ausführbare Datei auf dem Installationsmedium installiert wurde, wird es, wenn Sie später das Komplettinstallationsprogramm für eine neuere Version verwenden, nicht als aktualisierbar angezeigt. Aktualisieren Sie StoreFront als Workaround über die ausführbare Datei auf dem Installationsmedium. [#DNA-47816]
- Beim Aktualisieren des Delivery Controllers von einer früheren Version als 7.13 auf Version 7.13 und höher wird möglicherweise ein Fehler (Ausnahme) angezeigt, wenn die Einstellung "Timeout für autom. Wiederverbindung von Clients"in einer der Richtlinien konfiguriert ist. Dieser Fehler tritt auf, wenn der Einstellungswert für "Timeout für autom. Wiederverbindung von Clients"außerhalb des zulässigen Bereichs von 0 bis 300 liegt, der in Version 7.13 eingeführt wurde. Um diesen Fehler zu verhindern, verwenden Sie den PowerShell-Anbieter für Citrix Gruppenrichtlinien, um die Konfiguration der Einstellung aufzuheben oder einen Wert innerhalb des angegebenen Bereichs festzulegen. Ein Beispiel finden Sie unter CTX22947. [DNA-52476]
- Beim Auswählen und Hinzufügen von Maschinen können in Studio derselben Bereitstellungsgruppe Maschinen aus nicht kompatiblen Maschinenkatalogen hinzugefügt werden. (Wenn Sie zuerst eine Bereitstellungsgruppe auswählen und dann Maschinen hinzufügen, verhindert Stu-

dio, dass Maschinen aus nicht kompatiblen Maschinenkatalogen hinzugefügt werden.) [DNA-39589]

Allgemein

- Wenn MCS nicht permanente Maschinen in AWS erstellt, wird das Flag `DeleteOnTermination` auf *True*gesetzt. Beim Aus- und Wiedereinschalten erstellt MCS jedoch neue EBS-Volumes und tauscht sie gegen die alten aus, wodurch das Flag `DeleteOnTermination` in *False* geändert wird. [PMCS-4953]
- Bei Verwendung eines sitzungsinternen Zertifikat des Verbundauthentifizierungsdiensts für die Authentifizierung einer TLS 1.1-(oder früheren)-Verbindung kann die Verbindung fehlschlagen. Es wird Ereignis-ID 305 protokolliert, die eine nicht unterstützte Hash-ID anzeigt. Der Verbundauthentifizierungsdienst unterstützt SHAMD5-Hash nicht. Um dieses Problem zu umgehen, verwenden Sie TLS 1.2-Verbindungen. Dieses Problem betrifft XenApp und XenDesktop ab Version 7.9 bis zur vorliegenden Version. [DNA-47628]
- Die Einstellungen der Richtlinie "Druckertreiberzuordnung und -kompatibilität"werden nicht gespeichert. Verwenden Sie als Workaround den PowerShell-Anbieter für Citrix Gruppenrichtlinien zum Bearbeiten dieser Einstellungen. Weitere Informationen zu dem Workaround finden Sie unter CTX226589. [DNA-47423]
- Fehler in Windows-Ereignisprotokoll: Windows konnte die Abbildintegrität der Datei "MfApHook64.dll"nicht überprüfen. Weitere Informationen finden Sie unter CTX226397. [HDX-9063]
- Beim Starten einer Anwendung über StoreFront wird diese möglicherweise nicht im Vordergrund gestartet oder sie ist im Vordergrund, jedoch nicht im Fokus. Klicken Sie als Workaround auf das Symbol in der Taskleiste, um die Anwendung in den Vordergrund zu bringen bzw. auf das Anwendungsfenster, um sie in den Fokus bringen. [HDX-10126]
- Veröffentlichte Inhalte werden nicht erfolgreich gestartet, wenn sie vom Citrix Receiver aus initiiert wurden. Über den StoreFront-Webclient (oder das Webinterface) gestarteter Inhalt wird wie erwartet gestartet. [LC6316, RFWIN-4957]
- Wenn Sie einen Azure Resource Manager-Maschinenkatalog löschen, werden die zugeordneten Maschinen und Ressourcengruppen aus Azure gelöscht, selbst wenn Sie angeben, dass sie beibehalten werden sollen. [DNA-37964]
- Bei Verwendung einer neueren Version von Citrix Receiver für Windows als 4.6 kann per Multicast möglicherweise kein Video angezeigt werden. Audio steht weiterhin zur Verfügung. Fügen Sie als Workaround dem Endpunkt folgenden Registrierungsschlüssel hinzu:

HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream;
Name: DisableVMRSupport;

Typ: DWORD;
Wert: 4; [HDX-10055]

Drucken

- Bei Anhalten oder Neustarten des Citrix Druckmanagerdiensts hört der Prozess "CpSvc.exe" möglicherweise auf zu reagieren. Beenden Sie als Workaround CpsSvc.exe vor dem Beenden oder Neustarten des Diensts im Dienste-Snap-In oder starten Sie den VDA neu, um dieses Problem zu vermeiden. [HDX-10071]
- Auf dem virtuellen Desktop ausgewählte universelle Druckserver-Drucker werden im Fenster **Geräte und Drucker** in der Windows-Systemsteuerung nicht angezeigt. In den Anwendungen stehen diese Drucker den Benutzern jedoch zur Verfügung. Das Problem tritt nur unter Windows Server 2012, Windows 10 und Windows 8 auf. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX213540. [335153]

Sitzungsaufzeichnung

- Wenn von Maschinenerstellungsdienste (MCS) oder Provisioning Services (PVS) mehrere VDAs mit dem konfigurierten Masterimage und installiertem Microsoft Message Queuing (MSMQ) erstellt werden, erhalten die VDAs unter bestimmten Bedingungen ggf. die gleiche QMID. Dies kann u. a. zu folgenden Problemen führen:
  - Sitzungen werden nicht aufgezeichnet, selbst wenn eine Aufzeichnungsvereinbarung akzeptiert wurde.
  - Der Sitzungaufzeichnungsserver empfängt möglicherweise keine Sitzungsabmeldungssignale, sodass Sitzungen permanent den Status "Live"beibehalten.

Informationen für einen Workaround finden Sie in den Artikeln zur Installation der Sitzungsaufzeichnung. [528678]

Probleme mit Drittanbieterprodukten

- Citrix und Microsoft haben ein Problem beim Start von Seamlessanwendungen über einen VDA unter Windows Server 2016 gefunden. Wenn ein Benutzer eine über einen solchen VDA veröffentlichte Anwendung startet, bedeckt ein schwarzer Bildschirm in Citrix Receiver mehrere Sekunden lang den Arbeitsbereich, bevor die Anwendung gestartet wird. Weitere Informationen finden Sie unter CTX225819.

  Warnung: Wenn Sie Azure Active Directory (AAD) verwenden, führen Sie die in CTX225819 beschriebene Registrierungsänderung nicht durch. Wenn Sie diese Änderung vornehmen, können Sitzungsstartfehler für AAD-Benutzer auftreten. [HDX-5000]

- In einer Belastungstestumgebung stürzt Microsoft Windows WinLogon.exe mit einer Häufigkeit von unter 0,001 % von 20.000 Anmeldungen ab. [HDX-9938]

Hinweise zu Drittanbietern

August 18, 2021

Dieses Release von XenApp und XenDesktop enthält ggf. Software von Drittanbietern, die gemäß den in den folgenden Dokumenten aufgeführten Bestimmungen lizenziert ist:

XenApp und XenDesktop –Hinweise zu Drittanbietern (PDF-Download)

Non-Commercial Software Disclosure For FlexNet Publisher 2016 R1 (11.14.0.0)

FLEXnet Publisher Documentation Supplement: Open Source Software Licenses applicable to FlexNet Publisher 11.14.0 (PDF-Download)

Sitzungsaufzeichnung - Hinweise zu Drittanbietern (PDF-Download)

Veraltete und entfernte Produkte und Features

November 15, 2022

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

Die folgenden Plattformen, Citrix Produkte und Features sind *veraltet*: Dies bedeutet nicht, dass sie sofort außer Betrieb genommen werden. Der Support durch Citrix wird in XenApp und XenDesktop 7.15 LTSR (Long Term Service Release) fortgesetzt. Veraltete Elemente werden in einem aktuellen Release nach diesem LTSR entfernt. Alternativen für veraltete Elemente werden nach Möglichkeit vorgeschlagen.

Informationen zum Produktlebenszyklus-Support finden Sie unter Supportrichtlinie für Produktlebenszyklen.

Element	Einstellung der Unterstützung angekündigt in	Entfernt in	Alternative
StoreFront-Browserunterstützung für Microsoft Edge (Legacy)	7.15 LTSR CU7	-	Upgrade auf Microsoft Edge (basierend auf Chromium).
Browserinhaltsumleitung	7.15 LTSR CU7	-	Upgrade auf 1912 LTSR.
Citrix License Administration Console (zuletzt enthalten in Windows-Lizenzserver 11.16.3 Build 30000, ab Windows-Lizenzserver v11.16.6 Build 31000 entfernt).	7.15 LTSR CU6	7.15 LTSR CU6	Verwenden Sie den Citrix Licensing Manager.
Entfernen von Citrix Smart Tools Agent von Citrix Virtual Apps and Desktops-Installationsmedien.	1903 und 7.15 LTSR CU4	7.15 LTSR CU4	—
Citrix Receiver für Web, klassisches Design mit “grünen Blasen”	7.15 LTSR (und StoreFront 3.12)	—	Citrix Receiver für Web, einheitliche Benutzeroberfläche.
VDAs unter Windows 10 Version 1511 (Schwellenwert 2) und früheren Windows Desktopbetriebssystemreleases, einschließlich Windows 8.x oder Windows 7	7.15 LTSR (und 7.12)	7.16	Installieren Sie Desktopbetriebssystem-VDAs unter Windows 10 Version 1607 (Redstone 1) oder aktuellen halbjährlichen Kanälen. Bei der Verwendung von 1607 LTSB empfehlen wir einen VDA der Version 7.15.

Element	Einstellung der Unterstützung angekündigt in	Entfernt in	Alternative
VDAs unter Windows Server 2008 R2 und Windows Server 2012 (einschließlich Service Packs).	7.15 LTSR (und 7.12)	7.16	Installieren Sie Serverbetriebssystem-VDAs unter unterstützten Versionen z. B. Windows Server 2012 R2 oder Windows Server 2016.
Delivery Controller unter Windows Server 2012 und 2008 R2 (einschließlich Service Packs).	7.15 LTSR	—	Installieren Sie Delivery Controller unter einem anderen unterstützten Betriebssystem.
Studio unter Windows 7 (einschließlich Service Packs).	7.15 LTSR	7.18	Installieren Sie Studio unter einem anderen unterstützten Betriebssystem.
Flash-Umleitung	7.15 LTSR	—	Die Citrix Workspace-App 1912 und höher unterstützt HDX-Flash-Umleitung (Teil von XenApp und XenDesktop 7.15 LTSR CU6) nicht. HDX-Flash-Umleitung ist nur bis einschließlich Citrix Workspace-App 1911 verfügbar. Sie können auch Citrix Receiver 4.9 LTSR mit 7.15 LTSR CU6 verwenden.
DirectX Command Remoting (DCR)	7.15 LTSR	7.16	Verwenden Sie Thinwire.

Element	Einstellung der Unterstützung angekündigt in	Entfernt in	Alternative
Citrix Online-Integration (GoTo-Produkt) in StoreFront	7.14 (und StoreFront 3.11)	StoreFront 3.12	Ab StoreFront 3.12 kann dieses Feature nicht in der StoreFront-Verwaltungskonsole konfiguriert werden. Wenn Sie ein Upgrade auf StoreFront 3.12 durchführen, können Sie dieses Feature weiterhin verwenden. Zum Ändern der Konfiguration verwenden Sie das PowerShell-Cmdlet "Update-DSGenericApplications". Weitere Informationen finden Sie unter Integrieren von Citrix Online-Anwendungen in Stores.
Direkte Upgrades aus StoreFront 2.0, 2.1, 2.5 und 2.5.2	7.13	7.16	Führen Sie ein Upgrade einer dieser Versionen auf eine unterstützte neuere Version und dann auf XenApp und XenDesktop 7.13 durch.
Direkte Upgrades von XenDesktop 5.6 oder 5.6 FP1	7.12	7.16	Migrieren Sie Ihre XenDesktop 5.6- oder 5.6 FP1-Bereitstellung in die aktuelle XenDesktop-Version.

Element	Einstellung der Unterstützung angekündigt in	Entfernt in	Alternative
VDAs unter Windows 8.1 und früheren Windows-Desktopversionen	7.12	—	Installieren Sie Serverbetriebssystem-VDAs unter unterstützten Versionen z. B. Windows Server 2012 R2 oder Windows Server 2016.
XenDesktop 5.6 unter Windows XP. Es werden keine VDA-Installationen unter Windows XP mehr unterstützt.	7.12	—	Installieren Sie VDAs unter einer unterstützten Windows-Version.
CloudPlatform-Verbindungen.	7.12	—	Verwenden Sie einen anderen unterstützten Hypervisor oder Clouddienst.
Verbindungen mit Azure Classic (auch “Azure Service Management”).	7.12	—	Verwenden Sie Azure Resource Manager.
Installation der Kernkomponenten Delivery Controller, Director, StoreFront und Lizenzserver auf 32-Bit-Maschinen (Ausnahme: Studio).	7.12	7.16	Verwenden Sie 64-Bit-Maschinen.
Verbindungsleasing.	7.12	7.16	Verwenden Sie den lokalen Hostcache.
Legacy-Thinwire-Modus	7.12	7.16	Verwenden Sie Thinwire.
HDX-Desktopgestaltungsumleitung	7.12	—	—

Element	Einstellung der Unterstützung angekündigt in	Entfernt in	Alternative
AppDisks-Funktionalität (sowie unterstützende AppDNA-Integration in Studio)*	7.13	2003	Verwenden Sie Citrix App Layering.
Persönliche vDisk-Funktionalität*	7.13	2006	Verwenden Sie Citrix App Layering – Benutzerlayer oder Benutzerpersonal-isierungslayer.

*Feature nicht von der LTSR-Wartungsoption abgedeckt.

Section 508 Voluntary Product Accessibility Template

August 18, 2021

Compliance bezüglich Section 508 und Engagement im Rahmen von WCAG 2.0

Citrix ist bestrebt, Technologien jedermann zugänglich zu machen. Wir arbeiten derzeit an Initiativen mit hoher Priorität zur Gestaltung und Entwicklung von Produkten, bei denen ein Schwerpunkt auf verbesserter Benutzerfreundlichkeit und Barrierefreiheit für alle Kunden –mit oder ohne Behinderung –liegt. Citrix unterstützt Standards zur Barrierefreiheit, darunter Section 508 Compliance und WCAG 2.0.

Harmonisierung der Compliance bezüglich Section 508 und WCAG 2.0

Das World Wide Web Consortium (W3C) hat unter dem Titel *Web Content Accessibility Guidelines* (WCAG) Richtlinien für barrierefreie Onlineinhalte entwickelt. Diese wurden zum Standard ISO/IEC 40500 erklärt, der eine Reihe von Vorgaben enthält, um Onlineinhalte barrierefrei zu gestalten. In den Vereinigten Staaten gibt es ähnliche Bestimmungen. Section 508 ist Teil der Federal Acquisition Regulation (FAR), die dem Rehabilitation Act von 1973 entstammt. Ähnlich wie bei den WCAG besteht das vorrangige Ziel dieses Gesetzes darin, Menschen mit Behinderung einen gleichwertigen Zugang

zur Informations- und Kommunikationstechnik (ICT) der amerikanischen Bundesbehörden sowie deren Nutzung zu ermöglichen. Im Januar 2017 veröffentlichte das United States Access Board eine Richtlinie zur Harmonisierung von Section 508 und WCAG 2.0. Daher konzentriert sich Citrix verstärkt auf die neuen Updates der WCAG, um Kunden Produkte mit höchster Barrierefreiheit zur Verfügung zu stellen.

Voluntary Product Accessibility Template (VPAT)

VPAT-Dokumente für verschiedene Citrix Produkte und Komponenten können von https://www.citrix.com/about/legal/security-compliance/section-508.html heruntergeladen werden.

Systemanforderungen

January 6, 2023

Einführung

Die Systemanforderungen in diesem Dokument galten zum Zeitpunkt der Freigabe der Produktversion, Änderungen werden regelmäßig veröffentlicht. Nicht in diesem Dokument aufgeführte Systemanforderungen (z. B. StoreFront, Hostsysteme und Citrix Workspace-App, Plug-Ins und Provisioning Services) werden in der jeweiligen Dokumentation behandelt.

Wichtig: Vor Beginn einer Installation lesen Sie den Artikel Vorbereiten der Installation.

> **Hinweis:**
>
> *Unterstützung für Windows-Betriebssysteme: Citrix XenApp und XenDesktop sowie zugehörige Komponenten werden nur von Betriebssystemversionen unterstützt, für die deren Hersteller Support leistet. Kunden müssen möglicherweise erweiterten Support vom Hersteller ihres Betriebssystems erwerben.

Sofern nicht anders angegeben, wird erforderliche Software (z. B. .NET und C++-Pakete) automatisch bereitgestellt, wenn die erforderlichen Versionen nicht auf der Maschine erkannt werden. Das Citrix Installationsmedium enthält außerdem einige erforderliche Softwarekomponenten.

Das Installationsmedium enthält mehrere Komponenten von Drittanbietern. Bevor Sie diese Citrix Software verwenden, überprüfen Sie, ob Sicherheitsupdates von Drittanbietern nötig sind und installieren Sie sie.

Informationen zur Globalisierung finden Sie unter CTX119253.

Für Komponenten und Features, die auf Windows-Servern installiert werden können, werden Server Core- und Nano Server-Installationen nicht unterstützt, es sei denn, dies wird ausdrücklich erwähnt.

Komponenten und Features, die auf Maschinen mit Windows 10 verwendet werden können, unterstützen folgende Windows 10-Wartungsoptionen und -Versionen:

- Semi-Annual Channel: Pro, Enterprise, Education, Mobile Enterprise (IoT Core Pro Edition wird nur von Citrix Workspace-App unterstützt)
- Long-term Servicing Channel (LTSC): Enterprise LTSB Edition

Weitere Informationen finden Sie unter CTX224843.

Hardwareanforderungen

Schätzwerte für RAM und Datenträgerspeicherplatz verstehen sich zuzüglich des für Produktimage, Betriebssystem und andere Software auf der Maschine erforderlichen Speicherplatzes. Die Leistung hängt von der Konfiguration ab. Dazu gehören die verwendeten Features, die Anzahl der Benutzer und weitere Faktoren. Die Verwendung der Mindestkonfiguration kann die Leistung beeinträchtigen.

Der auf dem Controller für das standardmäßig aktivierte Verbindungsleasing erforderliche Speicherplatz hängt beispielsweise von der Anzahl Benutzer und Anwendungen und vom Modus ab: Bei 100.000 RDS-Benutzern mit 100 vor kurzem verwendeten Anwendungen werden ca. 3 GB für das Verbindungsleasing benötigt, bei Bereitstellungen mit mehr Anwendungen ist ggf. mehr Speicherplatz erforderlich. Bei dedizierten VDI-Desktops benötigen 40.000 Desktops mindestens 400-500 MB. Auf jeden Fall empfiehlt Citrix, mehrere GB an zusätzlichem Speicherplatz bereitzustellen.

Die folgende Tabelle enthält die Mindestanforderungen für die Kernkomponenten.

Komponente	Minimum
Alle Kernkomponenten auf einem Server, nur für eine Evaluierung, keine Produktionsbereitstellung	5 GB RAM
Alle Kernkomponenten auf einem Server, für Testbereitstellung oder kleinere Produktionsumgebung	12 GB RAM
Delivery Controller (mehr Speicherplatz für den lokalen Hostcache erforderlich)	5 GB RAM, 800 MB Festplatte
Studio	1 GB RAM, 100 MB Festplatte
Director	2 GB RAM, 200 MB Festplatte

Komponente	Minimum
StoreFront	2 GB RAM, Empfehlungen zum Datenträger finden Sie in der StoreFront-Dokumentation.
Lizenzserver	2 GB RAM, Empfehlungen zum Datenträger finden Sie in der Dokumentation zur Lizenzierung.

Dimensionierung von VMs zur Bereitstellung von Desktops und Anwendungen

Aufgrund der Komplexität und Dynamik des Hardwareangebots sind keine spezifischen Empfehlungen möglich. Außerdem hat jede XenApp- und XenDesktop-Bereitstellung ganz individuelle Anforderungen. Im Allgemeinen werden XenApp-VMs auf der Basis der Hardware und nicht der Benutzerarbeitslasten dimensioniert. Ausnahme bildet der RAM, der größer sein muss, wenn RAM-intensive Anwendungen verwendet werden. Citrix Tech Zone enthält die aktuellen Anweisungen zur VDA-Dimensionierung.

Microsoft Visual C++ Runtime-Versionen

Installieren von Microsoft Visual C++ 2017 Runtime auf einer Maschine, auf dem Microsoft Visual C++ 2015 Runtime installiert ist, kann dazu führen, dass Visual C++ 2015 Runtime automatisch entfernt wird. Das ist per Design.

Wenn Sie bereits Citrix-Komponenten installiert haben, die Visual C++ 2015 Runtime automatisch installieren, funktionieren diese Komponenten weiterhin korrekt mit Visual C++ 2017-Version.

Weitere Informationen finden Sie im Microsoft-Artikel https://developercommunity.visualstudio.com/content/problem/332815/visual-c-redistributable-2017-install-removes-visu.html.

Delivery Controller

Unterstützte Betriebssysteme:

- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition*

Anforderungen:

- Microsoft .NET Framework 3.5.1 (nur Windows Server 2008 R2)

- Microsoft .NET Framework 4.5.2 (4.6 bis 4.8 werden auch unterstützt)
- CU3 und früher: Windows PowerShell 2.0
- CU4 und höher: sowohl Windows PowerShell 2.0 als auch Windows PowerShell 3.0 oder höher
- Microsoft Visual C++ 2015 Runtime (32-Bit und 64-Bit)

Datenbanken

Unterstützte Versionen von Microsoft SQL Server für die Datenbanken für Sitekonfiguration, Konfigurationsprotokollierung und Überwachung:

- SQL Server 2019, Express, Standard und Enterprise Editionen unterstützen XenApp und XenDesktop 7.15 LTSR CU6 und höhere Versionen.
- SQL Server 2019, Express, Standard und Enterprise Editionen unterstützen Provisioning Services 7.15 LTSR CU7 und höhere Versionen.
- SQL Server 2017, Express, Standard und Enterprise Edition.
- SQL Server 2016 SP1 bis SP3, Express, Standard und Enterprise Edition.
- SQL Server 2014 SP1 bis SP3, Express, Standard und Enterprise Edition. Standardmäßig wird SQL Server 2014 SP2 Express zusammen mit dem Controller installiert, wenn keine unterstützte SQL Server-Installation erkannt wird.
- SQL Server 2012 bis SP4, Express, Standard und Enterprise Edition.
- SQL Server 2008 R2 SP2 und SP3, Express, Standard, Enterprise und Datacenter Edition.

Die folgenden Lösungen für hohe Verfügbarkeit der Datenbank werden unterstützt (außer bei SQL Server Express, das nur den eigenständigen Modus unterstützt):

- SQL Server AlwaysOn-Failoverclusterinstanzen
- SQL Server AlwaysOn-Verfügbarkeitsgruppen (einschließlich Basisverfügbarkeitsgruppen)
- SQL Server-Datenbankspiegelung

Die Windows-Authentifizierung ist für Verbindungen zwischen dem Controller und der SQL Server-Sitedatenbank erforderlich.

Wenn Sie einen Controller installieren, wird standardmäßig eine SQL Server Express-Datenbank zur Verwendung mit dem lokalen Hostcache installiert. Diese Installation erfolgt separat von der standardmäßigen SQL Server Express-Installation für die Sitedatenbank.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Datenbanken
- CTX114501
- Leitfaden für die Datenbankgröße
- Lokaler Hostcache

Citrix Studio

Unterstützte Betriebssysteme:

- Windows 10 (Informationen zu unterstützten Editionen siehe Abschnitt *Einführung*)
- Windows 8.1, Professional und Enterprise Edition*
- Windows 7, Professional, Enterprise und Ultimate Edition*
- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition*

Anforderungen:

- Microsoft .NET Framework 4.5.2 (4.6 bis 4.8 werden auch unterstützt)
- Microsoft Management Console 3.0 (in allen unterstützten Betriebssystemen enthalten)
- Windows PowerShell 2.0 (CU 3 und früher)
- Windows PowerShell 3.0 oder höher (CU 4 und höher)

Citrix Director

Unterstützte Betriebssysteme:

- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition*

Anforderungen:

- Microsoft .NET Framework 4.5.2 (4.6 bis 4.8 werden auch unterstützt)
- Microsoft .NET Framework 3.5 SP1 (nur Windows Server 2008 R2)
- Microsoft Internetinformationsdienste (IIS) 7.0 und ASP.NET 2.0. Stellen Sie sicher, dass der Static-Content-Rollendienst für die IIS-Serverrolle installiert ist. Wenn diese Komponenten nicht auf Ihrem Server installiert sind, werden Sie möglicherweise aufgefordert, das Windows Server-Installationsmedium einzulegen. Sie werden dann installiert.

> Hinweis:
>
> Um die Ereignisprotokolle auf Computern anzuzeigen, auf denen Citrix Director installiert ist, müssen Sie Microsoft .NET Framework 2.0 installieren.

Citrix User Profile Manager

- Stellen Sie sicher, dass Citrix User Profile Manager und das Citrix User Profile Manager WMI-Plug-In auf dem VDA installiert sind (Abschnitt "Zusätzliche Komponenten"im Installationsassistenten) und dass der Citrix Profilverwaltungsdienst ausgeführt wird, um die Benutzerprofildetails in Director anzuzeigen.

Anforderungen für eine System Center Operations Manager (SCOM)-Integration:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Unterstützte Browser zum Anzeigen von Director:

- Internet Explorer 11. (Auf Windows Server 2012 R2-Maschinen können Sie nur Internet Explorer 10 verwenden.) Der Kompatibilitätsmodus wird für Internet Explorer nicht unterstützt. Für den Zugriff auf Director müssen Sie die empfohlenen Webbrowsereinstellungen verwenden. Akzeptieren Sie bei der Installation von Internet Explorer die Standardeinstellung zur Verwendung der empfohlenen Sicherheits- und Kompatibilitätseinstellungen. Wenn Sie den Browser bereits installiert haben und die empfohlenen Einstellungen nicht verwenden möchten, gehen Sie zu Extras > Internetoptionen > Erweitert > Zurücksetzen und folgen Sie den Anweisungen.
- Microsoft Edge
- Firefox ESR (Extended Support Release)
- Chrome

Die empfohlene optimale Bildschirmauflösung für die Anzeige von Director ist 1366 x 1024.

Virtual Delivery Agent (VDA) für Desktopbetriebssysteme

Unterstützte Betriebssysteme:

- Windows 10 (Informationen zu unterstützten Editionen siehe Abschnitt *Einführung*). Die folgenden Features werden unter Windows 10 nicht unterstützt: Desktopgestaltungsumleitung und Legacy-Grafikmodus.
- Windows 8.1, Professional und Enterprise Edition*
- Windows 7 SP1, Professional, Enterprise und Ultimate Edition*

Anforderungen:

- Microsoft .NET Framework 4.5.2 (4.6 bis 4.8 werden auch unterstützt)
- Microsoft .NET Framework 3.5.1 (nur Windows 7)
- Microsoft Visual C++ 2013 und 2015 Runtime (32-Bit und 64-Bit)
- PowerShell 3.0 oder höher

Remote-PC-Zugriff verwendet diesen VDA, den Sie auf physischen Büro-PCs installieren. Dieser VDA unterstützt den sicheren Start für XenDesktop-Remote-PC-Zugriff unter Windows 10.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream-Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, werden die Multimediabeschleunigungsfeatures nicht installiert und sind nicht funktionsfähig. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine, sonst können sich Benutzer nicht an der Maschine anmelden. Bei den meisten Editionen von Windows-Desktopbetriebssystemen ist Media Foundation bereits installiert und kann nicht entfernt werden. Bei N-Editionen sind bestimmte medienrelevante Technologien nicht enthalten; Sie können die Software von Microsoft oder einem Drittanbieter beziehen. Weitere Informationen finden Sie unter Vorbereiten der Installation.

Bei der VDA-Installation können Sie den HDX 3D Pro-Modus des VDAs für Windows-Desktopbetriebssysteme auswählen. Dieser Modus eignet sich besonders für DirectX- und OpenGL-gesteuerte Anwendungen sowie Rich Media-Inhalte wie Video. Weitere Informationen zur Unterstützung finden Sie im Abschnitt HDX 3D Pro.

Informationen über den Linux VDA finden Sie in den Artikeln zu Linux Virtual Delivery Agent.

Für das Verwenden des Server-VDI-Features können Sie über die Befehlszeilenschnittstelle einen VDA für Windows-Desktopbetriebssysteme auf einem unterstützten Serverbetriebssystem installieren. Weitere Informationen finden Sie im Artikel Server-VDI.

Virtual Delivery Agent (VDA) für Serverbetriebssysteme

Unterstützte Betriebssysteme:

- Windows Server 2016, Standard und Datacenter Edition
- Windows Server 2012 R2, Standard und Datacenter Edition
- Windows Server 2012, Standard und Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise und Datacenter Edition*

Das Installationsprogramm stellt die folgenden Anforderungen automatisch bereit, die auch auf den Citrix Installationsmedien in den Ordnern Support zur Verfügung stehen:

- Microsoft .NET Framework 4.5.2 (4.6 bis 4.8 werden auch unterstützt)
- Microsoft .NET Framework 3.5.1 (nur Windows Server 2008 R2)
- Microsoft Visual C++ 2013 und 2015 Runtime (32-Bit und 64-Bit)
- PowerShell 3.0 oder höher

Das Installationsprogramm installiert und aktiviert automatisch die Rollendienste für Remotedesktopdienste, wenn sie nicht bereits installiert und aktiviert sind.

Mehrere Multimediabeschleunigungsfunktionen (z. B. HDX MediaStream-Windows Media-Umleitung) erfordern, dass Microsoft Media Foundation auf dem Computer installiert wird, auf dem der VDA installiert ist. Wenn Media Foundation nicht installiert ist, werden die Multimediabeschleunigungsfea-

tures nicht installiert und sind nicht funktionsfähig. Entfernen Sie Media Foundation nicht nach der Installation der Citrix Software von der Maschine, sonst können sich Benutzer nicht an der Maschine anmelden. Bei den meisten Windows-Versionen wird Media Foundation über den Server-Manager installiert (bei Windows Server 2012 und neuer: ServerMediaFoundation, bei Windows Server 2008 R2: DesktopExperience). Bei N-Editionen sind bestimmte medienrelevante Technologien nicht enthalten; Sie können die Software von Microsoft oder einem Drittanbieter beziehen. Weitere Informationen finden Sie unter Vorbereiten der Installation.

Wenn Media Foundation nicht auf dem VDA vorhanden ist, funktionieren diese Multimediafeatures nicht:

- Flash-Umleitung
- Windows Media-Umleitung
- HTML5-Videoumleitung
- HDX Realtime-Webcamumleitung

Informationen über den Linux VDA finden Sie in den Artikeln zu Linux Virtual Delivery Agent .

Hosts/Virtualisierungsressourcen

Einige XenApp- und XenDesktop-Features werden möglicherweise nicht auf allen Hostplattformen bzw. allen Plattformversionen unterstützt. AppDisks werden beispielsweise auf XenServer-, VMware- und System Center Virtual Machine Manager-Hosts unterstützt. Weitere Informationen finden Sie in der Dokumentation zu dem jeweiligen Feature.

Das Wake-On-LAN-Feature von Remote-PC-Zugriff erfordert mindestens Microsoft System Center Configuration Manager 2012.

WICHTIG: Die folgenden *major.minor*-Versionen werden unterstützt, einschließlich von Updates für diese Versionen. CTX131239 enthält aktuelle Hypervisorversionsinformationen sowie Links zu bekannten Problemen.

XenServer

CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

VMware vSphere (vCenter + ESXi)

Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.

CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

Weitere Informationen finden Sie unter VMware-Virtualisierungsumgebungen.

System Center Virtual Machine Manager

Enthält alle Versionen von Hyper-V, die mit den unterstützten Versionen von System Center Virtual Machine Manager registriert werden können.

CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

Weitere Informationen finden Sie unter Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen.

Nutanix Acropolis

CTX131239 enthält aktuelle Versionshinweise sowie Links zu bekannten Problemen.

Weitere Informationen finden Sie unter Nutanix-Virtualisierungsumgebungen.

Amazon Web Services (AWS)

- Sie können Anwendungen und Desktops auf unterstützten Windows Server-Betriebssystemen bereitstellen.
- Citrix unterstützt Amazon Relational Database Service (RDS). Weitere Informationen finden Sie unter Citrix Ready Marketplace und Citrix und AWS.

CloudPlatform

- Die unterstützte Mindestversion ist 4.2.1 mit Hotfixes 4.2.1-4.
- Bereitstellungen wurden mit XenServer 6.2 (mit Service Pack 1 und Hotfix XS62ESP1003) und vSphere 5.1-Hypervisors getestet.
- CloudPlatform unterstützt keine Hyper-V-Hypervisors.
- CloudPlatform 4.3.0.1 unterstützt VMware vSphere 5.5.
- Weitere Informationen finden Sie in der CloudPlatform-Dokumentation (einschließlich den Versionshinweisen zu Ihrer CloudPlatform-Version).

Microsoft Azure

Microsoft Azure Resource Manager

Funktionsebenen von Active Directory

Die folgenden Funktionsebenen werden für Active Directory-Gesamtstrukturen und -Domänen unterstützt:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Natives Windows 2000 (auf Domänencontrollern nicht unterstützt)

HDX

UDP-Audio für Multistream-ICA wird von der Citrix Workspace-App für Windows und der Citrix Workspace-App für Linux unterstützt.

Die Echounterdrückung wird von der Citrix Workspace-App für Windows unterstützt.

Siehe Informationen zu Unterstützung und Anforderungen für HDX unten.

HDX-Desktopgestaltungsumleitung

Das Windows-Benutzergerät bzw. der Thin Client muss Folgendes unterstützen oder enthalten:

- DirectX 9
- Pixel Shader 2.0 (in Hardware unterstützt)
- 32 Bit pro Pixel
- 1,5 GHz Prozessor (32-Bit oder 64-Bit)
- 1 GB RAM
- 128 MB Videospeicher auf der Grafikkarte oder einem integrierten Grafikprozessor

HDX überprüft das Windows-Gerät auf die erforderlichen GPU-Anforderungen und schaltet dann ggf. automatisch auf serverseitige Desktopgestaltung um. Geräte, die die erforderlichen GPU-Anforderungen erfüllen aber nicht die benötigte Prozessorgeschwindigkeit oder RAM-Spezifikationen haben, müssen in der GPO-Gruppe der Geräte erfasst werden, die von der Desktopgestaltungsumleitung ausgeschlossen sind.

Als Mindestausstattung ist eine verfügbare Bandbreite von 1,5 MBit/s erforderlich, empfohlen werden 5 MBit/s. Die Werte schließen End-to-End-Latenz ein.

HDX und Windows Media-Bereitstellung

Für den clientseitigen Abruf von Windows Media-Inhalten, die Windows Media-Umleitung und die Windows Media-Multimediatranscodierung in Echtzeit werden folgende Clients unterstützt: Citrix Workspace-App für Windows, Citrix Workspace-App für iOS und Citrix Workspace-App für Linux.

Um den clientseitigen Inhaltsabruf von Windows Media auf Windows 8-Geräten zu verwenden, legen Sie Citrix Multimedia Redirector als Standardprogramm fest: Navigieren Sie zu **Systemsteuerung > Programme > Standardprogramme > Standardprogramme festlegen**, wählen Sie **Citrix Multimedia Redirector** und klicken Sie auf **Dieses Programm als Standard festlegen** oder auf **Standards für dieses Programm auswählen**. Für die GPU-Transcodierung ist ein NVIDIA CUDA-fähiger GPU mit Compute Capability 1.1 oder höher erforderlich. Siehe https://developer.nvidia.com/cuda/cuda-gpus.

HDX-Flash-Umleitung

> **Hinweis:**
>
> Die Citrix Workspace-App 1912 und höher unterstützt HDX-Flash-Umleitung (Teil von XenApp und XenDesktop 7.15 LTSR CU6) nicht. HDX-Flash-Umleitung ist nur bis einschließlich Citrix Workspace-App 1911 verfügbar.

Die folgenden Clients und Adobe Flash Player werden unterstützt:

- Citrix Workspace-App für Windows: Die zweite Generation der Flash-Umleitungsfeatures erfordert Adobe Flash Player for Other Browsers, diese Version wird auch als NPAPI Flash Player (Netscape Plugin Application Programming Interface) bezeichnet.
- Citrix Workspace-App für Linux: Die zweite Generation der Flash-Umleitungsfeatures erfordert Adobe Flash Player for other Linux oder Adobe Flash Player for Ubuntu.
- Citrix Online Plug-In 12.1: Für Legacyfeatures der Flash-Umleitung wird Adobe Flash Player für Windows Internet Explorer benötigt (auch ActiveX Player genannt).

Die Hauptversionsnummer von Flash Player auf dem Benutzergerät muss größer oder gleich der Hauptversionsnummer von Flash Player auf dem Server sein. Wenn eine ältere Version oder gar keine Version von Flash Player auf dem Benutzergerät installiert ist, werden Flash-Inhalte auf dem Server wiedergegeben.

Die Maschinen, auf denen VDAs ausgeführt werden, erfordern Folgendes:

- Adobe Flash Player für Windows Internet Explorer (ActiveX Player)
- Internet Explorer 11 (im Modus "Nicht-moderne-Oberfläche"). Sie können Internet Explorer 7-10 verwenden, doch die von Microsoft unterstützte und von Citrix empfohlene Version ist Version 11. Flash-Umleitung erfordert Internet Explorer auf dem Server; mit anderen Browsern werden Flash-Inhalte auf dem Server wiedergegeben.
- Der geschützte Modus muss in Internet Explorer deaktiviert sein (Extras > Internetoptionen > Registerkarte "Sicherheit"> Kontrollkästchen "Geschützten Modus aktivieren"deaktiviert). Starten Sie Internet Explorer neu, damit die Änderung wirksam wird.

HDX 3D Pro

Wenn Sie einen VDA für Windows-Desktopbetriebssysteme installieren, können Sie die Version HDX 3D Pro installieren.

Auf der physischen bzw. virtuellen Maschine, auf der die Anwendung gehostet wird, kann GPU-Passthrough oder Virtual GPU (vGPU) verwendet werden:

- GPU-Passthrough ist mit folgenden Anwendungen verfügbar: Citrix XenServer, Nutanix AHV, VMware vSphere und VMware ESX (= "Virtual Direct Graphics Acceleration"bzw. vDGA) sowie Microsoft Hyper-V unter Windows Server 2016 (= "Discrete Device Assignment"bzw. DDA).
- vGPU ist mit Citrix XenServer, Nutanix AHV und VMware vSphere verfügbar; siehe https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html.

Als Minimalausstattung für den Hostcomputer empfiehlt Citrix 4 GB RAM und vier virtuelle CPUs mit einer Taktfrequenz von 2,3 GHz.

Grafikprozessor (GPU):

- Im Hinblick auf CPU-basierte Komprimierung, einschließlich verlustfreier Komprimierung, unterstützt HDX 3D Pro alle Grafikkarten auf dem Hostcomputer, die mit der bereitgestellten Anwendung kompatibel sind.
- Für Virtual Graphics Acceleration mit der NVIDIA GRID-API kann HDX 3D Pro mit unterstützten NVIDIA GRID-Karten verwendet werden (siehe NVIDIA GRID). NVIDIA GRID liefert eine hohe Framerate und dadurch eine sehr interaktive Benutzererfahrung.
- Virtual Graphics Acceleration wird auf Datencenter-Grafikplattformen der Serie Intel Xeon Processor E3 unterstützt. Weitere Informationen finden Sie unter https://www.citrix.com/intel sowie https://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Virtual Graphics Acceleration wird auf Serverkarten der AMD FirePro S-Serie mit AMD RapidFire unterstützt (siehe AMD –Virtualisierung).

Benutzergerät:

- HDX 3D Pro unterstützt alle Monitorauflösungen, die von dem GPU auf dem Hostcomputer unterstützt werden. Um mit den empfohlenen Minimalspezifikationen für Benutzergeräte und GPUs eine optimale Leistung zu erzielen, empfiehlt Citrix jedoch eine maximale Monitorauflösung für Benutzergeräte von 1920 x 1200 Pixeln für LAN-Verbindungen sowie von 1280 x 1024 Pixeln für WAN-Verbindungen.
- Als Mindestausstattung für Benutzergeräte empfiehlt Citrix mindestens 1 GB RAM und eine CPU mit einer Taktfrequenz von 1,6 GHz. Zur Verwendung des standardmäßigen Tiefenkomprimierungscodecs, der bei Verbindungen mit geringer Bandbreite erforderlich ist, ist eine leistungsfähigere CPU erforderlich, es sei denn, die Decodierung erfolgt in der Hardware. Zur Erzielung der optimalen Leistung empfiehlt Citrix die Ausstattung von Benutzergeräten mit mindestens 2 GB RAM und einer Dual-Core-CPU mit einer Taktfrequenz von mindestens 3 GHz.

- Bei Multimonitorzugriff empfiehlt Citrix Benutzergeräte mit Vierkern-CPUs.
- Benutzergeräte benötigen keinen GPU für den Zugriff auf Desktops oder Anwendungen, die mit HDX 3D Pro bereitgestellt werden.
- Die Citrix Workspace-App muss installiert sein.

Weitere Informationen finden Sie unter HDX 3D Pro und www.citrix.com/xenapp/3d.

HDX-Videokonferenzen –Anforderungen für Webcam-Videokomprimierung

Unterstützte Clients: Citrix Workspace-App für Windows, Citrix Workspace-App für Mac und Citrix Workspace-App für Linux.

Unterstützte Videokonferenzanwendungen:

- Adobe Connect
- Cisco WebEx
- Citrix GoToMeeting HDFaces
- Google + Hangouts
- IBM Sametime
- Media Foundation-basierte Videoanwendungen auf Windows 8.x, Windows Server 2012 und Windows Server 2012 R2
- Microsoft Lync 2010 und 2013
- Für Microsoft Office Communicator:
- Microsoft Skype 6.7

Zum Verwenden von Skype auf einem Windows-Client bearbeiten Sie die Registrierung auf Client und Server folgendermaßen:

Clientregistrierungsschlüssel HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

Name: DefaultHeight, Typ: REG_DWORD, Wert: 240

Name: DefaultWidth, Typ: REG_DWORD, Wert: 320

Serverregistrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Kompatibilität

Name: skype.exe, Typ: REG_DWORD, Wert: 0

Andere Anforderungen an Benutzergeräte:

- Geeignete Hardware für die Audiowiedergabe
- DirectShow-kompatible Webcam (Webcam-Standardeinstellungen verwenden). Hardware-codierungsfähige Webcams senken die clientseitige CPU-Nutzung.
- Webcam-Treiber (möglichst vom Kamerahersteller)

Sitzungsaufzeichnung

Verwaltungskomponenten der Sitzungsaufzeichnung

Sie können die Verwaltungskomponenten der Sitzungsaufzeichnung (Datenbank für die Sitzungsaufzeichnung, Sitzungsaufzeichnungsserver und Richtlinienkonsole) auf dem gleichen oder auf verschiedenen Servern installieren.

Datenbank für die Sitzungsaufzeichnung

Unterstützte Betriebssysteme:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1*

Unterstützte Microsoft SQL Server-Versionen:

- Microsoft SQL Server 2016 SP1 Enterprise, Express und Standard
- Microsoft SQL Server 2014 SP2 Enterprise, Express und Standard
- Microsoft SQL Server 2012 SP3 Enterprise, Express und Standard
- Microsoft SQL Server 2008 R2 SP3 Enterprise, Express und Standard

Voraussetzung: .NET Framework 4.7.2

Sitzungsaufzeichnungsserver

Unterstützte Betriebssysteme:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1*

Weitere Anforderungen:

- Internetinformationsdienste (IIS) Version 10, 8.5, 8.0 oder 7.5
- .NET Framework Version 4.7.2
- Wenn der Sitzungsaufzeichnungsserver HTTPS als Kommunikationsprotokoll verwendet, fügen Sie ein gültiges Zertifikat hinzu. Die Sitzungsaufzeichnung verwendet in der Standardeinstellung HTTPS; dies wird von Citrix empfohlen.

- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung
- Für die Administratorprotokollierung: neueste Version von Chrome, Firefox oder Internet Explorer 11

Richtlinienkonsole für die Sitzungsaufzeichnung

Unterstützte Betriebssysteme:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Voraussetzung: .NET Framework 4.7.2

Sitzungsaufzeichnungsagent

Installieren Sie den Sitzungsaufzeichnungsagent auf jedem XenApp und XenDesktop-Server, auf dem Sie Sitzungen aufzeichnen möchten.

Unterstützte Betriebssysteme:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1*
- Windows 10
- Windows 8.1*
- Windows 7 SP1*

Anforderungen:

- XenApp/XenDesktop 7.15 Platinum-Lizenz
- XenApp/XenDesktop 7.6.4000 mit Platinum-Lizenz (nur VDA für Windows-Serverbetriebssysteme, VDA für Windows-Desktopbetriebssysteme wird nicht unterstützt)
- .NET Framework 4.7.2
- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung

Sitzungsaufzeichnungsplayer

Unterstützte Betriebssysteme:

- Windows 10
- Windows 8.1*
- Windows 7 SP1*

Voraussetzung: .NET Framework 4.7.2

Für optimale Ergebnisse sollten Sie den Sitzungsaufzeichnungsplayer auf einer Arbeitsstation installieren, die folgende Anforderungen erfüllt:

- Eine Bildschirmauflösung von 1024 x 768
- Eine Farbtiefe von mindestens 32 Bit
- Mindestens 2 GB RAM, größere RAM- und CPU-/GPU-Ressourcen können die Leistung bei der Wiedergabe grafikintensiver Aufzeichnungen verbessern, insbesondere, wenn die Aufzeichnungen viele Animationen enthalten.

Die Reaktionszeit bei der Suche hängt von der Größe der Aufzeichnung und der Computerhardware ab.

Universeller Druckserver

Der universelle Druckserver umfasst Client- und Serverkomponenten. Die UpsClient-Komponente ist in der VDA-Installation enthalten. Die UpsServer-Komponente wird auf jedem Druckserver installiert, auf dem die freigegebenen Drucker gespeichert sind, die Sie mit dem universellen Druckertreiber von Citrix in Benutzersitzungen bereitstellen möchten.

Die UpsServer-Komponente wird unter folgenden Betriebssystemen unterstützt:

- Windows Server 2016
- Windows Server 2012 R2 und 2012
- Windows Server 2008 R2 SP1*

Voraussetzung: Microsoft Visual C++ 2013 Runtime (32-Bit und 64-Bit)

Für VDAs für Windows-Serverbetriebssysteme erfordert die Benutzerauthentifizierung bei Druckvorgängen, dass der universelle Druckserver in der gleichen Domäne ist wie der VDA.

Auch eigenständige Client- und Server-Komponentenpakete stehen zum Download zur Verfügung.

Weitere Informationen finden Sie unter Bereitstellen von Druckern.

Sonstiges

StoreFront 3.12.2000 ist die in diesem Release unterstützte Mindestversion. Zur Verwendung des Zonenpräferenz-Features müssen Sie mindestens StoreFront 3.12.2000 und NetScaler Gateway 11.0-65.x ausführen.

> **Hinweis:**
>
> Wenn Sie eine unbeaufsichtigte Installation von StoreFront 3.12.5000 versuchen, wird das Installationsprogramm möglicherweise unerwartet beendet. Das Problem tritt auf, wenn PowerShell Version 3.0 oder später nicht auf dem Server installiert ist.

Wenn Sie Provisioning Services mit diesem Release verwenden, wird als Mindestversion Provisioning Services 7.15.3 unterstützt.

Die unterstützte Mindestversion des Lizenzservers für XenApp und XenDesktop 7.15 LTSR CU6 ist 11.15.0.0 Build 24100. Weitere Informationen zu früheren CU-Versionen finden Sie unter Lizenzierung.

Die Microsoft-Gruppenrichtlinien-Verwaltungskonsole ist erforderlich, wenn Sie Citrix Richtlinieninformationen in Active Directory und nicht in der Sitekonfigurationsdatenbank speichern. Wenn Sie CitrixGroupPolicyManagement_x64.msi separat installieren (zum Beispiel auf einer Maschine, auf der keine XenApp- oder XenDesktop-Kernkomponente installiert ist), muss auf dieser Maschine Visual Studio 2015 Runtime installiert sein. Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Wenn Sie Citrix Scout unter Windows 7 oder Windows 2008 R2 verwenden möchten, müssen Sie PowerShell 3.0 auf den betreffenden Maschinen installieren. Vollständige Anforderungen finden Sie unter Citrix Scout.

Die Verwendung mehrerer Netzwerkkarten wird nicht unterstützt.

Standardmäßig wird zusammen mit einem VDA die Citrix Workspace-App für Windows installiert.

Informationen zu unterstützten Versionen von Microsoft App-V finden Sie unter App-V.

Unter Lokaler App-Zugriff finden Sie Informationen zu unterstützten Browsern für dieses Feature.

Informationen zu Unterstützung und Systemanforderungen für die Self-Service-Kennwortzurücksetzung finden Sie in der zugehörigen Dokumentation.

Clientordnerumleitung –unterstützte Betriebssysteme:

- Server: Windows Server 2008 R2 SP1, Windows Server 2012 und Windows Server 2012 R2
- Client (mit der aktuellen Version der Citrix Workspace-App für Windows): Windows 7, Windows 8, und Windows 8.1

Gemischte DPI-Werte bei mehreren Monitoren: Die Verwendung unterschiedlicher DPI-Werte bei mehreren Monitoren wird in Citrix XenDesktop and XenApp-Umgebungen nicht unterstützt. Sie können den DPI-Wert (Skalierung in %) unter "Windows-Systemsteuerung"> "Anzeige"überprüfen. Wenn Sie ein Windows 8.1- oder Windows 10-Clientgerät verwenden, können Sie unter "Windows-Systemsteuerung > Anzeige"mit der Option **Manuell eine Skalierungsstufe für alle Anzeigegeräte auswählen** die Monitore entsprechend konfigurieren. Weitere Informationen finden Sie unter CTX201696.

Diese Version von XenApp und XenDesktop ist nicht mit AppDNA 7.8 und 7.9 kompatibel. Citrix empfiehlt die Verwendung der aktuellen AppDNA-Version.

Technische Übersicht

January 6, 2023

XenApp und XenDesktop sind Virtualisierungslösungen, die IT die Steuerung von virtuellen Maschinen, Anwendungen sowie von der Lizenzierung und Sicherheit ermöglichen und gleichzeitig Benutzern von überall Zugriff mit jedem Gerät bieten.

XenApp und XenDesktop ermöglichen Folgendes:

- Endbenutzer können Anwendungen und Desktops unabhängig vom Betriebssystem und von der Benutzeroberfläche eines Geräts ausführen.
- Administratoren können Netzwerke verwalten und Zugriff von ausgewählten Geräten oder allen Geräten steuern.
- Administratoren können ein ganzes Netzwerk von einem Datencenter aus verwalten.

XenApp und XenDesktop haben eine einheitliche Architektur, die FlexCast Management Architecture (FMA) genannt wird. Die Hauptfunktion von FMA umfasst die Ausführung mehrerer Versionen von XenApp oder XenDesktop auf einer einzigen Site und die Bereitstellung von integriertem Provisioning.

Schlüsselkomponenten von XenApp und XenDesktop

Dieser Artikel ist besonders für neue Anwender von XenApp bzw. XenDesktop geeignet. Wenn Sie eine XenApp-Farm bis Version 6.x oder eine XenDesktop-Site bis Version 5.6 haben, lesen Sie auch die Informationen unter Änderungen in Version 7.x.

Diese Abbildung unten zeigt die wichtigsten Komponenten in einer typischen Bereitstellung, die als "Site"bezeichnet wird.

Delivery Controller:

Delivery Controller: Der Delivery Controller ist die zentrale Verwaltungskomponente einer XenApp- oder XenDesktop-Site. Jede Site hat einen oder mehrere Delivery Controller. Er muss auf mindestens einem Server im Datencenter installiert sein. Um die Zuverlässigkeit der Site zu gewährleisten, installieren Sie den Controller auf mehreren Servern. Wenn Ihre Bereitstellung virtuelle Maschinen auf einem Hypervisor oder in einem Clouddienst enthält, kommunizieren die Controller-Dienste mit dem Hypervisor, um Anwendungen und Desktops zu verteilen, den Benutzerzugriff zu authentifizieren und zu verwalten, Verbindungen zwischen Benutzern und ihren virtuellen Desktops und Anwendungen zu vermitteln, Benutzerverbindungen zu optimieren und einen Lastausgleich für die Verbindungen auszuführen.

Der Brokerdienst des Delivery Controllers protokolliert, welche Benutzer wo angemeldet sind, welche Sitzungsressourcen die Benutzer haben und ob Benutzer sich erneut mit vorhandenen Anwendungen verbinden müssen. Der Brokerdienst führt PowerShell-Cmdlets aus und kommuniziert mit einem Brokeragent auf den VDAs über TCP-Port 80. Er kann TCP-Port 443 nicht verwenden.

Der Überwachungsdienst sammelt historische Daten und speichert sie in der Überwachungsdatenbank. Dieser Dienst verwendet TCP-Port 80 oder 443.

Daten aus den Controllerdiensten werden in der Sitedatenbank gespeichert.

Der Controller verwaltet den Zustand von Desktops, startet und hält sie basierend auf dem Bedarf und der administrativen Konfiguration an. In bestimmten Editionen ermöglicht der Controller die Installation der Profilverwaltung, mit der Sie personalisierte Einstellungen in virtualisierten oder physischen Windows-Umgebungen verwalten.

Datenbank:

Mindestens eine Microsoft SQL Server-Datenbank ist pro XenApp- oder XenDesktop-Site zum Speichern der Konfigurations- und Sitzungsinformationen erforderlich. Diese Datenbank speichert die Daten, die von den Diensten des Controllers gesammelt und verwaltet werden. Installieren Sie die Datenbank in Ihrem Datencenter und stellen Sie eine persistente Verbindung mit dem Controller sicher. Die Site umfasst zudem eine Datenbank für die Konfigurationsprotokollierung und eine Überwachungsdatenbank. Standardmäßig werden diese Datenbanken am gleichen Speicherort wie die Sitedatenbank installiert, doch dies können Sie ändern.

Virtual Delivery Agent (VDA):

Der VDA ist auf jeder physischen oder virtuellen Maschine der Site installiert, die Sie Benutzern zur Verfügung stellen möchten. Die Maschinen dienen zur Bereitstellung von Anwendungen oder Desktops. Durch den VDA können sich die Maschinen beim Controller registrieren, sodass sie und die auf ihnen gehosteten Ressourcen Benutzern zur Verfügung gestellt werden können. VDAs erstellen und verwalten die Verbindung zwischen der Maschine und dem Benutzergerät, prüfen, ob eine Citrix Lizenz für den Benutzer oder die Sitzung verfügbar ist und wenden die für die Sitzung konfigurierten Richtlinien an.

Der VDA übermittelt über den Broker Agent Sitzungsinformationen an den Brokerdienst auf dem Controller. Der Brokeragent hostet mehrere Plug-Ins und sammelt Echtzeitdaten. Er kommuniziert mit dem Controller über TCP-Port 80.

Die Bezeichnung "VDA"wird häufig auch für den Agent selbst und die Maschine, auf der er installiert ist, verwendet.

VDAs sind für Windows-Serverbetriebssysteme und Windows-Desktopbetriebssysteme verfügbar. Mit VDAs für Windows-Serverbetriebssysteme können mehrere Benutzer gleichzeitig eine Verbindung mit dem Server herstellen. Mit VDAs für Windows-Desktopbetriebssysteme kann jeweils nur ein Benutzer eine Verbindung zum Desktop herstellen. Linux VDAs sind ebenfalls verfügbar.

Citrix StoreFront:

StoreFront authentifiziert Benutzer für Sites mit Ressourcen und verwaltet Desktops und Anwendungen für den Zugriff durch die Benutzer. Es kann den Unternehmensanwendungsstore hosten, über den Sie Benutzern Self-Service-Zugriff auf Desktops und Anwendungen gewähren. Außerdem werden Anwendungsabonnements, Verknüpfungsnamen und andere Daten der Benutzer gespeichert. Auf diese Weise wird eine konsistente Benutzererfahrung über mehrere Geräte sichergestellt.

Citrix Receiver:

Citrix Receiver wird auf Benutzergeräten und anderen Endpunkten (z. B. virtuellen Desktops) installiert und bietet den Benutzern schnellen, sicheren Self-Service-Zugriff auf Dokumente, Anwendungen und Desktops über beliebige Geräte (Smartphones, Tablets und PCs). Citrix Receiver bietet bedarfsgesteuerten Zugriff auf Windows-, Web- und SaaS-Anwendungen. Bei Geräten, auf denen die Citrix Receiver-Software nicht installiert werden kann, ermöglicht Citrix Receiver für HTML5 eine Verbindung über einen HTML5-kompatiblen Webbrowser.

Citrix Studio:

Studio dient als Verwaltungskonsole zum Konfigurieren und Verwalten der XenApp und XenDesktop-Bereitstellung. Dank Studio sind keine separaten Verwaltungskonsolen für die Verwaltung der Bereitstellung von Anwendungen und Desktops erforderlich. Studio bietet Assistenten, die Ihnen bei der Einrichtung der Umgebung, dem Erstellen der Workloads zum Hosten von Anwendungen und Desktops und beim Zuweisen von Anwendungen und Desktops zu Benutzern behilflich sind. Sie können mit Studio auch Citrix Lizenzen für die Site zuweisen und verfolgen.

Studio erhält die Informationen, die es anzeigt, vom Brokerdienst auf dem Controller und kommuniziert über TCP-Port 80.

Citrix Director:

Director ist ein webbasiertes Tool, mit dem die Support- und Helpdesk-Teams eine Umgebung überwachen, potenziell systembedrohende Probleme rechtzeitig behandeln und Unterstützung für Endbenutzer leisten können. Sie können mit einer Director-Bereitstellung Verbindungen zu mehreren XenApp- oder XenDesktop-Sites herstellen und diese überwachen.

In Director wird Folgendes angezeigt:

Echtzeit-Sitzungsdaten vom Brokerdienst auf dem Controller. Dazu gehören Daten, die der Brokerdienst von dem Brokeragent des VDAs erhält.

Historische Daten der Site vom Überwachungsdienst auf dem Controller.

Daten zum HDX-Datenverkehr (auch ICA-Datenverkehr genannt), die von HDX Insight auf dem NetScaler erfasst werden, wenn die Bereitstellung einen NetScaler und die XenApp- oder XenDesktop-Edition HDX Insight enthält.

Zudem können Sie durch Director auch Benutzersitzungen per Microsoft-Remoteunterstützung anzeigen und steuern.

Citrix Lizenzserver:

Der Lizenzserver verwaltet die Citrix Produktlizenzen. Er kommuniziert mit dem Controller, um die Lizenzierung jeder Benutzersitzung zu verwalten, und mit Studio, um Lizenzdateien zuzuteilen. Sie müssen mindestens einen Lizenzserver zum Speichern und Verwalten Ihrer Lizenzdateien erstellen.

Hypervisor oder Clouddienst:

Der Hypervisor oder Clouddienst hostet die virtuellen Maschinen der Site. Dies können virtuelle Maschinen sein, die Sie zum Hosten von Anwendungen und Desktops verwenden, und solche zum Hosten von XenApp und XenDesktop-Komponenten. Ein Hypervisor wird auf einem Hostcomputer installiert, der nur zur Ausführung des Hypervisors und dem Hosten virtueller Maschinen bestimmt ist.

XenApp und XenDesktop unterstützt diverse Hypervisors und Clouddienste.

Viele XenApp und XenDesktop-Bereitstellungen erfordern zwar einen Hypervisor, für die Bereitstellung von Remote-PC-Zugriff ist jedoch keiner erforderlich. Auch bei Bereitstellung von VMs mit Provisioning Services (PVS) ist kein Hypervisor erforderlich.

Weitere Informationen zu:

- Informationen zu Ports finden Sie unter Netzwerkports.
- Informationen zu Datenbanken finden Sie unter Datenbanken.
- Informationen zu Windows-Diensten in XenApp und XenDesktop-Komponenten finden Sie unter Konfigurieren von Benutzerrechten.
- Informationen zu unterstützten Hypervisors und Clouddiensten finden Sie unter Systemanforderungen.

Zusätzliche Komponenten

XenApp- oder XenDesktop-Bereitstellungen können die folgenden, nicht in der Abbildung oben gezeigten zusätzlichen Komponenten enthalten. Weitere Informationen finden Sie in der Dokumen-

tation dieser Komponenten.

Provisioning Services (PVS):

PVS ist eine optionale Komponente und steht in einigen Editionen zur Verfügung. Es bietet eine Alternative zu MCS für das Provisioning von virtuellen Maschinen. Während MCS Kopien eines Masterimages erstellt, streamt PVS das Masterimage zum Benutzergerät. PVS benötigt hierfür keinen Hypervisor, daher können Sie mit PVS physische Maschinen hosten. PVS kommuniziert mit dem Controller, um Benutzern Ressourcen bereitzustellen.

NetScaler Gateway:

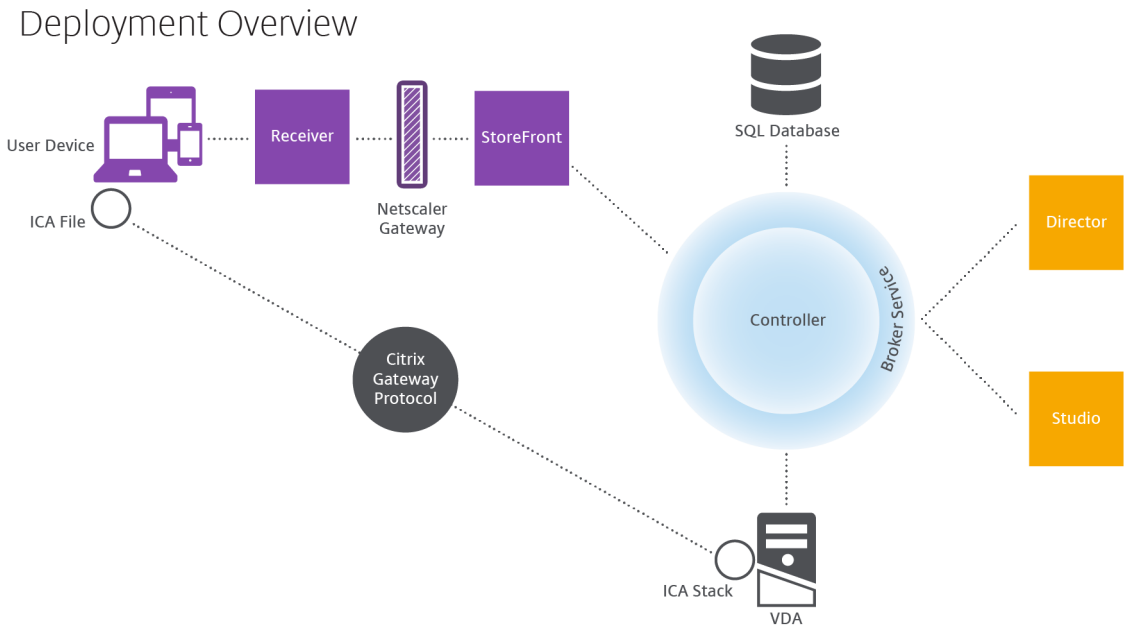
Wenn Benutzer eine Verbindung von außerhalb der Unternehmensfirewall herstellen, können diese Verbindungen in XenApp und XenDesktop mit Citrix NetScaler Gateway (früher "Access Gateway") mit TLS gesichert werden. Das virtuelle NetScaler Gateway- bzw. NetScaler VPX-Gerät ist ein SSL-VPN-Gerät, das in der DMZ bereitgestellt wird und sicheren, zentralen Zugriff über die Unternehmensfirewall bietet.

NetScaler SD-WAN:

Wenn Benutzern an Remotestandorten, wie in Zweigstellen, virtuelle Desktops bereitgestellt werden, kann mit Citrix NetScaler SD-WAN die Leistung optimiert werden. (Früher wurde Citrix CloudBridge, Branch Repeater oder WANScaler verwendet.) Repeater erhöhen die Leistung in WANs. Mit Repeatern im Netzwerk erleben Benutzer in Zweigstellen eine LAN-ähnliche Leistung über das WAN. NetScaler SD-WAN kann verschiedene Bereiche der Benutzererfahrung priorisieren. Ziel einer Priorisierung kann beispielsweise sein, dass die Benutzererfahrung in einer Zweigstelle sich nicht verschlechtert, wenn eine große Datei oder ein großer Druckauftrag über das Netzwerk gesendet wird. HDX WAN-Optimierung bietet Komprimierung mit Token sowie Datendeduplizierung, wodurch die Bandbreitenanforderungen reduziert werden und die Leistung verbessert wird.

Funktionsweise typischer Bereitstellungen

Sites bestehen aus Maschinen mit dedizierten Rollen, die Skalierbarkeit, hohe Verfügbarkeit und Failover gewährleisten und inhärent sicher sind. Eine Site besteht aus Server- und Desktopmaschinen mit installierten VDAs und dem Delivery Controller, der den Zugriff verwaltet.



Durch den VDA können Benutzer Verbindungen mit Desktops und Anwendungen herstellen. Er ist auf Server- oder Desktopmaschinen im Datencenter für die meisten Bereitstellungsmethoden installiert, aber er kann auch auf physischen PCs für Remote-PC-Zugriff installiert werden.

Der Controller besteht aus unabhängigen Windows-Diensten, die Ressourcen, Anwendungen und Desktops verwalten und die Last der Benutzerverbindungen optimieren und ausgleichen. Jede Site hat einen oder mehrere Controller. Da sich Latenz, Bandbreite und Netzwerkzuverlässigkeit auf Sitzungen auswirken, sollten alle Controller idealerweise im gleichen LAN sein.

Benutzer greifen niemals direkt auf den Controller zu. Der VDA dient als Vermittler zwischen den Benutzern und dem Controller. Wenn sich Benutzer über StoreFront bei der Site anmelden, werden ihre Anmeldeinformationen an den Brokerdienst auf dem Controller übermittelt. Der Brokerdienst ruft dann basierend auf den festgelegten Richtlinien die Benutzerprofile und verfügbare Ressourcen ab.

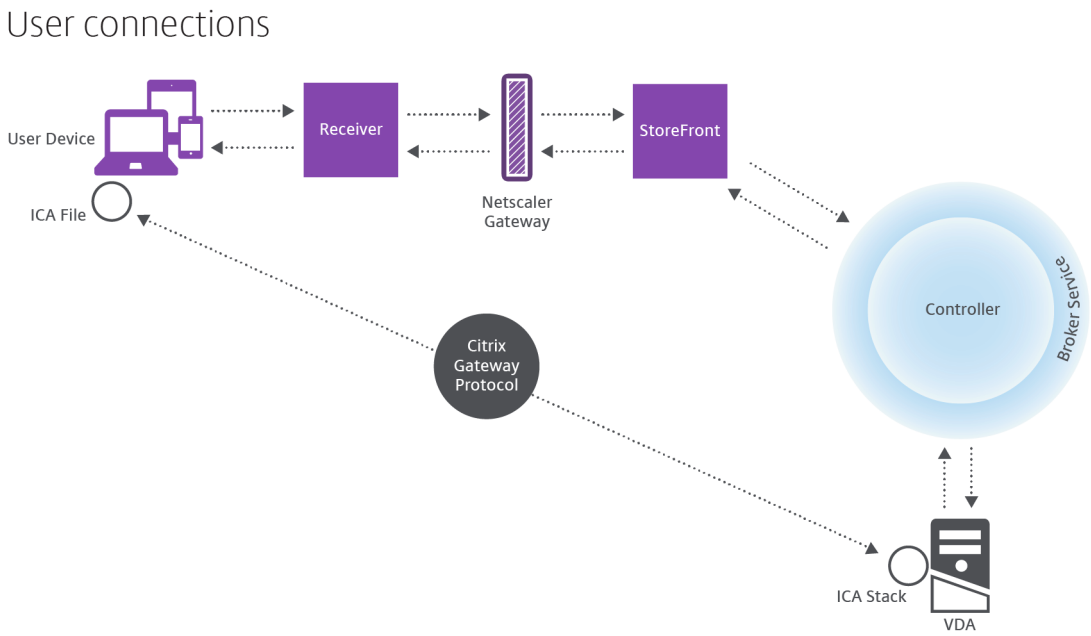
Behandlung von Benutzerverbindungen

Zum Starten einer Sitzung stellt der Benutzer eine Verbindung über Citrix Receiver (auf dem Benutzergerät installiert) oder über eine StoreFront Citrix Receiver für Web-Site her.

Der Benutzer wählt den gewünschten physischen oder virtuellen Desktop oder die gewünschte virtuelle Anwendung.

Die Anmeldeinformationen des Benutzers werden über diesen Weg an den Controller geleitet, der durch Kommunikation mit dem Brokerdienst bestimmt, welche Ressourcen benötigt werden. Citrix

empfiehlt die Installation eines SSL-Zertifikats unter StoreFront, sodass die von Citrix Receiver kommenden Anmeldeinformationen verschlüsselt werden.



Der Brokerdienst bestimmt, auf welche Desktops und Anwendungen der Benutzer zugreifen kann.

Wenn die Anmeldeinformationen geprüft wurden, werden die Informationen zu verfügbaren Anwendungen und Desktops über die StoreFront-Citrix Receiver-Route an den Benutzer gesendet. Wenn der Benutzer Anwendungen oder Desktops aus dieser Liste auswählt, werden diese Informationen wieder an den Controller geleitet. Der Controller bestimmt den richtigen VDA zum Hosten der einzelnen Anwendungen oder Desktops.

Der Controller sendet eine Nachricht mit den Anmeldeinformationen des Benutzers sowie alle Daten zu dem Benutzer und der Verbindung an den VDA. Der VDA akzeptiert die Verbindung und sendet die Informationen über die gleiche Route an Citrix Receiver zurück. Ein Satz erforderlicher Parameter wird in StoreFront gesammelt. Diese Parameter werden dann entweder als Teil der Protokollübermittlung zwischen Receiver und StoreFront an Citrix Receiver gesendet oder sie werden in eine ICA-Datei (Independent Computing Architecture) konvertiert und heruntergeladen. Wenn die Site ordnungsgemäß eingerichtet wurde, sind die Anmeldeinformationen während des gesamten Vorgangs verschlüsselt.

Die ICA-Datei wird auf das Benutzergerät kopiert und richtet eine direkte Verbindung zwischen dem Gerät und dem auf dem VDA ausgeführten ICA-Stack ein. Diese Verbindung umgeht die Verwaltungsinfrastruktur (Citrix Receiver, StoreFront und Controller).

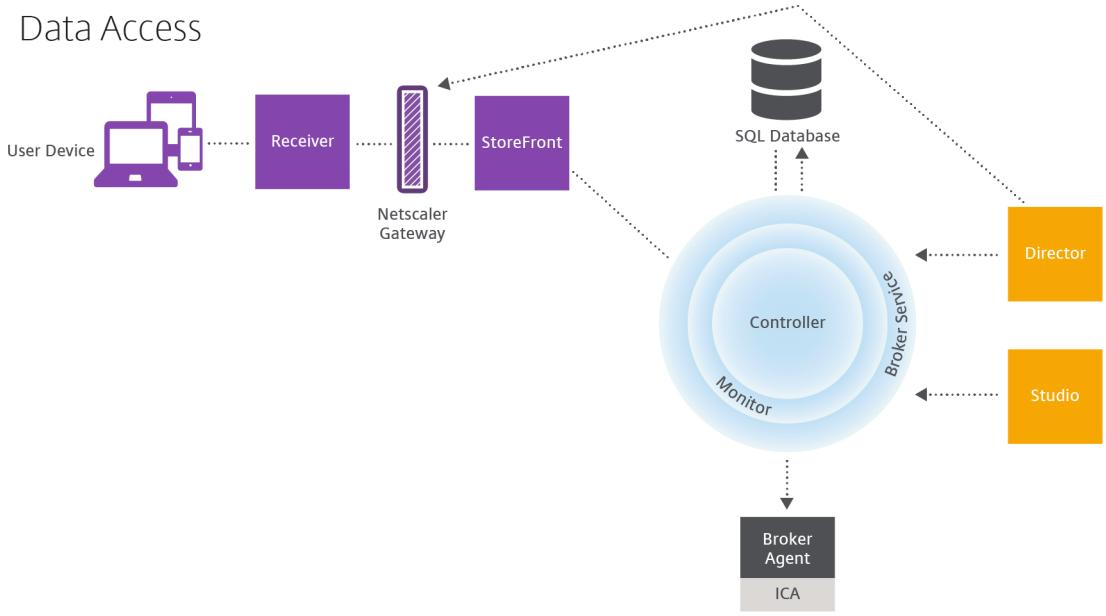
Die Verbindung zwischen Citrix Receiver und dem VDA verwendet das Citrix Gateway Protocol (CGP). Wenn eine Verbindung unterbrochen wird, kann der Benutzer bei aktivierter Sitzungszuverlässigkeit die Verbindung zum VDA wieder herstellen und muss sich nicht über die Verwaltungsinfrastruktur

erneut anmelden. Die Sitzungszuverlässigkeit kann über Citrix Richtlinien aktiviert oder deaktiviert werden.

Wenn der Client eine Verbindung mit dem VDA hergestellt hat, benachrichtigt der VDA den Controller darüber, dass der Benutzer angemeldet ist. Der Controller sendet diese Informationen an die Sitekonfigurationsdatenbank und beginnt mit der Protokollierung der Daten in der Überwachungsdatenbank.

Wie funktioniert der Datenzugriff

Jede Sitzung produziert Daten, auf die die IT-Mitarbeiter über Studio oder Director zugreifen können. Mit Studio können Administratoren auf Echtzeitdaten aus dem Brokeragent zugreifen und damit Sites verwalten. Director greift auf dieselben Echtzeitdaten sowie auf die in der Überwachungsdatenbank gespeicherten historischen Daten zu. Director greift außerdem zur Ermöglichung von Helpdesk-Support und Fehlerbehebung auf HDX-Daten von NetScaler Gateway zu.



Innerhalb des Controllers gibt der Brokerdienst Sitzungsdaten für jede Sitzung auf der Maschine als Echtzeitdaten zurück. Der Überwachungsdienst erfasst ebenfalls die Echtzeitdaten und speichert sie als historische Daten in der Überwachungsdatenbank.

Studio kommuniziert nur mit dem Brokerdienst und greift lediglich auf Echtzeitdaten zu. Director kommuniziert mit dem Brokerdienst (über ein Plug-In im Brokeragent), um auf die Sitedatenbank zuzugreifen.

Director kann zudem auf NetScaler Gateway zugreifen und Informationen zu HDX-Daten abrufen.

Bereitstellen von Desktops und Anwendungen: Maschinenkataloge, Bereitstellungsgruppen und Anwendungsgruppen

Zur Einrichtung der Maschinen für die Bereitstellung von Anwendungen und Desktops verwenden Sie Maschinenkataloge. Anschließend erstellen Sie unter Verwendung einiger oder aller Maschinen in den Maschinenkatalogen Bereitstellungsgruppen, um festzulegen, welche Anwendungen und Desktops bereitgestellt werden sollen und welche Benutzer darauf zugreifen können.

Maschinenkataloge:

Maschinenkataloge sind Sammlungen virtueller oder physischer Maschinen, die Sie als Einheit verwalten. Diese Maschinen und die Anwendungen oder virtuellen Desktops darauf sind die Ressourcen, die Sie den Benutzer bereitstellen. Auf allen Maschinen in einem Maschinenkatalog sind das gleiche Betriebssystem und der gleiche Virtual Desktop Agent (VDA) installiert. Sie enthalten außerdem die gleichen Anwendungen oder virtuellen Desktops.

Normalerweise erstellen Sie ein Masterimage und verwenden es zum Erstellen identischer VMs im Katalog. Für VMs eines Katalogs können Sie die Bereitstellungsmethode festlegen:Citrix Tools (PVS oder MCS) oder andere Tools. Alternativ können Sie eigene Images verwenden. In diesem Fall müssen Sie die Zielgeräte individuell oder kollektiv mit ESD-Tools (Electronic Software Distribution) verwalten.

Gültige Maschinentypen:

- **Serverbetriebssystemmaschinen:** virtuelle oder physische Maschinen, die auf einem Serverbetriebssystem basieren. Sie werden verwendet, um mit XenApp veröffentlichte Anwendungen (serverbasierte, gehostete Anwendungen) und mit XenApp veröffentlichte Desktops (servergehostete Desktops) bereitstellen. Mehrere Benutzer können gleichzeitig eine Verbindung mit diesen Maschinen herstellen.
- **Desktopbetriebssystemmaschinen:** virtuelle oder physische Maschinen, die auf einem Desktopbetriebssystem basieren. Sie werden für die Bereitstellung von (optional personalisierbaren) VDI-Desktops, von über VM gehosteten Anwendungen (Anwendungen von Desktopbetriebssystemen) und gehosteter physischer Desktops verwendet. Nur jeweils ein Benutzer kann eine Verbindung zu einem dieser Desktops herstellen.
- **Remote-PC-Zugriff:** ermöglicht Remotebenutzern den Zugriff auf ihre physischen Büro-PCs über ein beliebiges Gerät mit Citrix Receiver. Die Büro-PCs werden über die XenDesktop-Bereitstellung verwaltet und erfordern eine Positivliste mit Benutzergeräten.

Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Bereitstellungsgruppen:

Über Bereitstellungsgruppen wird angegeben, welche Benutzer Zugriff auf die Anwendungen und/oder Desktops von Maschinen erhalten. Bereitstellungsgruppen enthalten Maschinen aus den Maschinenkatalogen und Active Directory-Benutzer, die Zugriff auf die Site haben. Es kann sinnvoll sein, Benutzer den Bereitstellungsgruppen nach ihrer Active Directory-Gruppe zuzuweisen, da

sowohl Active Directory-Gruppen als auch Bereitstellungsgruppen Methoden sind, um Benutzer mit ähnlichen Anforderungen zu gruppieren.

Jede Bereitstellungsgruppe kann Maschinen aus mehreren Maschinenkatalogen enthalten und jeder Maschinenkatalog kann Maschinen für mehrere Bereitstellungsgruppen beitragen. Eine Maschine kann jedoch nur zu einer Bereitstellungsgruppe gehören.

Sie definieren, auf welche Ressourcen Benutzer in der Bereitstellungsgruppe zugreifen können. Beispiel: Um verschiedene Anwendungen verschiedenen Benutzern bereitzustellen, können Sie alle Anwendungen auf dem Masterimage für einen Maschinenkatalog installieren und dann in diesem Katalog genug Maschinen erstellen, um sie auf mehrere Bereitstellungsgruppen zu verteilen. Anschließend können Sie jede Bereitstellungsgruppe so konfigurieren, dass sie einen anderen Teil der auf den Maschinen installierten Anwendungen bereitstellt.

Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.

Anwendungsgruppen:

Anwendungsgruppen können für die Anwendungsverwaltung und Ressourcensteuerung gegenüber der Verwendung weiterer Bereitstellungsgruppen folgende Vorteile bieten: Mit Tagbeschränkungen können Sie Ihre vorhandenen Maschinen für mehrere Veröffentlichungstasks verwenden und sparen so die Kosten für die Bereitstellung und Verwaltung zusätzlicher Maschinen. Die Verwendung von Tagbeschränkungen kann man sich als Unterteilung (oder Partitionierung) der Maschinen in einer Bereitstellungsgruppe vorstellen. Anwendungsgruppen können auch zur Isolierung von Maschinengruppen in einer Bereitstellungsgruppe zur Problembehandlung nützlich sein.

Weitere Informationen finden Sie unter Erstellen von Anwendungsgruppen.

Active Directory

August 18, 2021

Active Directory ist zum Authentifizieren und Autorisieren erforderlich. Mit der Kerberos-Infrastruktur in Active Directory wird die Authentizität und Vertraulichkeit der Kommunikation zwischen den Delivery Controllern garantiert. Informationen zu Kerberos finden Sie in der Dokumentation von Microsoft.

Der Artikel Systemanforderungen enthält die unterstützten Funktionsebenen für Gesamtstruktur und Domäne. Zur Verwendung der Richtlinienmodellierung muss der Controller unter Windows 2003 oder höher bis Windows Server 2012 R2 ausgeführt werden. Dies wirkt sich nicht auf die Domänenfunktionsebene aus.

Dieses Produkt unterstützt Folgendes:

- Bereitstellungen, in denen die Benutzerkonten und Computerkonten in Domänen in einer einzigen Active Directory-Gesamtstruktur bestehen. Benutzer- und Computerkonten können in beliebigen Domänen in einer Gesamtstruktur bestehen. Alle Domänen- und Gesamtstrukturebenen werden in diesem Bereitstellungstyp unterstützt.
- Bereitstellungen, in denen die Benutzerkonten und die Computerkonten der Controller und virtuellen Desktops in unterschiedlichen Active Directory-Gesamtstrukturen bestehen. Bei diesem Bereitstellungstyp muss eine Vertrauensstellung zwischen den Domänen mit den Computerkonten der Controller und virtuellen Desktops und den Domänen mit den Benutzerkonten bestehen. Sie können Gesamtstruktur- oder externe Vertrauensstellungen verwenden. Alle Domänen- und Gesamtstrukturebenen werden in diesem Bereitstellungstyp unterstützt.
- Bereitstellungen, in denen die Computerkonten für Controller in einer Active Directory-Gesamtstruktur bestehen, die sich von den zusätzlichen Active Directory-Gesamtstrukturen mit den Computerkonten für die virtuellen Desktops unterscheidet. Bei diesem Bereitstellungstyp muss eine bidirektionale Vertrauensstellung zwischen den Domänen mit den Computerkonten der Controller und allen Domänen mit den Computerkonten der virtuellen Desktops bestehen. Bei diesem Bereitstellungstyp müssen alle Domänen mit Computerkonten für Controller oder virtuelle Desktops mindestens auf der Funktionsebene “Windows 2000 native”sein. Alle Funktionsebenen der Gesamtstruktur werden unterstützt.
- Beschreibbarer Domänencontroller. Schreibgeschützte Domänencontroller werden nicht unterstützt.

Virtual Delivery Agents (VDAs) können mit in Active Directory veröffentlichten Informationen die Contoller ermitteln, bei denen sie sich registrieren können (Discovery). Diese Methode wird primär für Abwärtskompatibilität unterstützt und ist nur verfügbar, wenn die VDAs und die Controller in derselben Active Directory-Gesamtstruktur sind. Informationen über diese Discovery-Methode finden Sie unter Active Directory-basierte Discovery und CTX118976.

> **Tipp**
>
> Ändern Sie weder den Computernamen noch die Domänenmitgliedschaft eines Delivery Controllers, nachdem Sie die Site konfiguriert haben.

Bereitstellen in einer Active Directory-Umgebung mit mehreren Gesamtstrukturen

Diese Informationen gelten für Versionen ab XenDesktop 7.1 und XenApp 7.5. Sie gelten nicht für ältere Versionen von XenDesktop und XenApp.

Bei einer Active Directory-Umgebung mit mehreren Gesamtstrukturen und unidirektionalen oder bidirektionalen Vertrauensstellungen können Sie DNS-Weiterleitungen zur Suche und Registrierung von Namen verwenden. Mit dem Assistenten zum Zuweisen der Objektverwaltung können Sie den entsprechenden Active Directory-Benutzern das Erstellen von Computerkonten ermöglichen. Weitere Informationen zu dem Assistenten finden Sie in der Microsoft-Dokumentation.

In der DNS-Infrastruktur sind keine Reverse-DNS-Zonen erforderlich, wenn die entsprechenden DNS-Weiterleitungen zwischen Gesamtstrukturen eingerichtet sind.

Der SupportMultipleForest-Schlüssel ist erforderlich, wenn der VDA und der Controller in unterschiedlichen Gesamtstrukturen eingerichtet sind, unabhängig davon, ob sich die Active Directory- und NetBIOS-Namen voneinander unterscheiden. Der Schlüssel "SupportMultipleForest"ist nur auf dem VDA nötig. Mit den folgenden Informationen fügen Sie einen Registrierungsschlüssel hinzu:

> **Achtung:**
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie ein Backup der Registrierung, bevor Sie sie bearbeiten.

- HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - Name: SupportMultipleForest
  - Typ: REG_DWORD
  - Wert: 0x00000001 (1)

Sie müssen möglicherweise die DNS-Konfiguration umkehren, wenn sich der DNS-Namespace vom Active Directory-Namespace unterscheidet.

Wenn externe Vertrauensstellungen während des Setups vorhanden sind, ist der Registrierungsschlüssel "ListOfSIDs"erforderlich. Der Registrierungsschlüssel "ListOfSIDs"ist auch erforderlich, wenn der vollqualifizierte Domänenname (FQDN) für Active Directory sich vom DNS-FQDN unterscheidet oder die Domäne mit dem Domänencontroller einen anderen NetBIOS-Namen hat als der Active Directory-FQDN. Verwenden Sie zum Hinzufügen des Registrierungsschlüssels die folgenden Informationen:

- Für einen 32-Bit- oder 64-Bit-VDA verwenden Sie folgenden Registrierungsschlüssel: HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs
  - Name: ListOfSIDs
  - Typ: REG_SZ
  - Daten: Sicherheits-ID (SID) der Controller

Wenn externe Vertrauensstellungen vorhanden sind, nehmen Sie die folgenden Änderungen auf dem VDA vor:

1. Navigieren Sie zur Datei: <Programme>\Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config.
2. Erstellen Sie ein Backup der Datei.
3. Öffnen Sie die Datei in einem Textbearbeitungsprogramm, z. B. Editor.
4. Suchen Sie den Text allowNtlm="false"und ändern Sie den Text in allowNtlm="true".

5. Speichern Sie die Datei.

Nach dem Hinzufügen des Registrierungsschlüssels "ListOfSIDs"und der Bearbeitung der Datei brokeragent.exe.config starten Sie den Citrix Desktopdienst neu, um die Änderungen anzuwenden.

In der folgenden Tabelle werden die unterstützten Vertrauenstypen aufgeführt:

Vertrauenstyp	Transitivität	Richtung	In diesem Release unterstützt
Über-/untergeordnet	Transitiv	Bidirektional	Ja
Strukturstamm	Transitiv	Bidirektional	Ja
Externe Schicht	Nicht transitiv	Unidirektional oder bidirektional	Ja
Gesamtstruktur	Transitiv	Unidirektional oder bidirektional	Ja
Verknüpfung	Transitiv	Unidirektional oder bidirektional	Ja
Bereich	Transitiv oder nicht transitiv	Unidirektional oder bidirektional	Nein

Weitere Informationen über komplexe Active Directory-Umgebungen finden Sie unter CTX134971.

Datenbanken

January 6, 2023

XenApp- bzw. XenDesktop-Sites verwenden drei SQL Server-Datenbanken:

- **Site:** (auch "Sitekonfiguration") enthält die Konfiguration der ausgeführten Site sowie den aktuellen Sitzungszustand und Verbindungsinformationen.
- **Konfigurationsprotokollierung:** (auch "Protokollierung") enthält Informationen über Änderungen an der Sitekonfiguration und Administratoraktivitäten. Diese Datenbank wird verwendet, wenn die Konfigurationsprotokollierung aktiviert ist (diese ist standardmäßig aktiviert).
- **Überwachung:** enthält von Director genutzte Daten, z. B. Sitzungs- und Verbindungsinformationen.

Jeder Delivery Controller kommuniziert direkt mit der Sitedatenbank. Die Windows-Authentifizierung ist für Verbindungen zwischen dem Controller und den Datenbanken erforderlich. Ein Controller kann entfernt oder ausgeschaltet werden, ohne dass dies Auswirkungen auf die anderen Controller in der

Site hat. Das bedeutet jedoch, dass die Datenbank einen zentralen Ausfallpunkt bildet. Wenn der Datenbankserver ausfällt, funktionieren vorhandene Verbindungen weiterhin, bis der Benutzer sich abmeldet oder die Verbindung trennt. Informationen zum Verbindungsverhalten, wenn die Sitedatenbank nicht mehr verfügbar ist, finden Sie unter Lokaler Hostcache.

Wenn Sie einer Site einen Delivery Controller hinzufügen, konfigurieren Sie Anmeldeinformationen für diese Maschine auf allen Replikatmaschinen mit SQL Server, die Sie für hohe Verfügbarkeit verwenden.

Citrix empfiehlt, dass Sie regelmäßig ein Backup der Datenbanken durchführen, damit diese bei einem Ausfall des Datenbankservers von dem Backup wiederhergestellt werden können. Die Backupstrategie kann für jede Datenbank anders sein. Anweisungen finden Sie unter CTX135207.

Wenn die Site mehr als eine Zone enthält, muss die Sitedatenbank in der primären Zone residieren. Controller in jeder Zone kommunizieren mit der Datenbank.

Hohe Verfügbarkeit

Es gibt einige Hochverfügbarkeitslösungen, die Sie in Betracht ziehen können, um automatisches Failover zu gewährleisten:

- **AlwaysOn-Verfügbarkeitsgruppen (einschließlich Basic-Verfügbarkeitsgruppen):** Dies ist eine Lösung für hohe Verfügbarkeit und Notfallwiederherstellung, die mit SQL Server 2012 eingeführt wurde. Damit können Sie die Verfügbarkeit für eine oder mehrere Datenbanken maximieren. AlwaysOn-Verfügbarkeitsgruppen erfordern, dass die SQL Server-Instanzen auf Windows Server Failover Clustering-Knoten (WSFC) residieren. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server?redirectedfrom=MSDN&view=sql-server-ver15.
- **Spiegelung der SQL Server-Datenbank:** Dies stellt sicher, dass ein automatisches Failover innerhalb weniger Sekunden stattfindet, falls der aktive Datenbankserver ausfällt. Die Benutzer werden in der Regel also nicht beeinträchtigt. Diese Methode ist teurer als andere Lösungen, da Volllizenzen für SQL Server auf jedem Datenbankserver erforderlich sind. In gespiegelten Umgebungen kann SQL Server Express nicht verwendet werden.
- **SQL-Clustering:** Mit dieser Technologie von Microsoft können Sie einem Server automatisch erlauben, die Aufgaben und Verantwortlichkeiten eines anderen, fehlerhaften Servers zu übernehmen. Es ist jedoch etwas komplizierter, diese Lösung einzurichten. Zudem ist der automatische Failoverprozess in der Regel langsamer als bei anderen Lösungen (etwa der SQL-Spiegelung).
- **Verwenden der Hochverfügbarkeitsfeatures des Hypervisors:** Bei dieser Methode wird die Datenbank als virtuelle Maschine bereitgestellt und die Hochverfügbarkeitsfeatures des Hypervisors werden verwendet. Diese Lösung ist billiger als das Spiegeln, da die bestehende Hypervisorsoftware verwendet wird und Sie zudem SQL Server Express verwenden können. Der

automatische Failoverprozess ist jedoch langsamer, da eine neue Maschine u. U. eine Weile braucht, bis sie gestartet wird, und dadurch auch die Datenbank. Möglicherweise wird also der Dienst für Benutzer unterbrochen.

Das Feature für den lokalen Hostcache ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist. Weitere Informationen finden Sie unter Lokaler Hostcache.

Für den Fall, dass alle Controller einer Site ausfallen, können Sie den Virtual Delivery Agent so konfigurieren, dass er im Hochverfügbarkeitsmodus arbeitet, damit Benutzer weiterhin auf Desktops und Anwendungen zugreifen und diese verwenden können. Im Hochverfügbarkeitsmodus akzeptiert der VDA direkte ICA-Verbindungen von Benutzern anstelle von durch den Controller vermittelten Verbindungen. Verwenden Sie dieses Feature nur in den seltenen Fällen, wenn die Kommunikation mit allen Controllern fehlschlägt. Es ist keine Alternative zu anderen Hochverfügbarkeitslösungen. Weitere Informationen finden Sie unter CTX 127564.

> **Hinweis**
>
> Die Installation eines Controllers auf einem Knoten in einer SQL-Clustering- oder SQL-Spiegelungsinstallation wird nicht unterstützt.

Installieren der Datenbanksoftware

Standardmäßig wird zusammen mit dem ersten Delivery Controller SQL Server Express installiert, wenn keine andere Instanz von SQL Server auf dem Server erkannt wird. Diese Standardaktion reicht im Allgemeinen für Machbarkeitsstudien oder Pilotbereitstellungen aus. SQL Server Express unterstützt jedoch keine Microsoft-Hochverfügbarkeitsfunktionen.

Die Standardinstallation verwendet die Standarddienstkonten und -privilegien von Windows. Informationen zu diesen Standards und dem Hinzufügen von Windows-Dienstkonten zur sysadmin-Rolle finden Sie in der Microsoft-Dokumentation. In dieser Konfiguration verwendet der Controller das Netzwerkdienstkonto. Der Controller erfordert keine weiteren SQL Server-Rollen oder -Berechtigungen.

Bei Bedarf können Sie zum Ausblenden der Datenbankinstanz die Option **Instanz ausblenden** wählen. Geben Sie beim Konfigurieren der Datenbankadresse in Studio die statische Portnummer statt des Namens ein. Informationen zum Ausblenden einer Instanz des SQL Server-Datenbankmoduls finden Sie in der Dokumentation von Microsoft.

In den meisten Produktionsbereitstellungen und in Bereitstellungen, in denen Microsoft-Features für hohe Verfügbarkeit verwendet werden, muss eine andere (unterstützte) SQL Server-Version als SQL Server Express auf den anderen Computern (als dem mit dem ersten Controller) installiert werden.

In dem Artikel über die Systemanforderungen werden die unterstützten SQL Server-Versionen aufgeführt. Die Datenbanken können auf einem oder mehreren Computern residieren.

Stellen Sie sicher, dass die SQL Server-Software installiert ist, bevor Sie eine Site erstellen. Sie müssen keine Datenbank erstellen, wenn Sie es jedoch tun, muss sie leer sein. Außerdem empfiehlt sich das Konfigurieren von Microsoft-Features für hohe Verfügbarkeit.

Halten Sie die SQL Server-Installation mit Windows Update auf dem neuesten Stand.

Einrichten der Datenbanken mit dem Assistenten für die Siteerstellung

Legen Sie Namen und Speicherorte der Datenbanken auf der Seite **Datenbanken** des Assistenten für die Siteerstellung fest. Siehe Datenbankadressformate. Zur Vermeidung von Fehlern bei künftigen Abfragen von Monitor Service durch Director verwenden Sie keine Leerzeichen im Namen der Überwachungsdatenbank.

Die Seite **Datenbanken** bietet zwei Optionen zum Einrichten der Datenbanken: automatisch und Skriptverwendung. Normalerweise können Sie die automatische Erstellung wählen, wenn Sie die erforderlichen Berechtigungen für die Datenbank haben (Studio-Benutzer und Citrix Administrator). Weitere Informationen finden Sie unter "Für die Einrichtung von Datenbanken erforderliche Berechtigungen"weiter unten.

Sie können den Speicherort der Datenbanken für Konfigurationsprotokollierung und Überwachung nach dem Erstellen einer Site ändern. Siehe Ändern des Speicherorts von Datenbanken.

Zum Konfigurieren einer Site für die Verwendung einer gespiegelten Datenbank führen Sie die folgenden Verfahren durch und fahren Sie dann mit der automatischen oder skriptbasierten Einrichtung fort:

1. Installieren Sie SQL Server auf zwei Servern, A und B.
2. Erstellen Sie auf Server A die Datenbank, die als Hauptdatenbank verwendet werden soll. Sichern Sie die Datenbank auf Server A und kopieren Sie sie anschließend auf Server B.
3. Stellen Sie auf Server B die Backupdatei wieder her.
4. Starten Sie die Spiegelung auf Server A.

Um die Spiegelung nach dem Erstellen der Site zu überprüfen, führen Sie das PowerShell-Cmdlet `get-configdbconnection` aus, um sicherzustellen, dass der Failoverpartner in der Verbindungszeichenfolge für die Spiegelung eingerichtet wurde.

Wenn Sie später einen Delivery Controller in einer gespiegelten Datenbankumgebung hinzufügen, verschieben oder entfernen möchten, gehen Sie wie unter "Delivery Controller"beschrieben vor.

Automatische Einrichtung

Wenn Sie die erforderlichen Datenbankberechtigungen haben, wählen Sie auf der Seite **Datenbanken** des Assistenten für die Siteerstellung die Option "Datenbanken mit Studio erstellen und einrichten" und geben Sie die Namen und Adressen der Hauptdatenbanken ein.

Gibt es an einer von Ihnen angegebenen Adresse eine Datenbank, muss sie leer sein. Gibt es an der angegebenen Adresse keine Datenbank, wird eine entsprechende Meldung angezeigt und Sie werden gefragt, ob eine Datenbank erstellt werden soll. Wenn Sie dies bejahen, werden die Datenbanken von Studio automatisch erstellt und die Initialisierungsskripts für die Haupt- und Replikatdatenbanken ausgeführt.

Einrichtung per Skript

Wenn Sie nicht die erforderlichen Datenbankberechtigungen haben, muss eine andere Person mit diesen Berechtigungen, z. B. ein Datenbankadministrator, helfen. Verfahren:

1. Wählen Sie im Assistenten für die Siteerstellung die Option **Skripts generieren**. Es werden insgesamt sechs Skripts für die drei Datenbanken erstellt (eines für jede Hauptdatenbank und eines für jedes Replikat). Sie können den Speicherort für die Skripts festlegen.
2. Geben Sie die Skripts Ihrem Datenbankadministrator. Der Assistent für die Siteerstellung hält an diesem Punkt automatisch an und wenn Sie später zurückkehren, werden Sie aufgefordert, die Siteerstellung fortzusetzen.

Der Datenbankadministrator erstellt dann die Datenbanken. Jede Datenbank muss folgende Merkmale haben:

- Sortierung, die in "_CI_AS_KS"endet. Citrix empfiehlt die Verwendung einer Sortierung, die in "_100_CI_AS_KS"endet.
- Zur Gewährleistung der optimalen Leistung aktivieren Sie den SQL Server-Read-Committed-Snapshot. Weitere Informationen finden Sie unter CTX 137161.
- Features für hohe Verfügbarkeit sollten nach Bedarf konfiguriert werden.
- Zum Konfigurieren der Spiegelung legen Sie für die Datenbank das vollständige Wiederherstellungsmodell fest (Standardeinstellung ist das einfache Wiederherstellungsmodell). Sichern Sie die Hauptdatenbank und kopieren Sie die Backupdatei auf den Spiegelungsserver. Stellen Sie in der Spiegeldatenbank die Backupdatei auf dem Spiegelserver wieder her. Starten Sie dann die Spiegelung auf dem Hauptserver.

Der Datenbankadministrator führt jedes xxx_Replica.sql-Skript mit dem SQLCMD-Befehlszeilenprogramm oder mit SQL Server Management Studio im SQLCMD-Modus in den SQL Server-Datenbankinstanzen mit hoher Verfügbarkeit (sofern konfiguriert) aus und dann jedes xxx_Principal.sql-Skript in den

Hauptinstanzen der SQL Server-Datenbank. Weitere Informationen zu SQLCMD können Sie der Dokumentation von Microsoft entnehmen.

Wenn alle Skripts erfolgreich ausgeführt wurden, übergibt der Datenbankadministrator dem Citrix Administrator die drei Hauptdatenbankadressen.

In Studio werden Sie aufgefordert, die Siteerstellung fortzusetzen, und die Seite **Datenbanken** wird wieder angezeigt. Geben Sie die Adressen ein. Wenn einer der Server mit einer Datenbank nicht erreicht werden kann, wird eine Fehlermeldung angezeigt.

Für die Einrichtung von Datenbanken erforderliche Berechtigungen

Zum Erstellen und Initialisieren der Datenbanken (bzw. zum Ändern des Speicherorts einer Datenbank) müssen Sie lokaler Administrator und Domänenbenutzer sein. Sie benötigen zudem bestimmte SQL Server-Berechtigungen. Die nachfolgend aufgeführten Berechtigungen können über eine Active Directory-Gruppenmitgliedschaft explizit konfiguriert oder erworben werden. Wenn Ihre Studio-Anmeldeinformationen diese Berechtigungen nicht umfassen, werden Sie aufgefordert, Benutzeranmeldeinformationen für SQL Server einzugeben.

Vorgang	Zweck	Serverrolle	Datenbankrolle
Erstellen einer Datenbank	Erstellen einer geeigneten leeren Datenbank	dbcreator	
Erstellen eines Schemas	Erstellen aller dienstspezifischen Schemas und Hinzufügen des ersten Controllers zur Site	securityadmin*	db_owner
Hinzufügen eines Controllers	Hinzufügen eines weiteren Controllers (zusätzlich zum ersten) zur Site	securityadmin*	db_owner
Hinzufügen eines Controllers (Spiegelungsserver)	Hinzufügen einer Controller-Anmeldung zu dem Datenbankserver, der derzeit die Spiegelrolle einer gespiegelten Datenbank hat	securityadmin*	

Vorgang	Zweck	Serverrolle	Datenbankrolle
Controller entfernen	Entfernen eines Controllers von der Site	**	db_owner
Aktualisieren eines Schemas	Anwenden von Aktualisierungen oder Hotfixes auf das Schema		db_owner

* Zwar ist die securityadmin-Serverrolle technisch restriktiver als die sysadmin-Serverrolle, aber in der Praxis ist sie als gleichwertig anzusehen.

** Wenn Sie einen Controller über Desktop Studio oder über mit Desktop Studio oder dem SDK generierten Skripts aus einer Site entfernen, wird die Controller-Anmeldung für den Datenbankserver nicht entfernt. Auf diese Weise wird vermieden, dass eine Anmeldung entfernt wird, die von den Diensten anderer Produkte als XenDesktop auf demselben Computer verwendet wird. Die Anmeldung muss manuell entfernt werden, wenn sie nicht mehr erforderlich ist. Dazu benötigen Sie die Berechtigungen der securityadmin-Serverrolle.

Wenn Sie diese Vorgänge mit Studio ausführen, muss das Benutzerkonto Mitglied der sysadmin-Serverrolle sein.

Datenbankadressformate

Datenbankadressen können in einem der folgenden Formate angegeben werden:

- `ServerName`
- `ServerName\\InstanceName`
- `ServerName,PortNumber`

Geben Sie für AlwaysOn-Verfügbarkeitsgruppen den Listener der Gruppe im Feld “Speicherort”an.

Ändern des Speicherorts von Datenbanken

Nachdem Sie eine Site erstellt haben, können Sie den Speicherort der Datenbanken für Konfigurationsprotokollierung und Überwachung ändern. (Sie können den Speicherort der Sitedatenbank nicht ändern.) Wenn Sie den Speicherort einer Datenbank ändern:

- Die Daten werden nicht aus der bestehenden Datenbank in die neue Datenbank importiert.
- Die Protokolle beider Datenbanken können beim Abrufen von Protokollen nicht aggregiert werden.

- Der erste Protokolleintrag in der neuen Datenbank gibt an, dass eine Datenbankänderung stattfand, die vorherige Datenbank wird jedoch nicht angegeben.

Sie können den Speicherort der Konfigurationsprotokollierungsdatenbank nicht ändern, wenn die verbindliche Protokollierung aktiviert ist.

Ändern des Datenbankspeicherorts

1. Vergewissern Sie sich, dass eine unterstützte Version von Microsoft SQL Server auf dem Server installiert ist, auf dem die Datenbank residieren soll. Richten Sie Features für hohe Verfügbarkeit nach Bedarf ein.
2. Wählen Sie im Studio-Navigationsbereich **Konfiguration** aus.
3. Wählen Sie die Datenbank aus, für die Sie einen neuen Speicherort angeben möchten, und wählen Sie dann im Bereich **Aktionen** die Option **Datenbank ändern**.
4. Geben Sie den neuen Speicherort und den Datenbanknamen ein.
5. Wenn die Datenbank von Studio erstellt werden soll und Sie die notwendigen Berechtigungen haben, klicken Sie auf **OK**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**. Die Datenbank wird dann von Studio automatisch erstellt. Studio versucht, mit Ihren Anmeldeinformationen auf die Datenbank zuzugreifen. Wenn dies fehlschlägt, werden Sie zur Eingabe der Anmeldeinformationen des Datenbankbenutzers aufgefordert. Das Datenbankschema wird dann von Studio in die Datenbank hochgeladen. Die Anmeldeinformationen werden nur für den Zeitraum der Datenbankerstellung gespeichert.
6. Wenn die Datenbank nicht von Studio erstellt werden soll oder Sie die erforderliche Berechtigung nicht haben, klicken Sie auf **Skript generieren**. Die generierten Skripts enthalten Anweisungen, wie Sie die Datenbank und ggf. die Spiegeldatenbank manuell erstellen. Stellen Sie vor dem Hochladen des Schemas sicher, dass die Datenbank leer ist und dass mindestens ein Benutzer Zugriffs- bzw. Änderungsberechtigung für die Datenbank hat.

Weitere Informationen

Dimensionierung der Sitedatenbank und Konfiguration von Verbindungszeichenfolgen bei Verwendung von SQL Server-Lösungen für hohe Verfügbarkeit.

Bereitstellungsmethoden

August 23, 2019

Es ist eine Herausforderung, die Anforderungen aller Benutzer mit einer Virtualisierungsbereitstellung erfüllen. Mit XenApp und XenDesktop können Administratoren die Benutzererfahrungen mit verschiedenen Methoden, die auch als FlexCast-Modelle bezeichnet werden, anpassen.

Diese Bereitstellungsmethoden, von denen jede ihre Vor- und Nachteile hat, bieten die beste Benutzererfahrung für jeden Anwendungsfall.

Mobilisieren von Windows-Anwendungen auf Mobilgeräten:

Touchscreen-Geräte, wie Tablets und Smartphones, sind jetzt Standard in Mobilität. Wenn Windows-basierte Anwendungen auf ihnen ausgeführt werden, die normalerweise auf großen Bildschirmen angezeigt werden und für volle Funktionalität Klicken mit der rechten Maustaste erfordern, können diese Geräte Probleme verursachen.

XenApp mit Citrix Receiver bietet eine sichere Lösung, sodass die Benutzer von Mobilgeräten Zugriff auf alle Funktionen ihrer Windows-basierten Apps haben, ohne dass diese kostenaufwendig für native mobile Plattformen umgeschrieben werden müssen.

Die Bereitstellungsmethode der mit XenApp veröffentlichten Anwendungen verwendet die HDX-Mobiltechnologie, die die mit der Mobilisierung von Windows-Anwendungen assoziierten Probleme löst. Mit dieser Methode können Windows-Anwendungen für die Toucheingabe umgestaltet werden, während Features wie Mehrfingerbewegungen, native Menüsteuerung, Kamera und GPS-Funktionen erhalten bleiben. Viele Touchfeatures sind nativ in XenApp und XenDesktop und zu ihrer Aktivierung sind keine Änderungen am Anwendungsquellcode nötig.

Zu diesen Features gehören Folgende:

- Automatische Anzeige der Tastatur, wenn ein bearbeitbares Feld den Fokus erhält
- Größeres Auswahlsteuerelement ersetzt Windows-Kombinationsfeld-Steuerelement
- Mehrfingergesten, z. B. Vergrößern und Verkleinern mit zwei Fingern
- Trägheitssensitiver Bildlauf
- Touchpad oder direkte Cursornavigation

Verringern der Aktualisierungskosten für PCs:

Das Aktualisieren von physischen Maschinen ist eine große Aufgabe, der sich viele Unternehmen alle drei bis fünf Jahre stellen müssen, besonders, wenn ein Unternehmen bei Betriebssystemen und Anwendungen immer auf dem neuesten Stand sein muss. Wachsende Unternehmen sehen sich zudem hohen Kosten für das Hinzufügen von neuen Maschinen zum Netzwerk gegenüber.

Mit der Bereitstellungsmethode eines VDI mit Personal vDisk können Einzelbenutzern vollständig personalisierte Desktopbetriebssysteme auf jeder Maschine oder jedem Thin Client mit Serverressourcen bereitgestellt werden. Administratoren können virtuelle Maschinen erstellen, deren Ressourcen, z. B. Verarbeitung, Arbeitsspeicher und Speicher, sich im Datencenter des Netzwerks befinden.

Dadurch kann das Leben älterer Maschinen verlängert werden, Software ist auf dem aktuellen Stand und Ausfallzeiten bei Upgrades werden minimiert.

Sicherer Zugriff auf virtuelle Apps und Desktops für Vertragsunternehmen und Partner:

Netzwerksicherheit ist ein wachsendes Problem, besonders bei der Arbeit mit Vertragsunternehmen, Partnern und gelegentlichen Mitarbeitern von Fremdfirmen, die Zugriff auf Unternehmensapps und

Daten benötigen. Die Mitarbeiter benötigen möglicherweise auch leihweise Laptops oder andere Geräte, die zusätzliche Kosten verursachen.

Daten, Anwendungen und Desktops sind bei XenDesktop und XenApp hinter der Firewall des sicheren Netzwerks gespeichert, sodass Endbenutzer nur die Ein - und Ausgabevorgänge der Benutzergeräte wie Tastatureingaben, Mausklicks, Audio und Bildschirmaktualisierungen übermitteln. Durch die Verwaltung dieser Ressourcen in einem Datencenter bieten XenDesktop und XenApp eine sicherere Remotezugriffslösung als das übliche SSL VPN.

Bei einer VDI-Bereitstellung mit Personal vDisk können Administratoren Thin Clients oder die persönlichen Geräte von Benutzern nutzen, indem sie eine virtuelle Maschine auf einem Netzwerkserver erstellen und ein Betriebssystem für einzelne Benutzer anbieten. Auf diese Weise können IT-Abteilungen die Sicherheit gegenüber Mitarbeitern von Vertragsunternehmen aufrechterhalten, ohne zusätzliches teures Gerät kaufen zu müssen.

Beschleunigte Migration:

Beim Wechsel zu einem neuen Betriebssystem kann es eine Herausforderung sein, Legacy- und nicht kompatiblen Anwendungen bereitzustellen.

Mit VM-gehosteten Apps können Benutzer ältere Anwendungen über Citrix Receiver auf der aktualisierten virtuellen Maschine ohne Kompatibilitätsprobleme ausführen. Dadurch haben IT-Mitarbeiter mehr Zeit, Kompatibilitätsprobleme zu testen und zu beheben, Benutzern den Übergang zu erleichtern und die Effizienz bei Helpdeskanrufen zu erhöhen.

Zusätzliche Vorteile bei der Verwendung von XenDesktop während der Migration sind u. a.:

- Reduzierte Komplexität von Desktops
- Verbesserte Steuerung für IT-Mitarbeiter
- Erhöhte Flexibilität der Endbenutzer im Hinblick auf Geräte und Arbeitsplatz

Virtualisierung professioneller 3D-Grafikanwendungen für Designer und Techniker:

Viele Designunternehmen und Herstellerfirmen sind stark auf professionelle 3D-Grafikanwendungen angewiesen. Die Kosten der für diese Art Software erforderlichen leistungsfähigen Hardware sind für diese Unternehmen eine große finanzielle Belastung. Dazu kommen logistische Probleme durch die Freigabe großer Designdateien über FTP, E-Mail und ähnliche Methoden.

Bei der Bereitstellungsmethode mit gehosteten physischen Desktops wird ein Desktopimage auf Arbeitsstationen und Bladeservern bereitgestellt, ohne dass Hypervisors benötigt werden, um grafikintensive 3D-Anwendungen auf einem systemeigenen Betriebssystem auszuführen.

Alle Dateien werden in einem zentralen Datencenter im Netzwerk gespeichert und große Designdateien können schneller und sicherer für andere Benutzer im Netzwerk freigegeben werden, da die Dateien nicht zwischen Arbeitsstationen übertragen werden müssen.

Transformation von Callcentern:

Unternehmen mit großen Callcentern stehen vor der Herausforderung, zu Spitzenzeiten genügend Maschinen und zu anderen Zeiten nicht zu viele Maschinen im Einsatz zu haben.

Die gepoolte VDI-Bereitstellungsmethode bietet dynamischen Zugriff auf einen standardisierten Desktop für viele Benutzer zu minimalen Kosten. Die gepoolten Maschinen werden pro Sitzung der Reihe nach zugeteilt.

Bei diesen virtuellen Maschinen fällt weniger alltägliche Verwaltung an, da während der Sitzung vorgenommene Änderungen verworfen werden, wenn der Benutzer sich abmeldet. Dies erhöht auch die Sicherheit.

Gehostete Desktops sind eine weitere Bereitstellungsmethode, die sich für Callcenter eignet. Bei dieser Methode werden mehrere Benutzerdesktops auf einem serverbasierten Betriebssystem gehostet.

Sie ist kosteneffizienter als die gepoolte VDI-Bereitstellung, aber bei gehosteten Desktops haben Benutzer keine Berechtigungen, um Anwendungen zu installieren, Systemeinstellungen zu ändern oder den Server neu zu starten.

Mit XenApp veröffentlichte Anwendungen und Desktops

August 18, 2021

Verwenden Sie Serverbetriebssystemmaschinen zum Bereitstellen von mit XenApp veröffentlichten Anwendungen und Desktops.

Anwendungsfall:

- Gewünscht wird eine kostengünstige, serverbasierte Bereitstellung, um die Kosten für die Bereitstellung von Anwendungen für eine große Anzahl von Benutzern gering zu halten, und gleichzeitig eine sichere High-Definition-Benutzererfahrung zu bieten.
- Die Benutzer führen vordefinierte Aufgaben aus, es wird keine Personalisierung oder kein Offlinezugriff auf Anwendungen benötigt. Hierzu können aufgabenorientierte Mitarbeiter, wie z. B. Callcenter- und Einzelhandelsarbeitskräfte gehören, oder Benutzer, die Arbeitsstationen gemeinsam verwenden.
- Anwendungstypen: beliebig

Vorteile und Überlegungen:

- Verwaltbare und skalierbare Lösung für das Datenzentrum.
- Kosteneffektivste Lösung für die Anwendungsbereitstellung.
- Gehostete Anwendungen werden zentral verwaltet und Benutzer können die Anwendung nicht ändern, wodurch eine konsistente, sichere und zuverlässige Benutzererfahrung bereitgestellt wird.

- Benutzer müssen online sein, um auf ihre Anwendungen zuzugreifen.

Benutzererfahrung:

- Benutzer fordern eine oder mehrere Anwendungen von StoreFront über ihr Startmenü oder eine von Ihnen vorgegebene URL an.
- Anwendungen werden virtuell bereitgestellt und in High Definition auf Benutzergeräten angezeigt.
- Abhängig von den Profileinstellungen werden Benutzeränderungen gespeichert, wenn die Anwendungssitzung des Benutzers beendet wird. Andernfalls werden die Änderungen werden gelöscht.

Verarbeiten, Hosten und Bereitstellen von Anwendungen:

- Die Anwendungsverarbeitung findet auf den Hostingmaschinen statt, nicht auf den Benutzergeräten. Die Hostingmaschine kann eine physische oder eine virtuelle Maschine sein.
- Anwendungen und Desktops sind auf einer Serverbetriebssystemmaschine gespeichert.
- Maschinen werden über Maschinenkataloge verfügbar gemacht.
- Maschinen aus Maschinenkatalogen sind in Bereitstellungsgruppen organisiert, die Benutzergruppen dieselben Anwendungen bereitstellen.
- Serverbetriebssystemmaschinen unterstützen Bereitstellungsgruppen, die Desktops oder Anwendungen oder beides hosten.

Sitzungsverwaltung und -zuweisung:

- Auf Serverbetriebssystemmaschinen werden mehrere Sitzungen auf einer einzelnen Maschinen ausgeführt, über die mehrere Anwendungen und Desktops an mehrere, gleichzeitig verbundene Benutzer bereitgestellt werden. Jeder Benutzer benötigt eine einzelne Sitzung, um die gehosteten Anwendungen auszuführen.

Beispiel: Ein Benutzer meldet sich an und fordert eine Anwendung an. Eine der Sitzungen auf dieser Maschine ist für die anderen Benutzer nicht mehr verfügbar. Ein zweiter Benutzer meldet sich an und fordert eine Anwendung an, die von dieser Maschine gehostet wird. Eine zweite Sitzung auf derselben Maschine ist damit jetzt nicht verfügbar. Wenn beide Benutzer weitere Anwendungen anfordern, werden keine zusätzlichen Sitzungen benötigt, da ein Benutzer mehrere Anwendungen in der gleichen Sitzung ausführen kann. Wenn zwei weitere Benutzer sich anmelden und Desktops anfordern, und zwei Sitzungen auf derselben Maschine verfügbar sind, hostet diese eine Maschine nun vier Sitzungen für vier verschiedene Benutzer.

- In der Bereitstellungsgruppe, der ein Benutzer zugewiesen ist, wird eine Maschine auf einem Server mit der geringsten Last ausgewählt. Ein Computer mit Sitzungsverfügbarkeit wird nach dem Zufallsprinzip zugewiesen und stellt einem Benutzer bei der Anmeldung Anwendungen bereit.

Bereitstellen mit XenApp veröffentlichter Anwendungen und Desktops

1. Installieren Sie die bereitzustellenden Anwendungen auf einem Masterimage mit einem unterstützten Windows-Serverbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage.
3. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen von Desktops und Anwendungen. Wenn Sie Anwendungen bereitstellen, wählen Sie die gewünschten aus.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.

VM-gehostete Apps

August 18, 2021

Bereitstellen VM-gehosteter Anwendungen über Desktopbetriebssystemmaschinen

Anwendungsfall:

- Gewünscht wird eine clientbasierte Anwendungsbereitstellungslösung, die eine sichere, zentrale Verwaltung bietet und eine große Anzahl von Benutzern pro Hostserver (oder Hypervisor) unterstützt und Benutzern Anwendungen bereitstellt, die problemlos in High Definition angezeigt werden.
- Benutzer sind interne und externe Auftragnehmer, Partner aus Fremdunternehmen und andere vorläufige Teammitglieder. Sie benötigen keinen Offlinezugriff auf gehostete Anwendungen.
- Anwendungsarten: Anwendungen, die möglicherweise nicht gut mit anderen Anwendungen funktionieren oder mit dem Betriebssystem interagieren, z. B. .NET Framework. Dieser Typ von Anwendungen eignet sich gut für das Hosting auf virtuellen Maschinen.

Vorteile und Überlegungen:

- Anwendungen und Desktops auf dem Masterimage werden sicher verwaltet, gehostet und auf Maschinen im Datenzentrum ausgeführt, womit eine kosteneffektivere Lösung für die Anwendungsbereitstellung bereitgestellt wird.
- Die Benutzer können bei der Anmeldung willkürlich einer Maschine in einer Bereitstellungsgruppe zugewiesen werden, die für das Hosting einer Anwendung konfiguriert ist. Sie können auch einem einzelnen Benutzer eine einzelne Maschine für die Anwendungsbereitstellung jedes Mal statisch zuweisen, wenn sich der Benutzer anmeldet. Bei statisch zugewiesenen Maschinen kann der Benutzer eigene Anwendungen auf der virtuellen Maschine installieren und verwalten.
- Das Ausführen mehrerer Sitzungen auf Desktopbetriebssystemmaschinen wird nicht unterstützt. Daher beansprucht jeder Benutzer bei der Anmeldung eine einzelne Maschine innerhalb einer Bereitstellungsgruppe und der Zugriff auf die Anwendungen muss online erfolgen.

- Bei dieser Methode werden die Serverressourcen für die Verarbeitung von Anwendungen sowie der Speicher für die persönlichen vDisks der Benutzer erhöht.

Benutzererfahrung:

Die gleiche nahtlose Anwendungserfahrung wie mit gehosteten, freigegebenen Anwendungen auf Serverbetriebssystemmaschinen.

Verarbeiten, Hosten und Bereitstellen von Anwendungen:

Wie bei Serverbetriebssystemmaschinen, nur dass es sich um virtuelle Desktopbetriebssystemmaschinen handelt.

Sitzungsverwaltung und -zuweisung:

- Desktopbetriebssystemmaschinen führen eine Desktopsitzung von einer Maschine aus. Nur beim Zugriff auf Anwendungen: Ein Benutzer kann mehrere Anwendungen verwenden (und ist nicht auf eine Anwendung eingeschränkt), da das Betriebssystem jede Anwendung als eine neue Sitzung ansieht.
- Innerhalb einer Bereitstellungsgruppe erhalten Benutzer bei der Anmeldung entweder statischen Zugriff auf eine Maschine (d. h. bei jeder Anmeldung die gleiche Maschine) oder es wird ihnen eine Maschine nach Sitzungsverfügbarkeit zugewiesen.

Bereitstellen von VM-gehosteten Apps:

1. Installieren Sie die bereitzustellenden Anwendungen auf einem Masterimage mit einem unterstützten Windows-Desktopbetriebssystem.
2. Erstellen Sie einen Maschinenkatalog für dieses Masterimage oder aktualisieren Sie einen vorhandenen Katalog mit dem Masterimage.
3. Entscheiden Sie beim Definieren der Desktopdarstellung für den Maschinenkatalog, ob Benutzer bei jeder Anmeldung mit einer neuen VM oder mit derselben VM verbunden werden.
4. Erstellen Sie eine Bereitstellungsgruppe zum Bereitstellen der Anwendungen für Benutzer.
5. Wählen Sie in der Liste der installierten Anwendungen die Anwendung aus, die Sie bereitstellen möchten.

Einzelheiten finden Sie in den Artikeln zu Installation und Konfiguration.

Netzwerkports

May 14, 2021

In der folgenden Tabelle sind die Standardnetzwerkports aufgeführt, die von XenApp und XenDesktop Delivery Controllern, Windows-VDAs, Director und dem Citrix Lizenzserver verwendet werden.

Wenn Citrix Komponenten installiert werden, wird standardmäßig die Hostfirewall des Betriebssystems gemäß diesen Standardnetzwerkports aktualisiert.

Eine Übersicht über Kommunikationsports, die in anderen Citrix Technologien und Komponenten verwendet werden, finden Sie unter Von Citrix-Technologien verwendete Kommunikationsports.

Sie benötigen diese Portinformationen eventuell in folgenden Situationen:

- Zum Zwecke der Erfüllung gesetzlicher Auflagen
- Wenn sich zwischen diesen Komponenten und anderen Citrix Produkten eine Netzwerkfirewall befindet, damit Sie diese richtig konfigurieren können
- Wenn Sie anstelle der Firewall des Betriebssystems eine Drittanbieter-Hostfirewall, etwa die eines Antimalware-Pakets, verwenden
- Wenn Sie die Konfiguration der Hostfirewall auf diesen Komponenten ändern (in der Regel Windows-Firewalldienst)
- Wenn Sie Features dieser Komponenten zur Verwendung eines anderen Ports konfigurieren und dann die nicht verwendeten Ports deaktivieren oder sperren möchten (Einzelheiten siehe Dokumentation der jeweiligen Komponente)

Informationen zu Ports für andere Komponenten, z. B. StoreFront oder Provisioning Services, finden Sie im aktuellen Artikel "Systemanforderungen"zu der jeweiligen Komponente.

In der Tabelle sind nur eingehende Ports aufgeführt. Ausgehende Ports werden in der Regel vom Betriebssystem bestimmt und haben andere Nummern. Informationen zu ausgehenden Ports sind in den o. g. Situationen normalerweise nicht erforderlich.

Einige dieser Ports sind bei der Internet Assigned Numbers Authority (IANA) registriert. Informationen zu den Portzuweisungen finden Sie unter https://www.iana.org/assignments/port-numbers. Die Beschreibungen der IANA entsprechen jedoch nicht immer der derzeitigen Nutzung.

Das Betriebssystem auf dem VDA und dem Delivery Controller benötigt außerdem eigene eingehende Ports. Einzelheiten finden Sie in der Microsoft Windows-Dokumentation.

VDA, Delivery Controller und Director

Komponente	Verwendung	Protokoll	Standardport, eingehend	Hinweise
VDA	ICA/HDX	TCP, UDP	1494	EDT erfordert 1494 für UDP. Siehe Einstellungen der Richtlinie "ICA".

Komponente	Verwendung	Protokoll	Standardport, eingehend	Hinweise
VDA	ICA/HDX mit Sitzungszuverlässigkeit	TCP, UDP	2598	EDT erfordert 2598 für UDP. Wenn Multistream und Multiport aktiviert sind, definiert der Administrator die Portnummern für die zusätzlichen drei Streams. Siehe Einstellungen der Richtlinie "ICA".
VDA	ICA/HDX über TLS/DTLS	TCP, UDP	443	Alle Citrix Receiver
VDA	ICA/HDX über WebSocket	TCP	8008	Nur Citrix Receiver für HTML5 und Citrix Receiver für Chrome 1.6 und ältere Versionen
VDA	ICA/HDX Audio über UDP Real-time Transport	UDP	16500..16509	
VDA	ICA/universeller Druckserver	TCP	7229	Wird vom Druckdatenstrom-Listener (CGP) des universellen Druckservers verwendet.

Komponente	Verwendung	Protokoll	Standardport, eingehend	Hinweise
VDA	ICA/universeller Druckserver	TCP	8080	Wird vom Listener des universellen Druckservers für eingehende HTTP/SOAP-Anforderungen verwendet.
VDA	Wake-On-LAN	UDP	9	Energieverwaltung für Remote-PC-Zugriff
VDA	Aktivierungsproxy	TCP	135	Energieverwaltung für Remote-PC-Zugriff
VDA	Delivery Controller	TCP	80	
Delivery Controller	VDA, StoreFront, Director, Studio	TCP	80	
Delivery Controller	StoreFront, Director, Studio über TLS	TCP	443	
Delivery Controller	Delivery Controller, VDA	TCP	89	Lokaler Host-Cache (Diese Verwendung von Port 89 könnte sich in zukünftigen Versionen ändern.)
Delivery Controller	Orchestrierung	TCP	9095	Orchestrierung
Director	Delivery Controller	TCP	80, 443	

Citrix Lizenzierung

Die folgenden Ports werden für die Citrix Lizenzierung verwendet.

Komponente	Verwendung	Protokoll	Standardport, eingehend
Lizenzserver	Lizenzserver	TCP	27000
Lizenzserver	Lizenzserver für Citrix (Vendor Daemon)	TCP	7279
Lizenzserver	License Administration Console	TCP	8082
Lizenzserver	Web Services for Licensing	TCP	8083

HDX

August 18, 2021

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Citrix HDX enthält eine breite Palette an Technologien für eine High-Definition-Benutzererfahrung.

Auf dem Gerät:

HDX nutzt die Computingfähigkeiten der Benutzergeräte und verbessert und optimiert die Benutzererfahrung. Die HDX-Technologie liefert einen gleichmäßigen Empfang von Multimediainhalten auf virtuellen Desktops und in Anwendungen. Mit Workspace Control können Benutzer virtuelle Desktops und Anwendungen anhalten und auf einem anderen Gerät an derselben Stelle weiterarbeiten.

Im Netzwerk:

HDX enthält erweiterte Optimierungs- und Beschleunigungsfunktionen und gewährleistet die beste Leistung in jedem Netzwerk, auch bei Verbindungen mit niedriger Bandbreite und bei WAN-Verbindungen mit hoher Latenz.

HDX-Features passen sich den Änderungen in der Umgebung an. Sie stimmen Lastausgleich und Bandbreite aufeinander ab. Es werden optimale Technologien für die jeweiligen Benutzerszenarios einge-

setzt und zwar sowohl bei lokalem Zugriff auf die Desktops oder Anwendungen im Unternehmensnetzwerk als auch bei Remotezugriff von außerhalb des Unternehmens.

Im Datencenter:

HDX nutzt die Verarbeitungsleistung und die Skalierbarkeit von Servern für eine erweitere Grafikleistung, unabhängig von den Funktionen des Clientgeräts.

Die in Citrix Director bereitgestellte HDX-Kanalüberwachung zeigt den Status der verbundenen HDX-Kanäle auf Benutzergeräten an.

HDX Insight

HDX Insight ist die Integration von NetScaler Network Inspector und Performance Manager in Director. Es erfasst Daten zum ICA-Datenverkehr und bietet eine Dashboardansicht von Echtzeit- und historischen Daten. Dazu gehören die clientseitige und serverseitige ICA-Sitzungslatenz, die Bandbreitennutzung der ICA-Kanäle und die ICA-Roundtrip-Zeit für jede Sitzung.

Erleben von HDX-Funktionen mit Ihrem virtuellen Desktop

- Probieren Sie aus, wie die Flash-Umleitung, eine von drei HDX-Multimediaumleitungstechnologien, die Bereitstellung von Adobe Flash-Multimediainhalt beschleunigt:

  1. Laden Sie Adobe Flash Player herunter (https://get.adobe.com/flashplayer/) und installieren Sie ihn auf dem virtuellen Desktop und dem Benutzergerät.
  2. Klicken Sie auf der Desktop Viewer-Symbolleiste auf **Einstellungen**. Klicken Sie im Dialogfeld "Desktop Viewer-Einstellungen"auf die Registerkarte **Flash** und wählen Sie **Inhalt optimieren**.
  3. Um zu sehen, wie die Flash-Umleitung die Bereitstellung von Flash-Multimediainhalten auf virtuellen Desktops beschleunigt, zeigen Sie auf dem Desktop ein Video von einer Website mit Flash-Videos an, z. B. YouTube. Die Flash-Umleitung erfolgt nahtlos, sodass Benutzer nicht wissen, wenn die Software ausgeführt wird. Sie können überprüfen, ob die Flash-Umleitung ausgeführt wird. Halten Sie hierzu nach einem Farbblock Ausschau, der vorübergehend vor dem Start von Flash Player angezeigt wird, oder klicken Sie mit der rechten Maustaste auf das Video und suchen Sie im Menü den Eintrag "Flash-Umleitung".

- So stellt HDX HD-Audio bereit:

  1. Konfigurieren Sie den Citrix Client für maximale Audioqualität; weitere Informationen hierzu finden Sie in der Citrix Receiver-Dokumentation.
  2. Geben Sie Musikdateien mit einem digitalen Audioplayer (z. B. iTunes) auf dem Desktop wieder.

HDX bietet standardmäßig qualitativ hochwertige Grafiken und Videos, für die meisten Benutzer ist keine Konfiguration erforderlich. Die standardmäßig aktivierten Citrix Richtlinieneinstellungen liefern die beste Lösung für die Mehrheit der Fälle.

- HDX wählt automatisch die beste Bereitstellungsmethode basierend auf Client, Plattform, Anwendung und Bandbreite und nimmt dann selbständig entsprechend der geänderten Bedingungen eine Einstellung vor.
- HDX optimiert die Leistung von 2D- und 3D-Grafiken und Video.
- HDX ermöglicht das Streamen von Multimediadateien für die Benutzergeräte direkt vom Quellenanbieter im Internet oder Intranet, ohne dass der Hostserver beteiligt wird. Wenn die Anforderungen für den clientseitigen Inhaltsabruf nicht erfüllt sind, wird bei der Medienbereitstellung automatisch auf serverseitigen Inhaltsabruf und Multimediaumleitung zurückgegriffen. Normalerweise ist keine Änderung der Richtlinien für die Multimediaumleitung erforderlich.
- HDX stellt hochwertige, auf dem Server wiedergegebene Videoinhalte auf virtuellen Desktops bereit, wenn die Multimediaumleitung nicht verfügbar ist: Zeigen Sie ein Video auf einer Website mit HD-Videos an, z. B. https://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Nützliche Info:

- Informationen zum Support und zu Systemanforderungen für HDX-Features finden Sie unter Systemanforderungen. Sofern nicht anders angegeben, stehen HDX-Features für unterstützte Windows-Serverbetriebssystemmaschinen, Windows-Desktopbetriebssystemmaschinen und Remote-PC-Zugriff-Desktops zur Verfügung.
- Nachfolgend wird beschrieben, wie Sie die Benutzererfahrung weiter optimieren, die Skalierbarkeit verbessern oder die Bandbreitenanforderungen reduzieren können. Weitere Informationen zur Verwendung von Citrix Richtlinien und Richtlinieneinstellungen finden Sie unter Citrix Richtlinien zu diesem Release.
- Vorsicht beim Bearbeiten der Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Einschränkung

Wenn Sie Windows Media Player mit aktivierten Remote-Audio und Video Erweiterungen (RAVE) in einer Sitzung verwenden, mit der rechten Maustaste auf den Videoinhalt klicken und **“Aktuelle Wiedergabe”immer oben anzeigen** wählen, wird ein schwarzer Bildschirm angezeigt.

Automatische Wiederverbindung von Clients und Sitzungszuverlässigkeit

Beim Zugriff auf gehostete Anwendungen oder Desktops können Unterbrechungen der Netzwerkverbindung auftreten. Zur Gewährleistung einer reibungsloseren Wiederverbindung bietet Citrix die automatische Wiederverbindung von Clients und die Sitzungszuverlässigkeit. In der Standardkonfiguration startet die Sitzungszuverlässigkeit gefolgt von der automatischen Wiederverbinden von Clients.

Automatische Wiederverbindung von Clients:

Die automatische Wiederverbindung startet die Clientengine, um die Verbindung mit der getrennten Sitzung wiederherzustellen. Die automatische Wiederverbindung schließt oder trennt die Benutzersitzung, nach der in der Einstellung festgelegten Zeit. Wenn die automatische Wiederverbindung im Gang ist, wird der Benutzer folgendermaßen über die Anwendungs- bzw. Desktopunterbrechung benachrichtigt:

- **Desktops:** Das Sitzungsfenster wird abgeblendet und ein Countdowntimer zeigt die bis zur Wiederverbindung verbleibende Zeit an.
- **Anwendungen:** Das Sitzungsfenster wird geschlossen und ein Dialogfeld mit dem Countdown bis zur Wiederverbindung wird angezeigt.

Bei der automatischen Wiederverbindung des Clients starten Sitzungen und erwarten eine Netzwerkverbindung. Der Benutzer kann während der automatischen Wiederverbindung nicht mit der Sitzung interagieren.

Bei der Wiederverbindung werden die gespeicherten Verbindungsinformationen verwendet. Der Benutzer kann dann normal mit Anwendungen und Desktops interagieren.

Standardeinstellungen der automatischen Wiederverbindung von Clients:

- Timeout beim automatischen Wiederverbinden von Clients: 120 Sekunden
- Automatische Wiederverbindung von Clients: aktiviert
- Authentifizierung bei automatischer Wiederverbindung von Clients: deaktiviert
- Protokollierung der automatischen Wiederverbindung von Clients: deaktiviert

Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients".

Sitzungszuverlässigkeit:

Die Sitzungszuverlässigkeit gewährleistet eine nahtlose Wiederverbindung von ICA-Sitzungen bei Netzwerkunterbrechungen. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der in der Einstellung festgelegte Zeitraum abgelaufen ist. Nach Ablauf des Zeitraums werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird

versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen. Wenn die Sitzungszuverlässigkeit im Gang ist, wird der Benutzer folgendermaßen über die Anwendungs- bzw. Desktopunterbrechung benachrichtigt:

- **Desktops:** Das Sitzungsfenster wird durchscheinend und ein Countdowntimer zeigt die bis zur Wiederverbindung verbleibende Zeit an.
- **Anwendungen:** Das Fenster wird durchscheinend und im Infobereich wird eine Benachrichtigung über die Verbindungsunterbrechung geöffnet.

Bei laufendem Sitzungszuverlässigkeitsverfahren kann der Benutzer nicht mit der ICA-Sitzung interagieren. Benutzeraktionen wie Tastatureingaben werden jedoch für ein paar Sekunden unmittelbar nach der Netzwerkunterbrechung gepuffert und erneut übertragen, wenn das Netzwerk wieder verfügbar ist.

Bei Wiederverbindung fahren Client und Server an dem Punkt des Austauschprotokolls fort, an dem die Verbindung unterbrochen wurde. Das Sitzungsfenster wird wieder normal angezeigt und im Infobereich werden entsprechende Benachrichtigungen für Anwendungen geöffnet.

Standardeinstellungen für die Sitzungszuverlässigkeit

- Sitzungszuverlässigkeit - Timeout: 180 Sekunden
- UI-Transparenzstufe während Wiederverbindung: 80 %
- Sitzungszuverlässigkeit - Verbindungen: aktiviert
- Sitzungszuverlässigkeit - Portnummer: 2598

Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Sitzungszuverlässigkeit".

NetScaler mit automatischer Wiederverbindung von Clients und Sitzungszuverlässigkeit:

Die Sitzungszuverlässigkeit und die automatische Wiederverbindung von Clients funktionieren nicht, wenn Multistream- und Multiport-Richtlinien auf dem Server aktiviert sind und mindestens eine oder folgenden Bedingungen vorliegt:

- Die Sitzungszuverlässigkeit ist unter NetScaler Gateway deaktiviert.
- Ein Failover findet auf dem NetScaler-Gerät statt.
- NetScaler SD-WAN wird mit NetScaler Gateway verwendet.

Tabletmodus für Geräte mit Touchscreen

In der Standardeinstellung wird jedes touchfähige Gerät, das eine Verbindung mit einem Windows 10-VDA herstellt, im Tabletmodus gestartet.

Der Tabletmodus erfordert mindestens Version 7.2 von XenServer. XenServer 7.2 wird im XenDesktop-VDA integriert und der Hypervisor wird geändert, um die virtuellen Firmwareeinstellungen für 2-in-1-Geräte zu ermöglichen. Basierend auf diesem aktualisierten BIOS lädt Windows 10

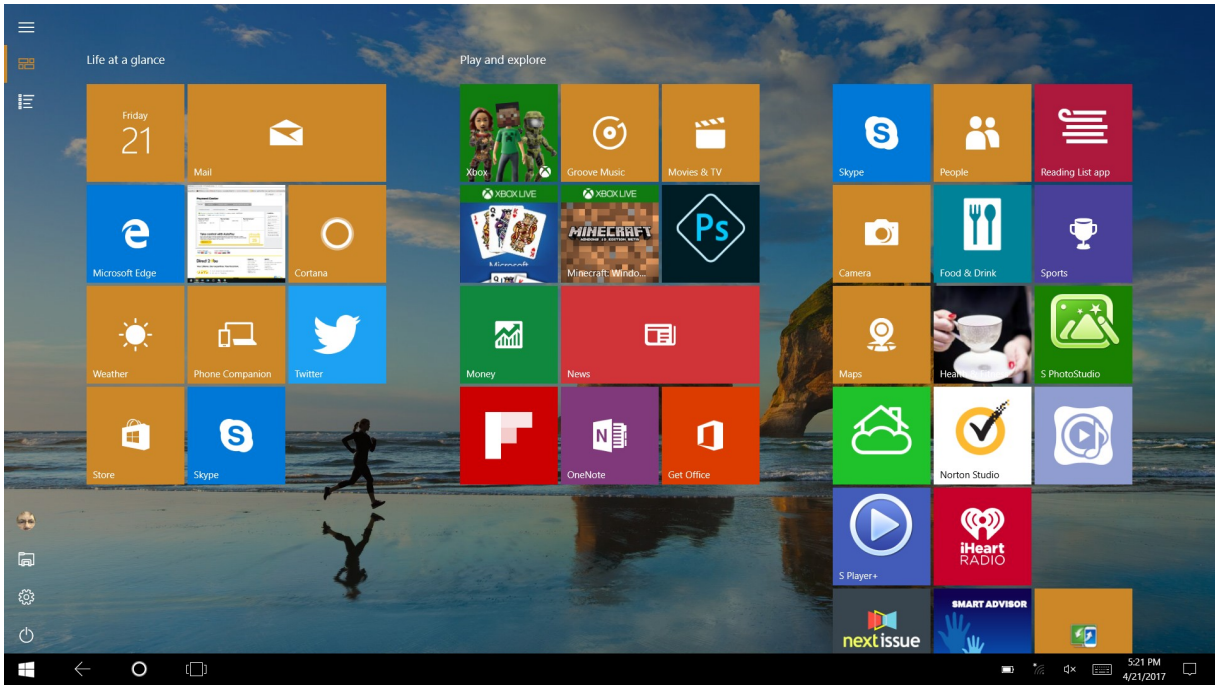
den GPIO-Treiber auf der Ziel-VM. Er wird für die Umschaltung zwischen Tablet- und Desktop-modus innerhalb der virtuellen Maschine verwendet. Weitere Informationen finden Sie unter https:/docs.citrix.com/en-us/xenserver/current-release/downloads/release-notes.pdf.

Der Tabletmodus bietet eine für Touchscreens besser geeignete Benutzeroberfläche:

- Die Schaltflächen sind etwas größer.
- Die Startseite und alle Apps werden im Vollbildmodus geöffnet.
- Die Taskleiste enthält eine Zurück-Schaltfläche.
- Die Taskleiste enthält keine Symbole.

Es besteht Zugriff auf den Datei-Explorer.

Web-Receiver unterstützen den Tabletmodus nicht.



Führen Sie folgenden XenServer CLI-Befehl zum Zulassen der Laptop-/Tablet-Umschaltung aus:

```
xe vm-param-set uuid=\<VM\\_UUID\> platform:acpi\\_laptop\\_slate=1
```

Zum Deaktivieren oder Aktivieren des Tabletmodus konfigurieren Sie die folgende Registrierungsein-stellung unter XenApp und XenDesktop:

HKEY_LOCAL_MACHINE\Software\Citrix\Sessions

Name: CitrixEnhancedUserExperience
Typ: REG_DWORD

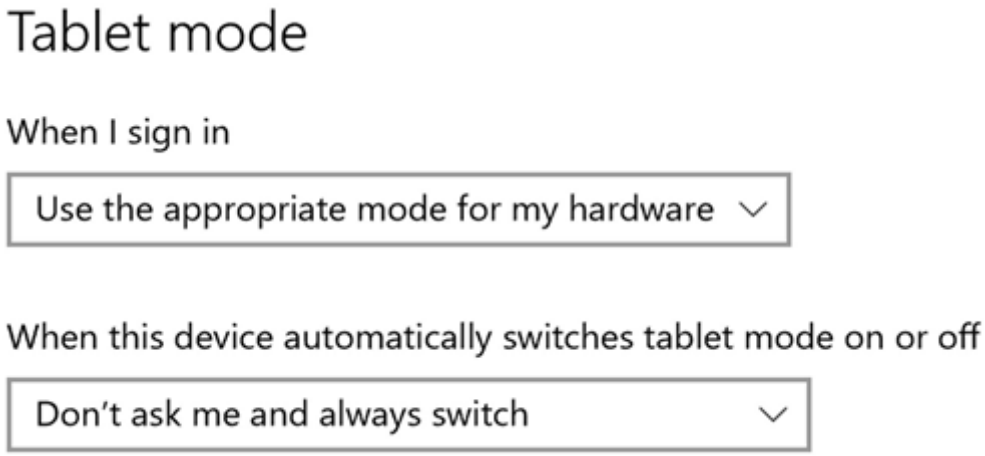
Wert:
0 (deaktivieren)
1 (aktivieren)

Vor dem Start einer Sitzung:

Es wird empfohlen, dass Sie vor dem Starten einer Sitzung auf dem VDA zu **Einstellungen > System > Tabletmodus** navigieren und die folgenden Optionen in den Dropdownlisten festlegen:

- Passenden Modus für meine Hardware verwenden
- Nicht fragen und immer wechseln

Wenn Sie diese Optionen nicht vor dem Start der Sitzung festgelegt haben, legen Sie sie nach dem Start fest und starten Sie dann den VDA neu.



Verbessern der Bildqualität an Benutzergeräten

Die folgenden Richtlinieneinstellungen für "Visuelle Anzeige"steuern die Qualität der Bilder, die von virtuellen Desktops auf Benutzergeräte gesendet werden.

- Bildqualität: steuert die visuelle Qualität der Bilder auf dem Benutzergerät: Mittel, Hoch, Immer verlustfrei, Zu verlustfrei verbessern (Standardeinstellung = Mittel). Die tatsächliche Videoqualität bei der Standardeinstellung "Mittel"hängt von der verfügbaren Bandbreite ab.
- Frameratesollwert: gibt die maximale Anzahl von Frames pro Sekunde an, die vom virtuellen Desktop zum Benutzergerät gesendet werden (Standardwert = 30). Bei Geräten mit langsamen CPUs erzielen Sie durch Festlegen eines niedrigeren Werts eine bessere Benutzererfahrung. Die maximal unterstützte Framerate pro Sekunde ist 60.
- Anzeigespeicherlimit: gibt die maximale Größe des Videopuffers (in Kilobyte) für die Sitzung an (Standardwert = 65536 KB). Für Verbindungen, die eine größere Farbtiefe und eine höhere Auflösung erfordern, erhöhen Sie den Grenzwert. Sie können den maximal erforderlichen Speicher berechnen.

Verbessern der Videokonferenzleistung

Mehrere gebräuchliche Videokonferenzanwendungen wurden für die Multimediaumleitung aus XenApp und XenDesktop optimiert (z. B. HDX RealTime Optimization Pack). Bei nicht optimierten Anwendungen verbessert die HDX-Webcam-Videokomprimierung die Bandbreiteneffizienz und Latenztoleranz für Webcams bei Videokonferenzen. Bei dieser Technologie werden die Webcamdaten über einen dedizierten virtuellen Multimediakanal gestreamt. Die Technologie beansprucht weniger Bandbreite als die isochrone HDX-Plug-n-Play-USB-Umleitung und funktioniert gut über WAN-Verbindungen.

Citrix Receiver-Benutzer können das Standardverhalten außer Kraft setzen, wenn sie in Desktop Viewer unter "Mikrofon & Webcam"die Einstellung **Mikrofon und Webcam nicht verwenden** auswählen. Um zu verhindern, dass Benutzer die HDX-Webcamvideokomprimierung ändern, deaktivieren Sie die Umleitung von USB-Geräten über die Richtlinieneinstellungen unter ICA > USB-Geräte.

HDX-Webcam-Videokomprimierung erfordert, dass die folgenden Richtlinieneinstellungen aktiviert sind (alle sind standardmäßig aktiviert).

- Clientaudioumleitung
- Clientmikrofonumleitung
- Multimediakonferenzen
- Windows Media-Umleitung

Bei Webcams, die H.264-Hardwarecodierung unterstützen, verwendet HDX-Videokomprimierung die Hardwarecodierung standardmäßig. Die Hardwarecodierung kann mehr Bandbreite verbrauchen als die Softwarecodierung. Zum Erzwingen der Softwarekomprimierung fügen Sie dem Registrierungsschlüssel "HKCU\Software\Citrix\HdxRealTime"den folgenden DWORD-Schlüsselwert hinzu: DeepCompress_ForceSWEncode=1.

Prioritäten für den Netzwerkdatenverkehr

Prioritäten für den Netzwerkdatenverkehr über mehrere Verbindungen für eine Sitzung werden zugewiesen, indem QoS-fähige Router verwendet werden. Vier TCP-Streams (real-time, interactive, background und bulk) und zwei UDP-Streams (Voice und Framehawk-Remoting) sind zum Übertragen von ICA-Daten zwischen dem Benutzergerät und dem Server verfügbar. Jeder virtuelle Kanal ist mit einer bestimmten Priorität verknüpft und wird von der entsprechenden TCP-Verbindung transportiert. Sie können die Kanäle basierend auf der Portnummer, die für die Verbindung verwendet wird, unabhängig voneinander festlegen.

Gestreamte Mehrkanalverbindungen werden für Virtual Delivery Agents (VDAs) unterstützt, die auf Windows 10-, Windows 8- und Windows 7-Maschinen installiert sind. Arbeiten Sie mit dem

Netzwerkadministrator Ihres Unternehmens zusammen, um sicherzustellen, dass die in der Einstellung "Multiport-Richtlinie"konfigurierten Common Gateway Protocol (CGP)-Ports auf den Netzwerkroutern richtig zugewiesen sind.

Quality of Service (QoS) wird nur unterstützt, wenn mehrere Sitzungszuverlässigkeitsports oder CGP-Ports konfiguriert sind.

> **Achtung:**
>
> Verwenden Sie Transportsicherheit, wenn Sie dieses Feature einsetzen. Citrix empfiehlt die Verwendung von Internetprotokollsicherheit (IPsec) oder Transport Layer Security (TLS). TLS-Verbindungen werden nur unterstützt, wenn die Verbindungen durch ein NetScaler Gateway passieren, das Multistream-ICA unterstützt. Bei internen Unternehmensnetzwerken werden Multistreamverbindungen mit TLS nicht unterstützt.

Fügen Sie folgende Citrix Richtlinieneinstellungen einer Richtlinie hinzu, um die Servicequalität für mehrere Streamingverbindungen festzulegen (weitere Details finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen"):

- Multiportrichtlinie: Diese Einstellung legt Ports für den ICA-Verkehr über mehrere Verbindungen fest und definiert die Netzwerkpriorität.

  - Wählen Sie in der Liste "CGP-Standardportpriorität"eine Priorität aus. Standardmäßig hat der primäre Port (2598) eine hohe Priorität.
  - Geben Sie in den Feldern "CGP-Port1", "CGP-Port2"und "CGP-Port3"je nach Bedarf zusätzliche CGP-Ports ein und geben Sie entsprechende Prioritäten an. Jeder Port muss eine eindeutige Priorität haben.

  Konfigurieren Sie die Firewalls auf VDAs explizit so, dass zusätzlicher TCP-Datenverkehr zulässig ist.

- Multistreamcomputereinstellung: Diese Einstellung ist standardmäßig deaktiviert. Wenn Sie Citrix NetScaler SD-WAN mit Multistream-Unterstützung in Ihrer Umgebung verwenden, müssen Sie diese Einstellung nicht konfigurieren. Konfigurieren Sie diese Richtlinieneinstellung, wenn Sie Router von Drittanbietern oder Legacy-Branch Repeater verwenden, um die gewünschte Quality of Service (QoS) zu erzielen.
- Multistreambenutzereinstellung: Diese Einstellung ist standardmäßig deaktiviert.

Damit die Richtlinien mit diesen Einstellungen wirksam werden, müssen sich Benutzer abmelden und dann am Netzwerk anmelden.

Unicode-Tastaturzuordnung

Citrix Receiver für andere Betriebssysteme als Windows verwenden das lokale Tastaturlayout (Unicode). Ändert ein Benutzer das lokale Tastaturlayout und das Servertastaturlayout (Scancode), erfolgt möglicherweise keine Synchronisierung und die Ausgabe ist falsch. Beispiel: User1 stellt das lokale Tastaturlayout von Englisch auf Deutsch um. User1 stellt dann die serverseitige Tastatur auf Deutsch um. Obwohl beide Tastaturlayouts auf Deutsch eingestellt wurden, sind sie möglicherweise nicht synchron und verursachen eine falsche Zeichenausgabe.

Aktivieren oder Deaktivieren der Unicode-Tastaturzuordnung:

Das Feature ist VDA-seitig standardmäßig deaktiviert. Zum Aktivieren des Features verwenden Sie den Registrierungs-Editor auf dem VDA.
Erstellen Sie unter HKEY_LOCAL_MACHINE/SOFTWARE/Citrix den Schlüssel "CtxKlMap"ein.
Legen Sie den DWORD-Wert von EnableKlMap auf 1 fest.

Zum Deaktivieren des Features legen Sie den DWORD-Wert von EnableKlMap auf 0 fest oder löschen Sie den Schlüssel "CtxKlMap".

Aktivieren des mit der Unicode-Tastaturzuordnung kompatiblen Modus:

Standardmäßig sorgt bei der Unicode-Tastaturzuordnung automatisch eine Windows-API dafür, dass die neue Unicode-Tastaturzuordnung neu geladen wird, wenn Sie das Tastaturlayout serverseitig ändern. Bei einigen Anwendungen ist die hierfür erforderliche Hook-Einbindung nicht möglich. Sie können Sie das Feature in den kompatiblen Modus versetzen, um Anwendungen ohne Hook zu unterstützen.

1. Leben Sie den DWORD-Wert "DisableWindowHook"des Schlüssels HKEY_LOCAL_MACHINE/SOFTWARE/Citrix auf 1 fest.
2. Legen Sie zur Verwendung der normalen Unicode-Tastaturzuordnung den DWORD-Wert "DisableWindowHook"auf 0 fest.

Verwandte Informationen

- Grafik
- Multimedia
- Allgemeine Inhaltsumleitung
- Adaptiver Transport

Adaptiver Transport

August 15, 2023

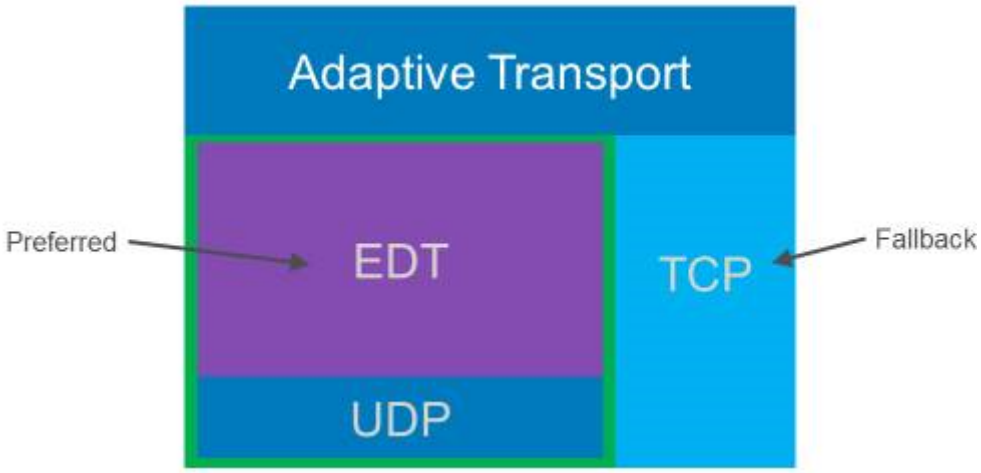
Einführung

Adaptiver Transport ist eine neue Datenübertragungsmethode für XenApp und XenDesktop. Sie ist schneller, skalierbarer, verbessert die Anwendungsinteraktivität und ist bei schwierigen Langstrecken-WAN- und Internetverbindungen interaktiver. Adaptiver Transport bietet eine hohe Serverskalierbarkeit und eine effiziente Bandbreitennutzung. Bei Verwendung des adaptiven Transports reagieren virtuelle ICA-Kanäle automatisch auf veränderliche Netzwerkbedingungen. Sie wechseln automatisch zwischen dem neuen Citrix Protokoll Enlightened Data Transport (EDT) und TCP, um die beste Leistung zu erzielen. Dadurch wird der Datendurchsatz für alle virtuellen ICA-Kanäle, darunter Thinwire-Anzeigeremoting, Dateiübertragung (Clientlaufwerkzuordnung), Drucken und Multimedia-Umleitung verbessert. Dieselbe Einstellung gilt für LAN- und WAN-Bedingungen.

Bei der Einstellung **Bevorzugt** erfolgt der Datentransport primär über EDT mit einem Fallback auf TCP.

Standardmäßig ist adaptiver Transport deaktiviert (**Aus**) und TCP wird immer verwendet.

Zu Testzwecken können Sie **Diagnosemodus** festlegen. Es wird dann nur das EDT-Protokoll ohne Fallback auf TCP verwendet.



Interoperabilität mit Citrix SD-WAN zur WAN-Optimierung

Die WAN-Optimierung (WANOP) mit Citrix SD-WAN ermöglicht eine sitzungsübergreifende tokenbasierte Datenkomprimierung (Deduplizierung), einschließlich des URL-basierten Zwischenspeicherns von Videos. Bei Verwendung von WANOP wird deutlich weniger Bandbreite benötigt, wenn zwei oder mehr Personen am Bürostandort dasselbe Video vom Client abrufen oder große Teile derselben Datei oder desselben Dokuments übertragen oder drucken. Die Prozesse zur ICA-Datenreduktion und Druckauftragskomprimierung auf dem Zweigstellengerät entlasten zudem die VDA-Server-CPU und sorgen für eine bessere Skalierbarkeit von XenApp und XenDesktop-Servern.

> **Wichtig:**
>
> Bei Verwendung von TCP als Datenübertragungsprotokoll unterstützt Citrix WANOP die Optimierungen, die im vorherigen Abschnitt beschrieben wurden. Wählen Sie TCP, wenn Sie Citrix WANOP für Netzwerkverbindungen verwenden. Durch Einsatz der Fluss- und Überlastkontrolle von TCP wird eine äquivalente Interaktivität mit EDT bei hoher Latenz und moderatem Paketverlust sichergestellt.

Anforderungen und Überlegungen

- XenApp und XenDesktop: Mindestversion 7.13
- VDA für Desktop-OS: Mindestversion 7.13
- VDA für Server-OS: Mindestversion 7.13
- StoreFront: Mindestversion 3.9
- Citrix Receiver für Windows: Mindestversion 4.7
- Citrix Receiver für Mac: Mindestversion 12.5
- Citrix Receiver für iOS: Mindestversion 7.2
- Citrix Receiver für Linux: Version 13.6 für direkte VDA-Verbindungen und Version 13.7 für DTLS-Unterstützung mit NetScaler Gateway (oder DTLS für direkte VDA-Verbindungen).
- Citrix Receiver für Android: Version 3.12.3 für direkte VDA-Verbindungen und Version 3.13 für DTLS-Unterstützung mit NetScaler Gateway (oder DTLS für direkte VDA-Verbindungen).
- Nur IPv4 VDAs; IPv6- und heterogene Konfigurationen mit IPv6 und IPv4 werden nicht unterstützt.
- NetScaler: Mindestversion 11.1-51.21. Weitere Informationen zur Konfiguration von NetScaler finden Sie unter Configuring NetScaler Gateway to support Advanced Transport.

Konfiguration

1. Installieren Sie XenApp und XenDesktop.
2. Installieren Sie StoreFront.
3. Installieren Sie den VDA (für Desktop- oder Serverbetriebssysteme).
4. Installieren Sie Citrix Receiver für Windows (oder Citrix Receiver für Mac bzw. für iOS).
5. Aktivieren Sie in Studio die Richtlinieneinstellung “Adaptiver HDX-Transport”(standardmäßig deaktiviert). Citrix empfiehlt außerdem, dieses Feature nicht als universelle Richtlinie für alle Objekte der Site zu aktivieren.
    - Zum Aktivieren der Richtlinieneinstellung legen Sie den Wert auf Bevorzugt fest und klicken Sie dann auf OK.
        - **Bevorzugt:** Nach Möglichkeit wird adaptiver Transport über EDT verwendet, andernfalls erfolgt ein Fallback auf TCP.

  - **Diagnosemodus:** Das EDT-Protokoll wird erzwungen, der Fallback auf TCP ist deaktiviert. Citrix empfiehlt diese Einstellung nur für die Problembehandlung.
  - **Aus.** TCP wird erzwungen und EDT wird deaktiviert.

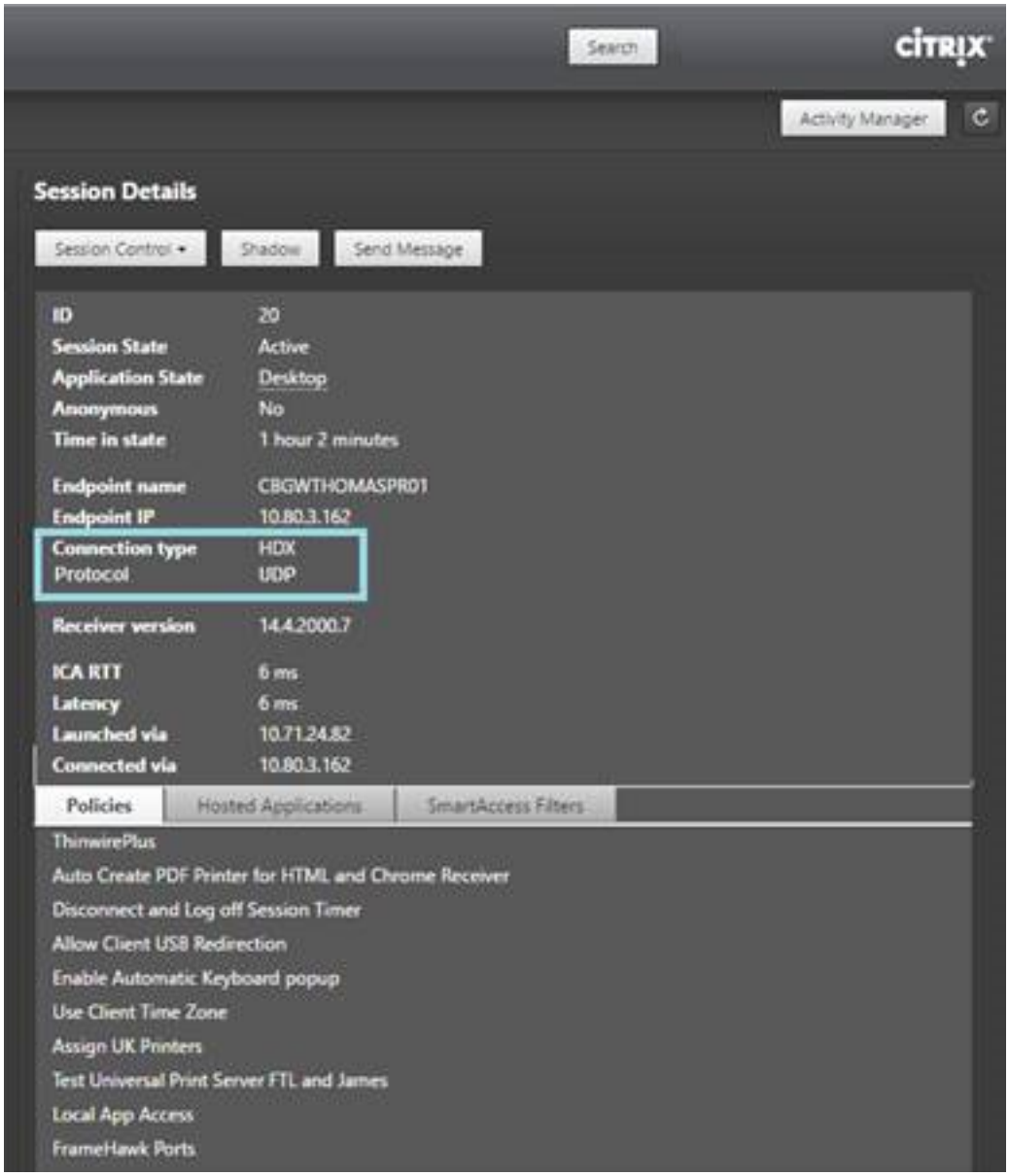
6. Klicken Sie auf "Weiter"und folgen Sie den Anweisungen im Assistenten.
7. Die Richtlinie wird wirksam, wenn die Verbindung mit der ICA-Sitzung wiederhergestellt wird. Optional können Sie **gpupdate/force** ausführen, um die Richtlinieneinstellung auf den Server zu übertragen. Die Benutzer müssen allerdings trotzdem die Verbindung mit der ICA-Sitzung wiederherstellen.
8. Starten Sie eine Sitzung unter einer unterstützten Citrix Receiver-Instanz, um eine Verbindung mit adaptivem Transport herzustellen.
9. Konfigurieren Sie für einen sicheren, externen Zugriff die DTLS-Verschlüsselung auf NetScaler Unified Gateway. Weitere Informationen finden Sie unter Configuring NetScaler Gateway to support Advanced Transport.

Prüfen, ob die Richtlinieneinstellung in Kraft gesetzt wurde

- Prüfen Sie mit netstat -a**, ob die ICA UDP-Dienste (User Datagram Protocol) auf einem VDA aktiviert sind.
- Vergewissern Sie sich, dass die virtuellen Kanäle über EDT laufen: Verwenden Sie hierfür **Director** oder das auf dem VDA verfügbare Befehlszeilenprogramm **CtxSession.exe**.

Beispiel Director:

In Director werden die Richtlinieneinstellungen unter **Sitzungsdetails > Verbindungstyp** angezeigt. Suchen Sie den Verbindungstyp **HDX**. Wird als Protokoll **UDP** angezeigt, ist das EDT-Protokoll für die Sitzung aktiv. Wird **TCP** angezeigt, ist die Sitzung im Fallback- bzw. Standardmodus. Wird als Verbindungstyp **RDP** angezeigt, wird ICA nicht verwendet und es gilt **kein Protokoll**. Weitere Informationen finden Sie unter Überwachen von Sitzungen.



Beispiel mit CtxSession.exe:

Dieses Beispiel zeigt, dass das EDT-Protokoll über UDP für die Sitzung aktiv ist. Geben Sie an der Befehlszeile "CtxSession.exe"ein.

C:\Programme (x86)\Citrix\System32>CtxSession

Session 2 Transport Protocols: UDP > CGP > ICA

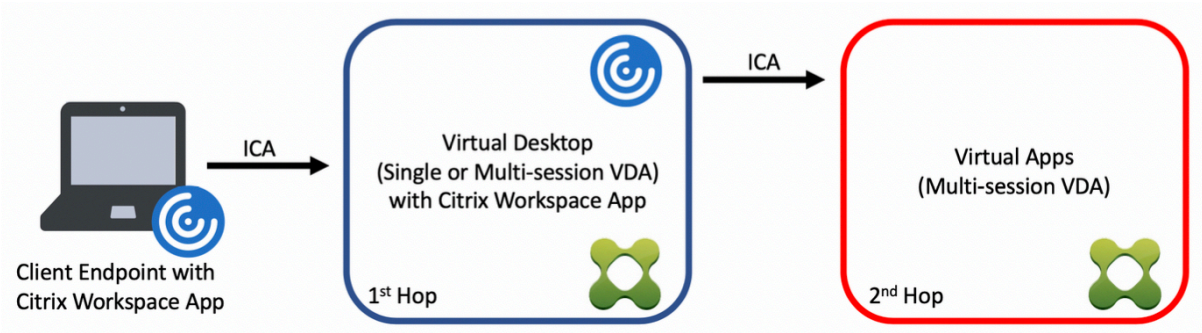
Verwenden Sie zum Anzeigen ausführlicher Statistiken die Option "-v":

```
CtxSession -v
```


Double-Hop in Citrix Virtual Apps and Desktops

May 24, 2024

Im Kontext mit Citrix Clientsitzungen bezieht sich der Begriff “Double-Hop”auf Citrix Virtual Apps-Sitzungen, die in einer Citrix Virtual Desktops-Sitzung ausgeführt werden. Die folgende Abbildung veranschaulicht einen Double-Hop.



Wenn ein Benutzer in einem Double-Hop-Szenario eine Verbindung zu einem virtuellen Citrix Desktop herstellt, der auf einem Einzelsitzungs-OS-VDA ausgeführt wird (“VDI”) bzw. zu einem virtuellen Desktop, der auf einem Multisitzungs-OS-VDA ausgeführt wird (“veröffentlichter Desktop”), gilt dies als erster Hop. Nach Erstellen der Verbindung kann der Benutzer eine Citrix Virtual Apps-Sitzung starten. Dies gilt als zweiter Hop.

Sie können eine Double-Hop-Bereitstellung für verschiedene Anwendungsfälle verwenden. Ein geläufiges Beispiel ist die Verwaltung der Citrix Virtual Desktop- und der Citrix Virtual Apps-Umgebung durch verschiedene Entitäten. Diese Methode kann auch bei der Lösung von Anwendungskompatibilitätsproblemen helfen.

Systemanforderungen

Alle Citrix Virtual Apps and Desktop-Editionen einschließlich Citrix Cloud Service unterstützen Double-Hop.

Der erste Hop muss eine unterstützte Version des VDAs für Einzelsitzungs-OS bzw. Multisitzungs-OS und der Citrix Workspace-App verwenden. Der zweite Hop muss eine unterstützte Version des VDAs für Multisitzungs-OS verwenden. Informationen zu unterstützten Versionen finden Sie in der Produktmatrix.

Zur Gewährleistung der optimalen Leistung und der Kompatibilität empfiehlt Citrix die Verwendung eines Citrix Clients der gleichen Version wie der des VDAs oder einer höheren Version.

Wenn am ersten Hop eine Lösung für virtuelle Desktops eines Drittanbieters (nicht von Citrix) in Kombination mit einer Citrix Virtual Apps-Sitzung beteiligt ist, beschränkt sich die Unterstützung auf die

Citrix Virtual Apps-Umgebung. Bei Problemen im Zusammenhang mit virtuellen Desktops von Drittanbietern (z. B. die Kompatibilität mit der Citrix Workspace-App, die Hardwareumleitung oder die Sitzungsleistung betreffend) kann Citrix nur begrenzt technischen Support leisten. Bei der Problembehandlung ist möglicherweise ein Citrix Virtual Desktop beim ersten Hop erforderlich.

Bereitstellung von HDX in Double-Hop-Szenarien

Generell ist jede Sitzung in einem Double-Hop einmalig und Client-Server-Funktionen sind auf einen Hop isoliert. Dieser Abschnitt enthält Informationen zu Bereichen, die von Citrix Administratoren besonders berücksichtigt werden müssen. Citrix empfiehlt Kunden, die benötigten HDX-Funktionen gründlich zu testen, um eine angemessene Benutzererfahrung und Leistung für die jeweilige Umgebungskonfiguration sicherzustellen.

Grafik

Verwenden Sie Standardgrafikeinstellungen (selektive Codierung) für den ersten und zweiten Hop. Für HDX 3D Pro empfiehlt Citrix dringend die lokale Ausführung aller Anwendungen, für die eine Grafikbeschleunigung erforderlich ist, im ersten Hop, wobei dem VDA die benötigten GPU-Ressourcen zur Verfügung stehen müssen.

Latenz

Die Ende-zu-Ende-Latenz kann sich auf die Benutzererfahrung auswirken. Berücksichtigen Sie die zusätzliche Latenz zwischen dem ersten und dem zweiten Hop. Dies ist besonders wichtig bei der Umleitung von Hardwaregeräten.

Multimedia

Die serverseitige (sitzungsinterne) Wiedergabe von Audio- und Videoinhalten funktioniert am besten im ersten Hop. Eine Videowiedergabe im zweiten Hop erfordert die De- und Recodierung im ersten Hop, wodurch die Bandbreiten- und Hardwareressourcennutzung erhöht wird. Audio- und Videoinhalte müssen möglichst auf den ersten Hop beschränkt werden.

USB-Geräteumleitung

HDX umfasst generische und optimierte Umleitungsmodi zur Unterstützung einer Vielzahl von USB-Gerätetypen. Achten Sie auf den in jedem Hop verwendeten Modus und verwenden Sie die folgende

Tabelle als Referenz für ein optimales Ergebnis. Weitere Informationen zur generischen und optimierten Umleitung finden Sie unter Generische USB-Geräte.

Erster Hop (VDI- oder veröffentlichter Desktop)	Zweiter Hop (virtuelle Apps)	Hinweise zur Unterstützung
Optimiert	Optimiert	Empfohlen (basierend auf Geräteunterstützung). Beispiele: USB-Massenspeicher, TWAIN-Scanner, Webcam, Audio.
Generisch	Generisch	Für Geräte, bei denen die Option "Optimiert" nicht verfügbar ist.
Generisch	Optimiert	Obwohl anders technisch möglich, wird empfohlen, den Modus "Optimiert" für beide Hops zu verwenden, wenn die Geräteunterstützung verfügbar ist.
Optimiert	Generisch	Nicht unterstützt

> Hinweis:
>
> Da USB-Protokolle inhärent gesprächig sind, kann die Leistung über Hops hinweg abnehmen. Funktionalität und Ergebnisse variieren je nach Gerät und Anwendungsanforderungen. Validierungstests werden für jede Geräteumleitung, insbesondere bei Double-Hop-Szenarien, dringend empfohlen.

Ausnahmen bei der Unterstützung

Double-Hop-Sitzungen unterstützen die meisten HDX-Funktionen mit Ausnahme der folgenden:

- Browserinhaltsumleitung
- Lokaler App-Zugriff
- RealTime Optimization Pack für Skype for Business
- Optimierung für Microsoft Teams

Installation und Konfiguration

August 18, 2021

Lesen Sie vor jedem Bereitstellungsschritt die Artikel, auf die verwiesen wird, um sich alle für die Bereitstellung erforderlichen Kenntnisse anzueignen.

Befolgen Sie bei der Bereitstellung von XenApp bzw. XenDesktop nachfolgend aufgeführte Reihenfolge.

Vorbereiten

Lesen Sie den Artikel Vorbereiten der Installation und erledigen Sie alle erforderlichen Aufgaben.

- Informationsquellen zu Konzepten, Features, Unterschieden zu früheren Releases, Systemanforderungen und Datenbanken
- Überlegungen bei der Entscheidung über den Installationsort der Kernkomponenten
- Anforderungen an Berechtigungen und Active Directory
- Informationen zu den Installationsprogrammen, Tools und Schnittstellen

Installieren der Kernkomponenten

Installieren Sie Delivery Controller, Citrix Studio, Citrix Director, Citrix Lizenzserver und Citrix StoreFront. Einzelheiten finden Sie unter Installieren von Kernkomponenten bzw. Installieren über die Befehlszeile.

Erstellen einer Site

Wenn Sie nach der Installation der Kernkomponenten Studio starten, werden Sie automatisch durch die Erstellung einer Site geführt.

Installieren eines oder mehrerer Virtual Delivery Agents (VDAs)

Installieren Sie einen VDA auf einem Windows-Computer, entweder auf dem Masterimage oder direkt auf jeder Maschine. Weitere Informationen finden Sie unter Installieren von VDAs und Installieren über die Befehlszeile. Beispielskripts werden bereitgestellt, wenn Sie die VDAs über Active Directory installieren möchten.

Folgen Sie bei Maschinen mit Linux-Betriebssystem den Anweisungen unter Linux Virtual Delivery Agent.

Installieren Sie für eine Remote-PC-Zugriff-Bereitstellung einen VDA für Desktopbetriebssysteme auf jedem Büro-PC. Wenn Sie nur die VDA-Kerndienste benötigen, verwenden Sie das eigenständige Installationsprogramm VDAWorkstationCoreSetup.exe und Ihre bestehenden ESD-Methoden (Electronic Software Distribution). Unter Vorbereiten der Installation finden Sie ausführliche Informationen zu den VDA-Installationsprogrammen.

Installieren optionaler Komponenten

Wenn Sie den universellen Druckserver von Citrix verwenden möchten, installieren Sie dessen Serverkomponente auf Ihren Druckservern. Weitere Informationen finden Sie unter Installieren von Kernkomponenten und Installieren über die Befehlszeile.

Damit StoreFront Authentifizierungsoptionen wie SAML-Assertions verwenden kann, installieren Sie den Citrix Verbundauthentifizierungsdienst.

Installieren Sie die Self-Service-Kennwortzurücksetzung, um den Benutzern mehr Kontrolle über ihre Benutzerkonten zu gestatten. Einzelheiten finden Sie in der Dokumentation zur Self-Service-Kennwortzurücksetzung.

Sie können auch weitere Citrix Komponenten in die XenApp- oder XenDesktop-Bereitstellung integrieren.

- Provisioning Services ist eine optionale Komponente von XenApp und XenDesktop, mit der Maschinen durch das Streaming eines Masterimages auf die Zielgeräte bereitgestellt werden.
- Citrix NetScaler Gateway ist eine sichere Anwendungszugriffslösung, die Administratoren durch Richtlinien auf Anwendungsebene und durch Aktionssteuerung ermöglicht, den Zugriff auf Anwendungen und Daten zu sichern.
- Citrix NetScaler SD-WAN bietet eine Reihe von Geräten, die die WAN-Leistung optimieren.

Installationsanweisungen finden Sie in der Dokumentation für die jeweiligen Komponenten.

Erstellen eines Maschinenkatalogs

Nachdem Sie eine Site in Studio erstellt haben, werden Sie durch das Erstellen eines Maschinenkatalogs geführt.

Ein Katalog kann physische oder virtuelle Maschinen (VMs) enthalten. Virtuelle Maschinen können aus einem Masterimage erstellt werden. Wenn Sie einen Hypervisor oder Clouddienst zum Bereitstellen von VMs verwenden möchten, erstellen Sie zuerst ein Masterimage auf dem betreffenden Host. Bei der Erstellung des Katalogs geben Sie dann das Image an, das zum Erstellen von VMs verwendet werden soll.

Erstellen einer Bereitstellungsgruppe

Nachdem Sie den ersten Maschinenkatalog in Studio erstellt haben, werden Sie durch das Erstellen einer Bereitstellungsgruppe geführt.

Bereitstellungsgruppen steuern, welche Benutzer auf Maschinen in einem Katalog zugreifen können und welche Anwendungen ihnen zur Verfügung stehen.

Erstellen einer Anwendungsgruppe (optional)

Nachdem Sie eine Bereitstellungsgruppe erstellt haben, können Sie wahlweise eine Anwendungsgruppe erstellen. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden.

Vorbereiten der Installation

January 6, 2023

Die Bereitstellung von XenApp und XenDesktop beginnt mit der Installation der nachstehenden Komponenten. Bei diesem Verfahren wird die Bereitstellung von Anwendungen und Desktops für Benutzer *innerhalb* der Firewall vorbereitet.

- Mindestens einen Delivery Controller
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Citrix Lizenzserver
- Mindestens einen Citrix Virtual Delivery Agent (VDAs)
- Optionale Komponenten und Technologien wie z. B. den universellen Druckserver, den Verbundauthentifizierungsdienst und die Self-Service-Kennwortzurücksetzung

Installieren und konfigurieren Sie für Benutzer *außerhalb* Ihrer Firewall eine zusätzliche Komponente wie NetScaler. Eine Einführung in die Verwendung von NetScaler mit StoreFront finden Sie unter Integrieren von NetScaler Gateway in XenApp und XenDesktop.

Installationsmethoden

Mit dem Produktinstallationsprogramm auf dem XenApp- und XenDesktop-ISO-Image können Sie viele Komponenten und Technologien installieren. VDAs können Sie mit dem eigenständigen VDA-

Installationsprogramm installieren. Alle Installationsprogramme bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle. Informationen finden Sie unter Installationsprogramme.

Das Produkt-ISO-Image enthält Beispielskripts, um VDAs für Maschinen in Active Directory zu installieren, zu aktualisieren oder zu entfernen. Sie können die Skripts auch zum Verwalten von Masterimages einsetzen, die von den Maschinenerstellungsdiensten und Provisioning Services verwendet werden. Weitere Informationen finden Sie unter Installieren von VDAs mit Skripts.

Als automatisierte Alternative zu den Installationsprogrammen verwendet Citrix Smart Tools Blueprints zum Erstellen einer XenApp- und XenDesktop-Bereitstellung. Einzelheiten finden Sie in der Smart Tools-Produktdokumentation.

Vor Installation zu lesende Informationen

- Technischer Überblick: Wenn Sie mit dem Produkt und den Komponenten nicht vertraut sind.
- Änderungen in 7.x: Wenn Sie ein Upgrade einer XenApp-Version 6.x oder von XenDesktop 5.6 auf die aktuelle Version planen.
- Sicherheit: Wenn Sie Ihre Bereitstellungsumgebung planen.
- Bekannte Probleme: Probleme, die in dieser Version auftreten können.
- Datenbanken: Informationen über die Systemdatenbanken und deren Konfiguration. Bei der Installation des Controllers können Sie SQL Server Express zur Verwendung als Sitedatenbank installieren. Das Gros der Datenbankinformationen konfigurieren Sie beim Erstellen einer Site, nachdem Sie die Kernkomponenten installiert haben.
- Remote-PC-Zugriff: Wenn Sie eine Umgebung bereitstellen, in der Benutzer remote auf ihre physischen Maschinen im Büro zugreifen können.
- Verbindungen und Ressourcen: Wenn Sie virtuelle Maschinen (VM) zum Hosten von Anwendungen und Desktops mit einem Hypervisor oder Clouddienst hosten. Die erste Verbindung können Sie beim Erstellen einer Site (nachdem Sie die Kernkomponenten installiert haben) konfigurieren. Richten Sie zu einem beliebigen Zeitpunkt vor Konfigurieren der Verbindung die Virtualisierungsumgebung ein.
- Microsoft System Center Configuration Manager: Wenn Sie den Zugriff auf Anwendungen und Desktops mit ConfigMgr verwalten oder Wake-On-LAN mit Remote-PC-Zugriff verwenden.

Installationsorte

Informationen zu den unterstützten Betriebssystemen, Plattformen und Versionen finden Sie unter Systemanforderungen. Die Komponentenvoraussetzungen werden automatisch installiert. Ausnahmen werden aufgeführt. In der Dokumentation zu Citrix StoreFront und Citrix Lizenzserver finden Sie Angaben zu den unterstützten Plattformen und Voraussetzungen.

Sie können die Kernkomponenten auf dem gleichen Server oder auf unterschiedlichen Servern installieren.

- Die Installation aller Kernkomponenten auf einem Server ist für Machbarkeitsstudien, Test- oder kleine Produktionsbereitstellungen geeignet.
- Zur Ermöglichung einer potenziellen Erweiterung der Bereitstellung in der Zukunft sollten Sie die Komponenten auf separaten Servern installieren. Wenn Sie beispielsweise Studio auf einer anderen Maschine als den Controller installieren, gestattet der Controller die Remoteverwaltung der Site.
- Für die meisten Produktionsbereitstellungen wird die Installation der Kernkomponenten auf separaten Servern empfohlen.

Sie können einen Delivery Controller und einen VDA für Serverbetriebssysteme auf demselben Server installieren. Starten Sie das Installationsprogramm und wählen Sie den Delivery Controller sowie alle weiteren gewünschten Kernkomponenten für diese Maschine. Starten Sie dann das Installationsprogramm noch einmal und wählen Sie den Virtual Delivery Agent für Serverbetriebssysteme.

Stellen Sie sicher, dass für jedes Betriebssystem die neuesten Updates ausgeführt wurden. Die Installation eines Controllers unter Windows Server 2012 R2 oder eines VDAs unter Windows 8.1 oder Windows Server 2012 R2 schlägt beispielsweise fehl, wenn Windows KB2919355 nicht installiert ist.

Stellen Sie sicher, dass bei allen Maschinen die Systemuhren synchronisiert sind. Die Kerberos-Infrastruktur, die die Kommunikation zwischen den Maschinen sichert, muss synchronisiert werden.

Optimierungsempfehlungen für Windows 10-Maschinen finden Sie unter CTX216252.

NICHT zur Installation geeignete Orte

- Installieren Sie keine Komponenten auf einem Active Directory-Domänencontroller.
- Die Installation eines Controllers auf einem Knoten in einer SQL-Cluster- oder Spiegelungsinstallation oder auf einem Server mit Hyper-V wird nicht unterstützt.
- Installieren Sie Studio nicht auf einem Server, auf dem XenApp 6.5 Feature Pack 2 für Windows Server 2008 R2 oder eine frühere Version von XenApp ausgeführt wird.

Berechtigungen und Active Directory-Anforderungen

Auf den Maschinen, auf denen Sie die Komponenten installieren, müssen Sie Domänenbenutzer und lokaler Administrator sein.

Für die Installation mit dem eigenständigen Installationsprogramm benötigen Sie erhöhte Administratorprivilegien oder verwenden Sie die Option **Als Administrator ausführen**.

Konfigurieren Sie die Active Directory-Domäne vor Beginn der Installation.

- Unter Systemanforderungen sind die unterstützten Active Directory-Funktionsebenen aufgeführt. Weitere Informationen finden Sie unter Active Directory.
- Sie müssen mindestens einen Domänencontroller mit Active Directory-Domänendiensten ausführen.
- Installieren Sie keine XenApp- bzw. XenDesktop-Komponenten auf einem Domänencontroller.
- Verwenden Sie keinen Schrägstrich (/), wenn Sie in Studio Namen für Organisationseinheiten festlegen.

Wenn Sie den Citrix Lizenzserver installieren, wird das hierfür verwendete Windows-Benutzerkonto automatisch als Volladministrator für die delegierte Administration auf dem Lizenzserver konfiguriert.

Weitere Informationen:

- Optimale Verfahren zur Sicherheit
- Delegierte Administration
- Dokumentation von Microsoft zur Konfiguration von Active Directory

Installationsleitfaden, Überlegungen und bewährte Methoden

Bei der Installation aller Komponenten

Normalerweise werden Voraussetzungen vom Installationsprogramm installiert, sofern sie nicht vorhanden sind. Nach der Installation einiger Voraussetzungen ist ein Neustart des Computers erforderlich.

Geben Sie beim Erstellen von Objekten vor, während und nach der Installation eindeutige Namen für jedes Objekt ein. Geben Sie z. B. eindeutige Namen für die Netzwerke, Gruppen, Kataloge und Ressourcen ein.

Bei Installationsproblemen wird die Installation angehalten und eine Fehlermeldung angezeigt. Komponenten, die erfolgreich installiert werden, bleiben gespeichert. Sie müssen nicht neu installiert werden.

Wenn Sie die Komponenten installieren (oder aktualisieren), werden automatisch Analysedaten gesammelt. Standardmäßig werden die Daten automatisch an Citrix hochgeladen, wenn die Installation abgeschlossen ist. Bei der Installation von Komponenten werden Sie außerdem automatisch beim Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) angemeldet, in dessen Rahmen anonyme Daten hochgeladen werden. Während der Installation können Sie wahlweise auch die Teilnahme bei anderen Citrix Programmen (z. B. Smart Tools) aktivieren, die Diagnosedaten zur Wartung und Problembehandlung erfassen. Informationen zu diesen Programmen finden Sie unter Citrix Insight Services.

Bei der VDA-Installation

Zusammen mit einem VDA wird standardmäßig Citrix Receiver für Windows installiert, außer bei Verwendung des Installationsprogramms VDAWorkstationCoreSetup.exe. Sie können Citrix Receiver von der Installation ausschließen. Sie oder die Benutzer können Citrix Receiver und anderen Receiver-Versionen von der Citrix Website herunterladen und installieren bzw. aktualisieren. Alternativ können Sie diese Citrix Receiver über StoreFront-Server zur Verfügung stellen.

Der Druckspoolerdienst ist auf den unterstützten Windows-Servern standardmäßig aktiviert. Ist dieser Dienst deaktiviert, können Sie keinen VDA für Windows-Serverbetriebssysteme installieren. Stellen Sie daher vor der VDA-Installation sicher, dass der Dienst aktiviert ist.

Bei den meisten unterstützten Windows-Editionen ist Microsoft Media Foundation bereits installiert. Wenn Media Foundation auf der Maschine, auf der Sie einen VDA installieren, nicht installiert ist (z. B. N-Editionen), werden mehrere Multimediafeatures nicht installiert und sind nicht funktionsfähig. Sie können diese Einschränkung bestätigen oder die VDA-Installation beenden und später, nach der Installation von Media Foundation neu beginnen. Diese Auswahl wird bei der grafischen Oberfläche per Meldung angeboten. In der Befehlszeile können Sie zum Bestätigen der Einschränkung "/no_mediafoundation_ack"verwenden.

Wenn Sie VDA installieren, wird automatisch eine neue lokale Benutzergruppe namens Benutzer mit direktem Zugriff erstellt. Auf VDAs für Desktopbetriebssysteme gilt diese Gruppe nur für RDP-Verbindungen. Auf VDAs für Serverbetriebssysteme gilt diese Gruppe nur für ICA- und RDP-Verbindungen.

Der VDA benötigt gültige Controlleradressen für die Kommunikation. Andernfalls können Sitzungen nicht eingerichtet werden. Sie können Controlleradressen bei der Installation des VDAs oder später festlegen. Sie dürfen es nur nicht vergessen.

Neustarts während und nach der VDA-Installation

Bei der VDA-Installation ist zum Abschluss ein Neustart erforderlich. Das Neustart erfolgt standardmäßig automatisch.

Um während der Installation möglichst wenige Neustarts durchführen zu müssen, führen Sie folgende Schritte aus:

- Stellen Sie vor der VDA-Installation sicher, dass eine unterstützte .NET Framework-Version installiert ist.
- Installieren und aktivieren Sie auf Windows-Serverbetriebssystemmaschinen vor der VDA-Installation die Rollendienste für Remotedesktopdienste.

Wenn Sie diese Voraussetzungen nicht vor dem VDA installieren:

- Wenn Sie die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle ohne /noreboot verwenden, wird die Maschine nach Installation der Voraussetzung automatisch neu gestartet.
- Wenn Sie die Befehlszeilenschnittstelle mit /noreboot verwenden, müssen Sie den Neustart selbst ausführen.

Führen Sie nach jedem Neustart das Installationsprogramm oder den Befehl erneut aus, um die VDA-Installation fortzusetzen.

Installationsprogramme

Komplettinstallationsprogramm

Mit dem im XenApp- und XenDesktop-ISO-Image enthaltenen Komplettinstallationsprogramm können Sie:

- Kernkomponenten von XenApp und XenDesktop (Delivery Controller, Studio, Director, StoreFront und Lizenzserver) installieren, aktualisieren oder entfernen
- Windows-VDAs für Server- oder Desktopbetriebssysteme installieren oder aktualisieren
- Ups Server-Komponente des universellen Druckservers auf den Druckservern installieren
- Verbundauthentifizierungsdienst installieren
- Self-Service-Kennwortzurücksetzung installieren

Zum Bereitstellen eines Desktops von einem Serverbetriebssystem für einen Benutzer (z. B. zur Webentwicklung) verwenden Sie die Befehlszeilenschnittstelle des Produktinstallationsprogramms. Weitere Informationen finden Sie unter Server-VDI.

Eigenständige VDA- Installationsprogramme

Eigenständige VDA- Installationsprogramme stehen auf den Citrix Downloadseiten zur Verfügung. Die eigenständigen VDA-Installationsprogramme sind wesentlich kleiner als das vollständige ISO-Image. Sie eignen sich besser für Bereitstellungen, auf die Folgendes zutrifft:

- Verwenden lokal bereitgestellte oder kopierte ESD-Pakete (Electronic Software Distribution)
- Umfassen physische Maschinen
- Umfassen Remotestandorte

Standardmäßig werden die Dateien im selbstextrahierenden Paket für VDAs in den Ordner Temp extrahiert. Zum Extrahieren in den Ordner Temp wird auf der Maschine mehr Speicherplatz beansprucht, als wenn Sie das Produktinstallationsprogramm verwenden. In den Ordner Temp extrahierte Dateien werden allerdings automatisch gelöscht, wenn die Installation abgeschlossen ist. Alternativ können Sie den Befehl /extract mit einem absoluten Pfad verwenden.

Drei eigenständige VDA-Installationsprogramme stehen zum Herunterladen zur Verfügung.

VDAServerSetup.exe Installiert einen VDA für Serverbetriebssysteme. Es unterstützt alle Optionen für VDAs für Serverbetriebssysteme, die auch das Produktinstallationsprogramm bietet.

VDAWorkstationSetup.exe Installiert einen VDA für Desktopbetriebssysteme. Es unterstützt alle Optionen für VDAs für Desktopbetriebssysteme, die auch das Produktinstallationsprogramm bietet.

VDAWorkstationCoreSetup.exe Installiert einen VDA für Desktopbetriebssysteme, der für Remote PC-Zugriff-Bereitstellungen oder Kern-VDI-Installationen optimiert ist. Remote PC Access verwendet physische Maschinen. Kern-VDI-Installationen sind VMs, die nicht als Masterimage verwendet werden. Es werden nur die für VDA-Verbindungen erforderlichen Kerndienste installiert. Daher unterstützt es nur einen Teil der Optionen des Produktinstallationsprogramms bzw. von VDAWorkstationSetup.exe.

Dieses Installationsprogramm installiert keine Komponenten für Folgendes:

- App-V.
- Profilverwaltung. Das Ausschließen der Citrix Profilverwaltung bei der Installation hat Auswirkungen auf die Anzeigen von Citrix Director. Weitere Informationen finden Sie unter Installieren von VDAs.
- Maschinenidentitätsdienst.
- Persönliche vDisk oder AppDisks.

Citrix Receiver für Windows wird nicht von dem Installationsprogramm **VDAWorkstationCoreSetup.exe** installiert bzw. ist nicht in diesem enthalten.

Die Verwendung von **VDAWorkstationCoreSetup.exe** entspricht der Installation eines VDAs für Desktopbetriebssysteme mit dem Installationsprogramm **VDAWorkstationSetup** und:

- Grafische Oberfläche: Auswahl der Option "Remote-PC-Zugriff"auf der Seite **Umgebung** und Deaktivieren des Kontrollkästchens "Citrix Receiver"auf der Seite **Komponenten**.
- Befehlszeilenschnittstelle: Verwendung der Optionen "/remotepc"und "components/vda".
- Befehlszeilenschnittstelle: Festlegen von /components vda und /exclude "Citrix Personalization für App-V - VDA"*"Personal vDisk"*"Machine Identity Service"*"Citrix User Profile Manager"*"Citrix User Profile Manager WMI Plugin".

Sie können die ausgelassenen Komponenten/Features später mit dem Produktinstallationsprogramm installieren. Diese Aktion installiert alle fehlende Komponenten.

Microsoft Azure Resource Manager-Virtualisierungsumgebungen

August 18, 2021

Folgen Sie diesen Anleitungen, wenn Sie mit Microsoft Azure Resource Manager virtuelle Maschinen in Ihrer XenApp- oder XenDesktop-Umgebung bereitstellen.

Sie können XenApp oder XenDesktop für die Bereitstellung von Ressourcen in Azure Resource Manager bei der Erstellung der XenApp- bzw. XenDesktop-Site konfigurieren (welche das Erstellen einer Verbindung umfasst) oder später beim Erstellen einer Hostverbindung.

Sie sollten mit folgenden Elementen vertraut sein:

- Azure Active Directory: https://azure.microsoft.com/en-us/documentation/articles/active-directory-howto-tenant/
- Einverständniserklärung: https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications/
- Dienstprinzipal: https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/

Die Azure-Datenträgerverschlüsselung wird nicht unterstützt, wenn Sie Maschinenerstellungsdienste verwenden.

Diese Version von XenApp und XenDesktop unterstützt nur ein nicht verwaltetes Azure-Datenträgerspeichersystem. Standardmäßig verwendet Azure ein verwaltetes Datenträgerspeichersystem. Informationen zu Azure-Speicherlösungen mit und ohne Verwaltung finden Sie unter Azure Managed Disks.

Erstellen einer Verbindung mit Azure Resource Manager

Vollständige Informationen zu allen Seiten in den Assistenten zum Erstellen einer Site bzw. einer Verbindung finden Sie in den Artikeln Erstellen einer Site und Verbindungen und Ressourcen. Die nachfolgenden Informationen gelten nur für Azure Resource Manager-Verbindungen.

Es gibt zwei Möglichkeiten, eine Hostverbindung mit Azure Resource Manager zu herzustellen:

- Authentifizierung bei Azure Resource Manager zum Erstellen eines Dienstprinzipals
- Verwenden der Informationen eines zuvor erstellten Dienstprinzipals für die Verbindung mit Azure Resource Manager

Authentifizierung bei Azure Resource Manager zum Erstellen eines Dienstprinzipals

Bevor Sie anfangen, stellen Sie Folgendes sicher:

- Sie haben ein Benutzerkonto des Azure Active Directory-Mandanten Ihres Abonnements.
- Das Azure Active Directory-Benutzerkonto ist Co-Administrator des Azure-Abonnements, das Sie für die Bereitstellung von Ressourcen verwenden möchten.

Führen Sie im Assistenten zum Einrichten einer Site oder zum Hinzufügen einer Verbindung und von Ressourcen folgende Schritte aus:

1. Wählen Sie auf der Seite **Verbindung** den Verbindungstyp **Microsoft Azure** und Ihre Azure-Umgebung.
2. Geben Sie auf der Seite **Verbindungsdetails** die ID Ihres Azure-Abonnements und einen Namen für die Verbindung ein. Der Verbindungsname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: \/;:#.*?=<>|[]{}'" ()'). Nachdem Sie die Abonnement-ID und den Verbindungsnamen eingegeben haben, wird die Schaltfläche **Neu erstellen** verfügbar.
3. Geben Sie den Benutzernamen und das Kennwort des Azure Active Directory-Kontos ein.
4. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Akzeptieren**, um XenApp oder XenDesktop die aufgelisteten Berechtigungen zu geben. In XenApp bzw. XenDesktop wird ein Dienstprinzipal erstellt, der die Verwaltung von Azure Resource Manager-Ressourcen für den angegebenen Benutzer ermöglicht.
6. Nachdem Sie auf **Akzeptieren** geklickt haben, kehren Sie auf die Seite **Verbindung** in Studio zurück. Beachten Sie, dass bei der erfolgreichen Authentifizierung bei Azure die Schaltflächen **Neu erstellen** und **Vorhandene verwenden** durch **Verbunden** ersetzt werden und ein grünes Häkchen für die erfolgreiche Verbindung mit Ihrem Azure-Abonnement angezeigt wird.
7. Geben Sie an, welche Tools zum Erstellen der virtuellen Maschinen verwendet werden sollen, und klicken Sie dann auf **Weiter**. (Sie kommen über diese Seite im Assistenten nur hinaus, wenn Sie sich bei Microsoft Azure authentifiziert und die Erteilung der erforderlichen Berechtigungen akzeptiert haben.)

Ressourcen umfassen Region und Netzwerk.

- Wählen Sie auf der Seite **Region** eine Region aus.
- Gehen Sie auf der Seite **Netzwerk** folgendermaßen vor:
  - Geben Sie einen Ressourcennamen zur Identifizierung der Kombination aus Region und Netzwerk in Studio ein. Der Name muss aus 1–64 Zeichen bestehen. Der Ressourcenname darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: \/;:#.*?=<>|[]{}'"()'.
  - Wählen Sie eine Kombination aus virtuellem Netzwerk und Ressourcengruppe. (Da mehrere virtuelle Netzwerke den gleichen Namen haben können, erzielen Sie durch die Kombination aus Netzwerknamen und Ressourcengruppe Einmaligkeit.) Wenn Sie auf der vorherigen Seite eine Region ohne virtuelle Netzwerke gewählt haben, müssen Sie zu der Seite zurückkehren und eine Region wählen, die virtuelle Netzwerke enthält.

Schließen Sie den Assistenten ab.

Verwenden der Informationen eines zuvor erstellten Dienstprinzipals für die Verbindung mit Azure Resource Manager

Zum manuellen Erstellen eines Dienstprinzipals stellen Sie eine Verbindung mit Ihrem Azure Resource Manager-Abonnement her und verwenden Sie die u. a. PowerShell-Cmdlets.

Voraussetzungen:

- $SubscriptionId: Azure Resource Manager-Abonnement-ID des Abonnements, für das Sie VDAs bereitstellen möchten.
- $AADUser: Azure AD-Benutzerkonto des Abonnement-AD-Mandanten.
- Legen Sie $AADUser als Co-Administrator des Abonnements fest.
- $ApplicationName: Name der Anwendung, die in Azure AD erstellt werden soll.
- $ApplicationPassword: Kennwort für die Anwendung. Verwenden Sie dieses Kennwort als Anwendungsgeheimnis beim Erstellen der Hostverbindung.

Führen Sie zum Erstellen eines Dienstprinzipals folgende Schritte aus:

Schritt 1: Stellen Sie eine Verbindung mit Ihrem Azure Resource Manager-Abonnement her.

```
1 Login-AzureRmAccount.
```

Schritt 2: Wählen Sie das Azure Resource Manager-Abonnement, in dem Sie den Dienstprinzipal erstellen möchten.

```
1 Select-AzureRmSubscription -SubscriptionID $SubscriptionId;
```

Schritt 3: Erstellen Sie die Anwendung im AD-Mandanten.

```
1 $AzureADApplication = New-AzureRmADApplication -DisplayName
    $ApplicationName -HomePage "https://localhost/$ApplicationName" -
    IdentifierUris https://$ApplicationName -Password
    $ApplicationPassword
```

Schritt 4: Erstellen Sie einen Dienstprinzipal.

```
1 New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
    ApplicationId
```

Schritt 5: Weisen Sie dem Dienstprinzipal eine Rolle zu.

```
1 New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $AzureADApplication.ApplicationId – scope /
    subscriptions/$SubscriptionId
```

Schritt 6: Notieren Sie die im Ausgabefenster der PowerShell-Konsole angezeigte Anwendungs-ID (ApplicationId). Sie müssen diese ID beim Erstellen der Hostverbindung angeben.

Führen Sie im Assistenten zum Einrichten einer Site oder zum Hinzufügen einer Verbindung und von Ressourcen folgende Schritte aus:

1. Wählen Sie auf der Seite **Verbindung** den Verbindungstyp **Microsoft Azure** und Ihre Azure-Umgebung.
2. Geben Sie auf der Seite **Verbindungsdetails** die ID Ihres Azure-Abonnements und einen Namen für die Verbindung ein. (Der Verbindungsname muss aus 1–64 Zeichen bestehen, er darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: \/;:#.*?=<>|[]{}'" ()').
3. Klicken Sie auf **Vorhandene verwenden**. Geben Sie die Abonnement-ID, den Namen des Abonnements, die Authentifizierungs-URL, die Verwaltungs-URL, das Speichersuffix, die Active Directory- oder Mandanten-ID, die Anwendungs-ID und das Anwendungsgeheimnis für den vorhandenen Dienstprinzipal an. Nachdem Sie die Details eingegeben haben, ist die Schaltfläche **OK** aktiviert. Klicken Sie auf **OK**.
4. Geben Sie an, welche Tools zum Erstellen der virtuellen Maschinen verwendet werden sollen, und klicken Sie dann auf **Weiter**. Die von Ihnen eingegebenen Dienstprinzipalinformationen werden zum Herstellen der Verbindung mit Ihrem Azure-Abonnement verwendet. (Sie können im Assistenten erst fortfahren, wenn Sie gültige Angaben für die Option Vorhandene verwenden gemacht haben.)

Ressourcen umfassen Region und Netzwerk.

- Wählen Sie auf der Seite **Region** eine Region aus.
- Gehen Sie auf der Seite **Netzwerk** folgendermaßen vor:
  - Geben Sie einen Ressourcennamen zur Identifizierung der Kombination aus Region und Netzwerk in Studio ein. Der Name muss aus 1–64 Zeichen bestehen. Der Ressourcenname darf nicht ausschließlich aus Leerzeichen bestehen und folgende Zeichen nicht enthalten: \/;:#.*?=<>|[]{}'"()'.
  - Wählen Sie eine Kombination aus virtuellem Netzwerk und Ressourcengruppe. (Da mehrere virtuelle Netzwerke den gleichen Namen haben können, erzielen Sie durch die Kombination aus Netzwerknamen und Ressourcengruppe Einmaligkeit.) Wenn Sie auf der vorherigen Seite eine Region ohne virtuelle Netzwerke gewählt haben, müssen Sie zu der Seite zurückkehren und eine Region wählen, die virtuelle Netzwerke enthält.

Schließen Sie den Assistenten ab.

Erstellen eines Maschinenkatalogs unter Verwendung eines Azure Resource Manager-Masterimages

Diese Informationen ergänzen die Anleitungen im Artikel Erstellen von Maschinenkatalogen.

Ein Masterimage wird als Vorlage zum Erstellen der VMs in einem Maschinenkatalog verwendet. Erstellen Sie vor dem Erstellen des Maschinenkatalogs ein Masterimage in Azure Resource Manager. All-

gemeine Informationen über Masterimages finden Sie im Artikel "Erstellen von Maschinenkatalogen" .

Für das Erstellen eines Maschinenkatalogs in Studio gilt Folgendes:

- Die Seiten **Betriebssystem** und **Maschinenverwaltung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen in dem Artikel zum Erstellen von Maschinenkatalogen.
- Wählen Sie auf der Seite **Masterimage** eine Ressourcengruppe und navigieren Sie per Drilldown durch die Container zu der Azure-VHD, die Sie als Masterimage verwenden möchten. Auf der VHD muss ein Citrix VDA installiert sein. Wenn die VHD einer VM angeschlossen ist, muss die VM angehalten werden.
- Die Seite **Speicher- und Lizenztypen** wird nur angezeigt, wenn Sie ein Azure Resource Manager-Masterimage verwenden.

  Wählen Sie den Speichertyp (Standard oder Premium). Der gewählte Speichertyp bestimmt, welche Maschinengrößen auf der Seite Virtuelle Maschinen des Assistenten angeboten werden. Bei beiden Speichertypen werden mehrere synchrone Kopien der Daten in einem einzigen Datencenter erstellt. Weitere Informationen über Speichertypen und Speicherreplikation bei Azure finden Sie in den folgenden Artikeln:

  https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction

  https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-types#premium-ssd

  https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

  Wählen Sie aus, ob vorhandene lokale Windows Server-Lizenzen verwendet werden sollen. Bei Verwendung solcher Lizenzen in Kombination mit lokalen Windows Server-Images wird Azure Hybrid Use Benefits (HUB) verwendet. Weitere Details finden Sie unter https://azure.microsoft.com/pricing/hybrid-use-benefit/.

  HUB senkt die Kosten des Ausführens von VMs in Azure auf die Grundgebühr für Computekapazität, da keine Gebühren für zusätzliche Windows Server-Lizenzen aus dem Azure-Katalog erhoben werden. Sie müssen Ihre eigenen on-premises Windows Server-Images in Azure bringen, um HUB zu verwenden. Images aus dem Azure-Katalog werden nicht unterstützt. Lokale Windows Client-Lizenzen werden derzeit nicht unterstützt. Siehe https://blogs.msdn.microsoft.com/azureedu/2016/04/13/how-can-i-use-the-hybrid-use-benefit-in-azure/.

  Um zu prüfen, ob bereitgestellte virtuelle Maschinen HUB einwandfrei nutzen, führen Sie den folgenden PowerShell-Befehl aus

  ```
  Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM
  ```

  Überprüfen Sie, dass der Lizenztyp `Windows_Server` ist. Weitere Anweisungen finden Sie unter https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-

benefit-licensing?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json.

- Geben Sie auf der Seite **VMs** an, wie viele VMs Sie erstellen möchten. Sie müssen mindestens eine angeben. Wählen Sie eine Maschinengröße. Nach dem Erstellen eines Maschinenkatalogs können Sie die Maschinengröße nicht mehr ändern. Wenn Sie später eine andere Größe wünschen, löschen Sie den Maschinenkatalog und erstellen Sie einen neuen mit demselben Masterimage und der gewünschten Größe.

VM-Namen dürfen keine nicht-ASCII- oder Sonderzeichen enthalten.

- Die Seiten **Netzwerkkarten**, **Computerkonten** und **Zusammenfassung** enthalten keine Azure-spezifischen Informationen. Folgen Sie den Anleitungen in dem Artikel zum Erstellen von Maschinenkatalogen.

Schließen Sie den Assistenten ab.

Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen

August 18, 2021

Befolgen Sie die nachfolgenden Anweisungen, wenn Sie Hyper-V mit Microsoft System Center Virtual Machine Manager (VMM) zur Bereitstellung von virtuellen Maschinen verwenden.

Dieses Release unterstützt die im Artikel Systemanforderungen aufgeführten VMM-Versionen.

Verwenden Sie Provisioning Services und Maschinenerstellungsdienste zum Bereitstellen folgender Elemente:

- Desktop- oder Serverbetriebssystem-VM der ersten Generation
- Windows Server 2012 R2-, Windows Server 2016- und Windows 10-VM (mit oder ohne sicheren Start) der zweiten Generation

Aktualisieren von VMM

- Upgrade von VMM 2012 auf VMM 2012 SP1 oder VMM 2012 R2

  Informationen zu VMM- und Hyper-V-Hosts finden Sie unter https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg610649(v=sc.12)?redirectedfrom=MSDN. Informationen zu VMM-Konsolenanforderungen finden Sie unter https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg610640(v=sc.12)?redirectedfrom=MSDN.

Ein gemischter Hyper-V-Cluster wird nicht unterstützt. Ein gemischter Cluster ist beispielsweise einer, bei dem eine Hälfte des Clusters Hyper-V 2008 und die andere Hälfte Hyper-V 2012 ausführen.

- Upgrade von VMM 2008 R2 auf VMM 2012 SP1

  Wenn Sie ein Upgrade von XenDesktop 5.6 unter VMM 2008 R2 ausführen, halten Sie folgende Reihenfolge ein, um die Ausfallzeit von XenDesktop möglichst kurz zu halten:

  1. Upgrade von VMM auf 2012 (jetzt XenDesktop 5.6 und VMM 2012)
  2. Upgrade von XenDesktop auf die aktuelle Version (jetzt aktuelle XenDesktop-Version und VMM 2012)
  3. Upgrade von VMM von 2012 auf 2012 SP1 (jetzt aktuelle XenDesktop-Version und VMM 2012 SP1)

- Upgrade von VMM 2012 SP1 auf VMM 2012 R2

  Wenn Sie ein Upgrade von XenDesktop oder XenApp 7 unter VMM 2012 SP1 ausführen, halten Sie folgende Reihenfolge ein, um die Ausfallzeit von XenDesktop möglichst kurz zu halten:

  1. Upgrade von XenDesktop oder XenApp auf die aktuelle Version (jetzt aktuelle XenDesktop-/XenApp-Version und VMM 2012 SP1)
  2. Upgrade von VMM 2012 SP1 auf 2012 R2 (jetzt aktuelle XenDesktop- oder XenApp-Version und VMM 2012 R2)

Zusammenfassung von Installation und Konfiguration

> **Wichtig:**
>
> Alle Delivery Controller müssen in derselben Gesamtstruktur sein wie die VMM-Server.

1. Installieren und konfigurieren Sie einen Hypervisor.

   a) Installieren Sie Microsoft Hyper-V Server und VMM auf Ihren Servern.
   b) Installieren Sie die System Center VMM-Konsole auf allen Controllern. Die Konsolenversion muss mit der Version des Verwaltungsservers übereinstimmen. Obwohl eine frühere Konsole eine Verbindung zum Verwaltungsserver herstellen kann, schlägt die Bereitstellung von VDAs fehl, wenn die Versionen sich unterscheiden.
   c) Überprüfen Sie die folgenden Kontoinformationen:
      - Das Konto, das Sie zum Festlegen von Hosts in Studio verwenden, ist ein VMM-Administrator oder delegierter VMM-Administrator für die relevanten Hyper-V-Maschinen. Wenn dieses Konto nur über die delegierte Administratorrolle in VMM verfügt, werden die Speicherdaten in Studio beim Erstellen des Hosts nicht aufgeführt.

- Das Benutzerkonto, das für die Studio-Integration verwendet wird, muss auch Mitglied der lokalen Administratorsicherheitsgruppe auf jedem Hyper-V-Server sein, um zur Lebenszyklusverwaltung von VM (z. B. VM erstellen, aktualisieren und löschen) berechtigt zu sein.
  Hinweis: Die direkte Installation eines Controllers auf einem Server, auf dem Hyper-V ausgeführt wird, wird nicht unterstützt.

2. Erstellen Sie eine Master-VM.

   a) Installieren Sie einen Virtual Delivery Agent auf der Master-VM und wählen Sie die Option zur Desktopoptimierung aus. Dies verbessert die Leistung.
   b) Erstellen Sie einen Snapshot der Master-VM, um diesen als Sicherungskopie zu verwenden.

3. Erstellen Sie virtuelle Desktops. Bei Verwendung von MCS zum Erstellen von VM beim Erstellen einer Site oder einer Verbindung:

   a) Wählen Sie den Typ des Microsoft-Virtualisierungshosts aus.
   b) Geben Sie die Adresse als vollqualifizierten Domänennamen des Hostservers ein.
   c) Geben Sie die Anmeldeinformationen für das zuvor erstellte Administratorkonto ein, das Berechtigungen zum Erstellen von VM enthält.
   d) Wählen Sie im Dialogfeld Hostdetails den Cluster oder eigenständigen Host aus, der beim Erstellen der neuen VMs verwendet werden soll.
   Wichtig: Sie müssen auch dann zu einem Cluster oder eigenständigen Host navigieren und diesen auswählen, wenn Sie eine Bereitstellung mit einem einzelnen Hyper-V-Host verwenden.

MCS auf SMB 3-Dateifreigaben

Bei Maschinenkatalogen, die mit MSC auf SMB 3-Dateifreigaben für VM-Speicher erstellt wurden, müssen Sie darauf achten, dass die Anmeldeinformationen die nachfolgenden Anforderungen erfüllen, damit Aufrufe von der Hypervisor Communications Library (HCL) des Controllers die Verbindung mit dem SMB-Speicher herstellen:

- Die VMM-Benutzeranmeldeinformationen müssen vollständigen Lese-/Schreibzugriff auf den SMB-Speicher umfassen.
- Speichervorgänge auf dem virtuellen Datenträger werden bei Vorgängen im Lebenszyklus der VM über den Hyper-V-Server mit den VMM-Anmeldeinformationen durchgeführt.

Wenn Sie SMB als Speicher verwenden, aktivieren Sie das Feature "CredSSP"(Credential Security Support Provider) vom Controller auf den einzelnen Hyper-V-Maschinen, wenn Sie VMM 2012 SP1 mit Hyper-V unter Windows Server 2012 verwenden. Weitere Informationen finden Sie unter CTX137465.

Über eine standardmäßige Remote-PowerShell V3-Sitzung verwendet die HCL CredSSP zum Öffnen einer Verbindung mit der Hyper-V-Maschine. Dieses Feature übergibt mit Kerberos verschlüsselte Benutzeranmeldeinformationen an die Hyper-V-Maschine. Die PowerShell-Befehle in dieser Sitzung auf der Remotemaschine mit Hyper-V werden dann unter Verwendung der angegebenen Anmeldeinformationen (in diesem Fall, derer des VMM-Benutzers) ausgeführt, sodass eine ordnungsgemäße Kommunikation mit dem Speicher gewährleistet wird.

Die folgenden Tasks verwenden PowerShell-Skripts der HCL, die an die Hyper-V-Maschine zur Verwendung mit SMB 3.0-Speicher gesendet werden.

- **Konsolidieren des Masterimages:** Ein Masterimage erstellt ein neues MCS-Provisioningschema (Maschinenkatalog). Die Master-VM wird durch dieses Schema geklont und vereinfacht, damit sie zum Erstellen neuer VM aus dem neu erstellten Datenträger bereit ist (die Abhängigkeit zur ursprünglichen Master-VM wird entfernt).

  ConvertVirtualHardDisk im Namespace root\virtualization\v2

  Beispiel:

  ```
  $ims = Get-WmiObject -class $class -namespace "root\
     virtualization\v2";
  $result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
  $result
  ```

- **Erstellen eines differenzierenden Datenträgers**: erstellt einen differenzierenden Datenträger aus dem Masterimage, das durch Konsolidierung des Masterimages generiert wurde. Der differenzierende Datenträger wird dann an eine neue VM angeschlossen.

  CreateVirtualHardDisk im Namespace root\virtualization\v2

  Beispiel:

  ```
  $ims = Get-WmiObject -class $class -namespace "root\
     virtualization\v2";
  $result = $ims.CreateVirtualHardDisk($vhdastext);
  $result
  ```

- **Upload von Identitätsdisks:** Von der HCL kann die Identitätsdisk nicht direkt in den SMB-Speicher hochgeladen werden. Daher muss der Identitätsdatenträger von der Hyper-V-Maschine hochgeladen und in den Speicher kopiert werden. Da die Hyper-V-Maschine die Disk nicht auf dem Controller lesen kann, muss sie von der HCL zuerst wie folgt über die Hyper-V-Maschine kopiert werden:

  1. Upload der Identitätsdisk durch die HCL auf die Hyper-V-Maschine über die Administratorfreigabe.
  2. Der Datenträger wird von der Hyper-V-Maschine über ein PowerShell-Skript, das in der Remote-PowerShell-Sitzung ausgeführt wird, in den SMB-Speicher kopiert. Auf der Hyper-

V-Maschine wird ein Ordner erstellt, dessen Berechtigungen nur für den VMM-Benutzer gesperrt sind (über die remote PowerShell-Verbindung).

3. Die HCL löscht die Datei aus der Administratorfreigabe.
4. Wenn der Upload des Identitätsdatenträgers durch die HCL auf die Hyper-V-Maschine abgeschlossen ist, werden die Identitätsdatenträger von der Remote-PowerShell-Sitzung in den SMB-Speicher kopiert und dann aus der Hyper-V-Maschine gelöscht.

   Falls der Ordner des Identitätsdatenträgers gelöscht wird, wird er neu erstellt, damit er zur Wiederverwendung verfügbar ist.

- **Download von Identitätsdisks:** Wie beim Upload wird die Identitätsdisk über die Hyper-V-Maschine an die HCL übergeben. Beim folgenden Prozess wird, falls noch nicht vorhanden, ein Ordner erstellt, der nur VMM-Benutzerbenutzerberechtigungen auf dem Hyper-V-Server hat.

  1. Die Disk wird von der Hyper-V-Maschine aus dem SMB-Speicher in den lokalen Hyper-V-Speicher kopiert, und zwar über ein PowerShell-Skript, das in der Remote-PowerShell V3-Sitzung ausgeführt wird.
  2. Die HCL liest den Datenträger aus der Administratorfreigabe der Hyper-V-Maschine in den Speicher.
  3. Die HCL löscht die Datei aus der Administratorfreigabe.

- **Erstellen einer persönlichen vDisk:** Wenn der Administrator die VM in einem Personal vDisk-Maschinenkatalog erstellt, muss eine leere Disk (PvD) erstellt werden.

  Der Aufruf zum Erstellen einer leeren Disk erfordert keinen direkten Zugriff auf den Speicher. Wenn Sie PvDs auf anderen Speichern als dem Haupt- oder dem Betriebssystemdatenträger haben, verwenden Sie Remote-PowerShell zum Erstellen der PvD in einem Ordner mit dem gleichen Namen wie die VM, aus dem sie erstellt wurde. Verwenden Sie Remote-PowerShell nicht mit CSV oder LocalStorage. VMM-Befehlsfehler werden vermieden, wenn zuerst das Verzeichnis und dann die leere Disk erstellt werden.

  Führen Sie auf der Hyper-V-Maschine mkdir an dem Speicher aus.

Microsoft System Center Configuration Manager-Umgebungen

August 18, 2021

Bei Sites, in denen der Zugriff auf Anwendungen und Desktops auf physischen Geräten mit Microsoft System Center Configuration Manager (Configuration Manager) verwaltet wird, kann diese Verwendung über die Integrationsoptionen auf XenApp bzw. XenDesktop ausgeweitet werden.

- **Citrix Connector 7.5 für Configuration Manager 2012:** Citrix Connector bildet eine Brücke zwischen Configuration Manager und XenApp bzw. XenDesktop. Mit Citrix Connector können Sie alltägliche Vorgänge in den mit Configuration Manager verwalteten physischen Umgebungen und den mit XenApp bzw. XenDesktop verwalteten virtuellen Umgebungen übergreifend vereinheitlichen. Weitere Informationen zum Connector finden Sie unter Citrix Connector 7.5 für System Center Configuration Manager 2012.
- **Configuration Manager Wake Proxy-Feature:** Für das Wake-On-LAN-Feature für den Remote-PC-Zugriff wird Configuration Manager benötigt. Weitere Informationen finden Sie weiter unten.
- **XenApp- und XenDesktop-Eigenschaften:** XenApp- und XenDesktop-Eigenschaften ermöglichen die Identifizierung virtueller Citrix Desktops für die Verwaltung durch Configuration Manager. Diese Eigenschaften werden automatisch von Citrix Connector verwendet, sie können aber auch manuell konfiguriert werden, wie im folgenden Abschnitt beschrieben.

Eigenschaften

Eigenschaften stehen Microsoft System Center Configuration Manager für die Verwaltung virtueller Desktops zur Verfügung.

Boolesche Eigenschaften in Configuration Manager können als 1 oder 0 statt “True”oder “False” angezeigt werden.

Die Eigenschaften stehen in der Klasse Citrix_virtualDesktopInfo im Namespace Root\Citrix\DesktopInformation zur Verfügung. Die Namen der Eigenschaften stammen vom Anbieter für Windows-Verwaltungsinstrumentation (WMI).

Eigenschaft	Beschreibung
AssignmentType	Legt den Wert auf IsAssigned fest. Gültige Werte sind: ClientIP, ClientName, None und User (setzt *IsAssigned* auf “True”)
BrokerSiteName	Site, gibt den gleichen Wert wie HostIdentifier zurück.
DesktopCatalogName	Dem Desktop zugewiesener Maschinenkatalog
DesktopGroupName	Dem Desktop zugewiesene Bereitstellungsgruppe
HostIdentifier	Site, gibt den gleichen Wert wie BrokerSiteName zurück.
IsAssigned	True = ordnet den Desktop einem Benutzer zu; False = zufälliger Desktop.

Eigenschaft	Beschreibung
IsMasterImage	Ermöglicht Entscheidungen bezüglich der Umgebung. Beispielsweise können Sie Anwendungen auf dem Masterimage und nicht auf den bereitgestellten Maschinen installieren, besonders dann, wenn diese Maschinen auf Bootmaschinen in einem fehlerfreien Zustand sind. Gültige Werte: **True** auf einer VM, die als Masterimage verwendet wird (dieser Wert wird während der Installation basierend auf einer Auswahl festgelegt), **Cleared** auf einer VM, die von diesem Image bereitgestellt wird.
IsVirtualMachine	True für eine virtuelle Maschine, False für eine physische Maschine
OSChangesPersist	False, wenn das Betriebssystemimage des Desktops bei jedem Neustart in einen fehlerfreien Zustand versetzt wird, andernfalls True
PersistentDataLocation	Der Speicherort, an dem Configuration Manager persistente Daten speichert. Benutzer haben hierauf keinen Zugriff.
PersonalvDiskDriveLetter	Bei einem Desktop mit einer persönlichen vDisk ist dies der Laufwerksbuchstabe, den Sie der persönlichen vDisk zuweisen.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Festgelegt, wenn der Desktop sich beim Controller registriert; bei Desktops, die noch nicht vollständig registriert sind, NULL

Zum Sammeln der Eigenschaften führen Sie eine Hardwareinventur in Configuration Manager durch. Zum Anzeigen der Eigenschaften verwenden Sie den Ressourcen-Explorer von Configuration Manager. In diesen Fällen können die Namen Leerzeichen enthalten oder vom Eigenschaftsnamen etwas abweichen. **BrokerSiteName** kann z. B. als “Broker Site Name”angezeigt werden.

- Konfigurieren von Configuration Manager zum Sammeln von Citrix WMI-Eigenschaften vom Citrix VDA
- Erstellen abfragebasierter Gerätesammlungen mit Citrix WMI-Eigenschaften
- Erstellen globaler Bedingungen basierend auf Citrix WMI-Eigenschaften
- Verwenden globaler Bedingungen zum Definieren von Anforderungen für Anwendungsbereitstellungstypen

Sie können in der Microsoft-Klasse CCM_DesktopMachine im Namespace Root\ccm_vdi auch Microsoft-Eigenschaften verwenden. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Configuration Manager und Wake-On-LAN-Feature für den Remote-PC-Zugriff

Zum Konfigurieren des Wake-On-LAN-Features von Remote-PC-Zugriff führen Sie die folgenden Schritte aus, bevor Sie einen VDA auf den Büro-PCs installieren und mit Studio die Remote-PC-Zugriff-Bereitstellung erstellen oder aktualisieren:

- Konfigurieren Sie Configuration Manager 2012, 2012 R2 oder 2016 im Unternehmen. Stellen Sie dann den Configuration Manager-Client auf allen Remote-PC-Zugriff-Maschinen bereit. Warten Sie, bis der geplante SCCM-Bestandszyklus ausgeführt wurde (oder erzwingen Sie manuell eine Ausführung). Die Zugriffsanmeldeinformationen, die Sie in Studio zum Konfigurieren der Verbindung mit ConfigMgr festlegen, müssen Sammlungen im Geltungsbereich und die Rolle "Remotetoolsverantwortlicher"umfassen.
- Für die Unterstützung von Intel Active Management Technology (AMT) gilt Folgendes:
  - Die unterstützte Mindestversion auf dem PC ist AMT 3.2.1.
  - Stellen Sie den PC für die Verwendung von AMT mit Zertifikaten und zugehörigen Provisioningvorgängen bereit.
  - Nur Configuration Manager 2012 und 2012 R2 können verwendet werden, nicht aber Configuration Manager 2016.
- Für die Unterstützung von ConfigMgr Wake Proxy bzw. Magic Packet gilt Folgendes:
  - Konfigurieren Sie Wake-On-LAN in den BIOS-Einstellungen aller PCs.
  - Zur Unterstützung von Wake Proxy aktivieren Sie die entsprechende Option in Configuration Manager. Für jedes Subnetz des Unternehmens mit PCs, auf denen das Wake-On-LAN-Feature für Remote-PC-Zugriff verwendet wird, müssen mindestens drei Maschinen als Sentinelmaschinen fungieren können.
  - Zur Unterstützung von Magic Packet konfigurieren Sie Netzwerkrouter und Firewalls so, dass Magic Packets entweder per subnetzgesteuertem Broadcast oder Unicast gesendet werden können.

Nach der Installation des VDAs auf Büro-PCs aktivieren oder deaktivieren Sie die Energieverwaltung beim Erstellen der Remote-PC-Zugriff-Bereitstellung in Studio.

- Wenn Sie die Energieverwaltung aktivieren, geben Sie Verbindungsdetails an, d. h. ConfigMgr-Adresse, Anmeldeinformationen und einen Namen.
- Wenn Sie die Energieverwaltung nicht aktivieren, können Sie später eine Energieverwaltungsverbindung (Configuration Manager) hinzufügen und dann den Remote-PC-Zugriff-

Maschinenkatalog bearbeiten, um die Energieverwaltung zu aktivieren und eine neue Energieverwaltungsverbindung anzugeben.

Sie können eine Energieverwaltungsverbindung bearbeiten, um die Verwendung von ConfigMgr Wake Proxy und Magic Packets zu konfigurieren und die Paketübertragungsmethode zu ändern.

Informationen hierzu finden Sie unter Remote-PC-Zugriff.

VMware-Virtualisierungsumgebungen

January 22, 2019

Folgen Sie diesen Anweisungen, wenn Sie zur Bereitstellung von virtuellen Maschinen VMware verwenden.

Installieren Sie vCenter Server und die Verwaltungstools. (Der "Linked Mode"-Betrieb von vSphere vCenter wird nicht unterstützt.)

Wenn Sie MCS verwenden möchten, deaktivieren Sie nicht das Datastore Browser-Feature in vCenter Server (siehe https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567). Wenn Sie das Feature deaktivieren, funktioniert MCS nicht richtig.

Erforderliche Berechtigungen

Erstellen Sie ein VMware-Benutzerkonto und mindestens eine VMware-Rolle mit einigen oder allen unten aufgeführten Berechtigungen. Berücksichtigen Sie bei der Rollenerstellung die erforderliche Granularität für die Benutzerberechtigungen zum jederzeitigen Anfordern der verschiedenen XenApp- oder XenDesktop-Vorgänge. Zum Gewähren spezifischer Berechtigungen für jeden Zeitpunkt weisen Sie dem Benutzer die entsprechende Rolle mindestens auf Datencenterebene zu.

Die folgenden Tabellen zeigen die Zuordnungen zwischen XenApp- und XenDesktop-Vorgängen und die erforderlichen VMware-Mindestberechtigungen.

Hinzufügen von Verbindungen und Ressourcen

SDK	Benutzeroberfläche
System.Anonymous, System.Read und System.View	Automatisch hinzugefügt. Kann die integrierte Lesezugriff-Rolle verwenden.

Bereitstellen von Maschinen (Maschinenerstellungsdienste)

SDK	Benutzeroberfläche
Datastore.AllocateSpace	Datastore > Allocate Space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2 und vSphere 5.1, Update 1: Virtual machine > State > Create snapshotvSphere 5.5: Virtual machine > Snapshot management > Create snapshot

Wenn Sie die erstellten VMs mit Tags kennzeichnen wollen, fügen Sie die folgenden Berechtigungen dem Benutzerkonto hinzu.

Um sicherzustellen, dass Sie ein sauberes Basisimage zum Erstellen neuer VMs verwenden, fügen Sie Tags den VMs hinzu, die mit den Maschinenerstellungsdiensten erstellt wurden. Damit schließen Sie sie aus der Liste der für Basisimages verfügbaren virtuellen Maschinen aus.

SDK	Benutzeroberfläche
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Manage custom attributes

Bereitstellen von Maschinen (Provisioning Services)

Alle Berechtigungen von **Bereitstellen von Maschinen (Maschinenerstellungsdienste)** sowie folgende:

SDK	Benutzeroberfläche
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template

Energieverwaltung

SDK	Benutzeroberfläche
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend

Updates und Rollbacks von Images

SDK	Benutzeroberfläche
Datastore.AllocateSpace	Datastore > Allocate Space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Löschen bereitgestellter Maschinen

SDK	Benutzeroberfläche
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

AppDisks erstellen

Gilt für VMware vSphere ab Version 5.5 und XenApp und XenDesktop ab Version 7.8.

SDK	Benutzeroberfläche
Datastore.AllocateSpace	Datastore > Allocate Space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.EditDevice	Virtual machine > Configuration > Modify Device Settings
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On

AppDisks löschen

Gilt für VMware vSphere ab Version 5.5 und XenApp und XenDesktop ab Version 7.8.

SDK	Benutzeroberfläche
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off

Beschaffen und Importieren eines Zertifikats

Um die vSphere-Kommunikation zu schützen, empfiehlt Citrix die Verwendung von HTTPS statt HTTP. HTTPS benötigt digitale Zertifikate. Citrix empfiehlt die Verwendung eines digitalen Zertifikats, das von einer Zertifizierungsstelle unter Berücksichtigung der Sicherheitsrichtlinie Ihrer Organisation erstellt wurde.

Wenn Sie kein digitales Zertifikat verwenden können, das von einer Zertifizierungsstelle ausgestellt wurde, können Sie das mit VMware installierte selbstsignierte Zertifikat verwenden, vorausgesetzt, die Sicherheitsrichtlinie Ihrer Organisation lässt dies zu. Fügen Sie das VMware vCenter-Zertifikat jedem Controller hinzu.

Schritt 1. Fügen Sie den vollqualifizierten Domänennamen (FQDN) des Computers, auf dem vCenter Server ausgeführt wird, der Hostdatei auf dem Server im Verzeichnis %SystemRoot%/WINDOWS/system32/Drivers/ hinzu. Dieser Schritt ist nur erforderlich, wenn der FQDN des Computers, auf dem vCenter Server ausgeführt wird, nicht bereits im Domänennamensystem vorhanden ist.

Schritt 2. Rufen Sie das vCenter-Zertifikat mit einer der folgenden drei Methoden ab:

Führen Sie auf dem vCenter-Server folgende Schritte aus:

1. Kopieren Sie die Datei rui.crt vom vCenter-Server zu einem Speicherort, auf den Ihre Delivery Controller zugreifen können.
2. Navigieren Sie auf dem Controller zu dem Speicherort des exportierten Zertifikats und öffnen Sie die Datei rui.crt.

Laden Sie das Zertifikat über einen Webbrowser herunter: Bei Verwendung von Internet Explorer müssen Sie (abhängig von Ihrem Benutzerkonto) ggf. in Internet Explorer mit der rechten Maustaste klicken und **Als Administrator ausführen** wählen, um das Zertifikat herunterzuladen und zu installieren.

1. Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her (z. B. `https://server1.domain1.com`).
2. Akzeptieren Sie die Sicherheitswarnungen.
3. Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
4. Zeigen Sie das Zertifikat an und klicken Sie auf die Registerkarte "Details".
5. Wählen Sie **Copy to file and export in .CER format** und geben Sie bei entsprechender Aufforderung einen Namen an.
6. Speichern Sie das exportierte Zertifikat.
7. Navigieren Sie auf den Speicherort des exportierten Zertifikats und öffnen Sie die CER-Datei.

Direkter Import von Internet Explorer, der als Administrator ausgeführt wird:

1. Öffnen Sie einen Webbrowser und stellen Sie eine sichere Webverbindung mit dem vCenter-Server her (z. B. `https://server1.domain1.com`).
2. Akzeptieren Sie die Sicherheitswarnungen.
3. Klicken Sie auf die Adressleiste, in der der Zertifikatfehler angezeigt wird.
4. Zeigen Sie das Zertifikat an.

Schritt 3: Importieren Sie das Zertifikat auf jedem Controller in den Zertifikatspeicher.

1. Klicken Sie auf **Zertifikat installieren**, wählen Sie **Lokaler Computer** und klicken Sie dann auf **Weiter**.

2. Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie dann auf **Durchsuchen**.

Windows Server 2008 R2: Aktivieren Sie das Kontrollkästchen **Physikalischen Speicher anzeigen**. Erweitern Sie **Vertrauenswürdige Personen**. Wählen Sie **Lokaler Computer**. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Spätere unterstützte Version: Wählen Sie **Vertrauenswürdige Personen** und klicken Sie dann auf **OK**. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Wichtig: Wenn Sie den Namen des vSphere-Servers nach der Installation ändern, müssen Sie ein neues selbstsigniertes Zertifikat auf diesem Server erstellen, bevor Sie das neue Zertifikat importieren.

Überlegungen zur Konfiguration

Erstellen einer Master-VM:

Verwenden Sie eine Master-VM zur Bereitstellung von Benutzerdesktops und Anwendungen in einem Maschinenkatalog. Auf dem Hypervisor:

1. Installieren Sie einen VDA auf der Master-VM unter Auswahl der Option zur Desktopoptimierung, wodurch die Leistung verbessert wird.
2. Erstellen Sie einen Snapshot der Master-VM, um diesen als Backup zu verwenden.

Erstellen einer Verbindung:

Führen Sie im Assistenten für die Verbindungserstellung folgende Schritte aus:

- Wählen Sie den Verbindungstyp "VMware".
- Geben Sie die Adresse des Zugriffspunkts für das vCenter SDK an.
- Geben Sie die Anmeldeinformationen für ein zuvor eingerichtetes VMware-Konto ein, das Berechtigungen zum Erstellen neuer VMs hat. Geben Sie den Benutzernamen im Format Domäne/Benutzername ein.

VMware SSL-Fingerabdruck

Mit dem VMware SSL-Fingerabdruckfeature wurde ein häufig aufgetretener Fehler beim Erstellen einer Hostverbindung mit einem VMware vSphere-Hypervisor behoben. Bisher musste der Administrator eine Vertrauensstellung zwischen den Site-Delivery Controllern und dem Hypervisor-Zertifikat vor dem Erstellen einer Verbindung manuell erstellen. Dank VMware SSL-Fingerabdruck ist dies nicht mehr nötig. Der Fingerabdruck des nicht vertrauenswürdigen Zertifikats wird in der Sitedatenbank gespeichert, damit der Hypervisor zwar nicht von den Controllern, jedoch von XenApp bzw. XenDesktop immer als vertrauenswürdig eingestuft wird.

Beim Erstellen einer vSphere-Hostverbindung in Studio wird ein Dialogfeld mit dem Zertifikat der Maschine angezeigt, mit der Sie eine Verbindung herstellen. Sie können dann wählen, ob sie als vertrauenswürdig gelten soll.

Nutanix-Virtualisierungsumgebungen

August 18, 2021

Folgen Sie diesen Anleitungen, wenn Sie mit Nutanix Acropolis virtuelle Maschinen in Ihrer XenApp- oder XenDesktop-Bereitstellung bereitstellen. Der Setupvorgang umfasst die folgenden Aufgaben:

- Installieren und Registrieren des Nutanix-Plug-Ins in der XenApp- oder XenDesktop-Umgebung.
- Erstellen einer Verbindung mit dem Nutanix Acropolis-Hypervisor.
- Erstellen eines Maschinenkatalogs mit dem Snapshot eines Masterimages, das auf dem Nutanix-Hypervisor erstellt wurde.

Weitere Informationen finden Sie in der Installationsdokumentation zum Nutanix Acropolis MCS-Plug-In, das vom Nutanix Support Portal auf https://portal.nutanix.com heruntergeladen werden kann.

Supportinformationen zu Nutanix und Provisioning Services finden Sie im Knowledge Center Artikel CTX131239.

Installieren und Registrieren des Nutanix-Plug-Ins

Nach der Installation der XenApp- oder XenDesktop-Komponenten führen Sie die folgenden Schritte aus, um das Nutanix-Plug-In auf den Delivery Controllern zu installieren und zu registrieren. Sie können dann mit Studio eine Verbindung mit dem Nutanix-Hypervisor erstellen und zudem einen Maschinenkatalog erstellen, der einen in der Nutanix-Umgebung erstellten Snapshot von einem Masterimage verwendet.

1. Beziehen Sie das Nutanix-Plug-In von Nutanix und installieren Sie es auf den Delivery Controllern.
2. Stellen Sie sicher, dass ein Nutanix Acropolis-Ordner mit folgendem Pfad erstellt wurde: C:\Programme\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Führen Sie Folgendes aus: **C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe –PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"** .
4. Starten Sie den Citrix Hostdienst, Citrix Brokerdienst und Citrix Maschinenerstellungsdienste neu.

5. Führen Sie die folgenden PowerShell-Cmdlets aus, um sicherzustellen, dass das Nutanix Acropolis-Plug-In registriert wurde:

   Add-PSSnapin Citrix*

   Get-HypHypervisorPlugin

Erstellen einer Verbindung mit Nutanix

Vollständige Informationen zu allen Seiten in den Assistenten zum Erstellen einer Verbindung finden Sie in den Artikeln Erstellen einer Site und Verbindungen und Ressourcen.

Wählen Sie im Assistenten zum Einrichten einer Site oder zum Hinzufügen einer Verbindung und von Ressourcen auf der Seite **Verbindung** den Verbindungstyp **Nutanix**. Geben Sie dann die Hypervisoradresse und Anmeldeinformationen sowie einen Namen für die Verbindung ein. Wählen Sie auf der Seite **Netzwerk** ein Netzwerk für die Hostingeinheit aus.

Erstellen eines Maschinenkatalogs mit einem Nutanix-Snapshot

Diese Informationen ergänzen die Anleitungen im Artikel Erstellen von Maschinenkatalogen. Es werden nur die Felder beschrieben, die für Nutanix gelten.

Der von Ihnen ausgewählte Snapshot wird als Vorlage zum Erstellen der VMs im Maschinenkatalog verwendet. Erstellen Sie erst Images und Snapshots in Nutanix, bevor Sie den Maschinenkatalog erstellen.

- Allgemeine Informationen über Masterimages finden Sie im Artikel "Erstellen von Maschinenkatalogen".
- Anleitungen zum Erstellen von Images und Snapshots in Nutanix finden Sie in der Nutanix-Dokumentation, auf die zuvor verwiesen wurde.

Die Seiten **Betriebssystem** und **Maschinenverwaltung** enthalten keine Nutanix-spezifischen Informationen. Folgen Sie den Anleitungen in dem Artikel zum Erstellen von Maschinenkatalogen.

Wählen Sie auf der Seite **Container**, die nur für Nutanix gilt, den Container aus, in dem die Festplatten der VMs platziert werden.

Wählen Sie auf der Seite **Masterimage** den Snapshot des Images aus. Acropolis-Snapshotnamen muss das Präfix "XD_"vorangestellt sein, damit sie in XenApp und XenDesktop verwendet werden können. Verwenden Sie bei Bedarf die Acropolis-Konsole, um die Snapshots umzubenennen. Wenn Sie Snapshots umbenennen, starten Sie den Assistenten zum Erstellen von Katalogen neu, damit eine aktualisierte Liste angezeigt wird.

Geben Sie auf der Seite **Virtuelle Maschinen** die Anzahl der virtuellen CPUs und die Anzahl der Kerne pro vCPU an.

Die Seiten **Netzwerkkarten**, **Computerkonten** und **Zusammenfassung** enthalten keine Nutanix-spezifischen Informationen. Folgen Sie den Anleitungen in dem Artikel zum Erstellen von Maschinenkatalogen.

Microsoft Azure-Virtualisierungsumgebungen

August 18, 2021

Verbindungskonfiguration

Wenn Sie Studio zum Erstellen einer Microsoft Azure-Verbindung verwenden, benötigen Sie Informationen aus der Datei mit den Veröffentlichungseinstellungen von Microsoft Azure. Die Informationen in dieser XML-Datei für die einzelnen Abonnements sehen in etwa folgendermaßen aus (das tatsächliche Verwaltungszertifikat ist viel länger):

```
<Subscription
ServiceManagementUrl="https://management.core.windows.net"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl;
   sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
<!--NeedCopy-->
```

Bei dem folgenden Verfahren wird davon ausgegangen, dass Sie mit Studio eine Verbindung erstellen und entweder den Assistenten für die Siteerstellung oder den Assistenten für die Verbindungserstellung gestartet haben.

1. Rufen Sie in einem Browser https://manage.windowsazure.com/publishsettings/index auf.
2. Klicken Sie auf das Cloudshellsymbol neben dem Suchfeld und folgen Sie den Anweisungen um die Datei für die Veröffentlichungseinstellungen herunterzuladen.
3. Klicken Sie in Studio auf der Seite **Verbindung** des Assistenten nach Auswahl des Verbindungstyps “Microsoft Azure”auf “Importieren”.
4. Wenn Sie mehrere Abonnements haben, werden Sie zur Auswahl des gewünschten Abonnements aufgefordert.

ID und Zertifikat werden automatisch und ohne Benutzereingriff in Studio importiert.

Energieaktionen, für die eine Verbindung verwendet wird, unterliegen Schwellenwerten. Im Allgemeinen sind die Standardwerte geeignet und sollten nicht geändert werden. Sie können sie jedoch beim Bearbeiten einer Verbindung ändern (beim Erstellen von Verbindungen können diese Werte nicht geändert werden). Weitere Informationen finden Sie unter Bearbeiten einer Verbindung.

Virtuelle Maschinen

Die Auswahl der Größe einzelner virtueller Maschine beim Erstellen eines Maschinenkatalogs in Studio hängt von den angezeigten Optionen, den Kosten und der Leistung des jeweiligen VM-Instanztyps und der Skalierbarkeit ab.

In Studio werden alle VM-Instanzoptionen angezeigt, die von Microsoft Azure in der jeweiligen Region angeboten werden. Diese Auswahl kann von Citrix nicht geändert werden. Daher sollten Sie mit Ihren Anwendungen und deren CPU-, Arbeitsspeicher- und E/A- Bedarf vertraut sein. Es stehen diverse Optionen zu verschiedenen Preis- und Leistungsstufen zur Auswahl. Einzelheiten zu den Optionen finden Sie in den nachfolgend aufgeführten Microsoft-Artikeln.

- MSDN –VM- und Cloudgrößen für Azure: https://docs.microsoft.com/en-us/previous-versions/azure/dn197896(v=azure.100)?redirectedfrom=MSDN
- Preise virtueller Maschinen: https://azure.microsoft.com/en-us/pricing/details/virtual-machines

Basic-VMs: VMs der Klasse "Basic"sind Basisdatenträger. Sie unterliegen primär der von Microsoft unterstützten IOPS-Stufe 300. Solche VMs werden für die Arbeitslast von Desktopbetriebssystemen (VDI) und Serverbetriebssystem-RDSHs (Remotedesktop-Sitzungshost) nicht empfohlen.

Standard-VMs: Standard-VMs sind in vier Serien unterteilt: A, D, DS und G.

Reihe	Anzeige in Studio
A	Sehr klein, klein, mittel, groß, sehr groß, A5, A6, A7, A8, A9, A10, A11. Mittel und Groß werden für Tests mit Arbeitslasten der Kategorie Desktopbetriebssystem (VDI) oder Serverbetriebssystem-RDSH empfohlen.
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. Diese VMs bieten SSDs für die temporäre Speicherung.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14: Diese VMs bieten einen lokalen SSD-Speicher für alle Datenträger.
G	Standard_G1 –G5: Diese VMs sind für High Performance Computing geeignet.

Stellen Sie beim Provisioning von Maschinen in Azure Storage Premium sicher, dass Sie eine Maschinengröße auswählen, die im Storage Premium-Konto unterstützt wird.

Kosten- und Leistung von VM-Instanztypen

Die US-Listenpreise der einzelnen VM-Instanztypen pro Stunde finden Sie unter https://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

Bei der Arbeit mit Cloudumgebungen spielen die tatsächlichen Computing-Anforderungen eine wichtige Rolle. Für Machbarkeitsstudien oder anderen Tests werden gerne Hochleistungsinstanztypen verwendet. Zur Einsparung von Kosten kann es hingegen verlockend sein, die VMs mit der niedrigsten Leistung zu wählen. Allerdings sollte idealerweise die für die jeweilige Aufgabe am besten geeignete VM verwendet werden. Die VMs der höchsten Leistungsklasse erzielen möglicherweise nicht das gewünschte Ergebnis und werden mit der Zeit sehr teuer –manchmal schon innerhalb einer Woche. Weniger teure VMs einer niedrigen Leistungsklasse sind der jeweiligen Aufgabe u. U. nicht gewachsen.

Tests mit Login VSI bei mittlerer Arbeitslast haben ergeben, dass für Desktopbetriebssysteme (VDI) und Serverbetriebssystem-RDSH Instanzen des Typs "Mittel"(A2) und "Groß"(A3) das beste Preis-/Leistungsverhältnis bieten.

Die Reihen Mittel (A2) und Groß (A3 oder A5) bieten das beste Preis-/Leistungsverhältnis für die Arbeitslastanalyse. Alles darunter wird nicht empfohlen. Leistungsfähigere VM-Reihen bieten ggf. die von Anwendungen und Benutzern geforderte Leistung und Benutzerfreundlichkeit. Es empfiehlt sich jedoch, die drei o. g. Instanztypen als Grundwert anzusetzen, um zu ermitteln, ob die höheren Kosten einer leistungsstärkeren VM einen echten Mehrwert bringen.

Skalierbarkeit

Die Skalierbarkeit von Katalogen in einer Hostingeinheit unterliegt einigen Schranken. Einige davon, z. B. die Zahl der CPU-Kerne des Azure-Abonnements, können ausgeräumt werden, indem beim Support von Microsoft Azure eine Erhöhung des Standardwerts (20) angefordert wird. Andere, etwa die Zahl der VMs in einem virtuellen Netzwerk pro Abonnement (2048), können nicht geändert werden.

Derzeit unterstützt Citrix 40 Maschinen pro Katalog.

Zur Erhöhung der Zahl der virtuellen Maschinen in einem Katalog oder Host wenden Sie sich an den Microsoft Azure-Support. Die Standardskalierungslimits von Microsoft Azure verhindern die Überschreitung einer bestimmten VM-Anzahl. Diese Limits ändern sich jedoch häufig. Die aktuellen Limits finden Sie unter https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/.

Ein Microsoft Azure Virtual Network unterstützt bis zu 2048 VMs.

Microsoft empfiehlt ein Limit von 40 Standarddatenträger-VM-Images pro Clouddienst. Berücksichtigen Sie beim Skalieren die Zahl der Clouddienste, die für die VMs der gesamten Verbindung benötigt

werden. Ziehen Sie darüber hinaus die VMs in Betracht, die für gehostete Anwendungen benötigt werden.

Wenden Sie sich an den Support von Microsoft Azure, um in Erfahrung zu bringen, ob die Standardzahl der CPU-Kerne für Ihre Arbeitslasten erhöht werden muss.

Installieren der Kernkomponenten

August 18, 2021

Die Kernkomponenten sind der Delivery Controller, Studio, Director und der Lizenzserver.

(In Versionen vor 7.15 LTSR CU6 gehört StoreFront zu den Kernkomponenten. Sie können StoreFront weiterhin installieren, indem Sie im Abschnitt **Erweitern der Bereitstellung Citrix StoreFront** wählen oder den Befehl auf dem Installationsmedium ausführen.)

Wichtig: Lesen Sie vor der Installation die Informationen unter Vorbereiten der Installation. Lesen Sie außerdem den vorliegenden Artikel, damit Sie wissen, was zu erwarten ist.

Der vorliegende Abschnitt enthält Informationen zu der Reihenfolge der Schritte mit dem Installationsassistenten bei der Installation der Kernkomponenten. Die entsprechenden Befehle für die Befehlszeile werden ebenfalls angegeben. Weitere Informationen finden Sie unter Installieren an der Befehlszeile.

Schritt 1. Herunterladen der Produktsoftware und Starten des Assistenten

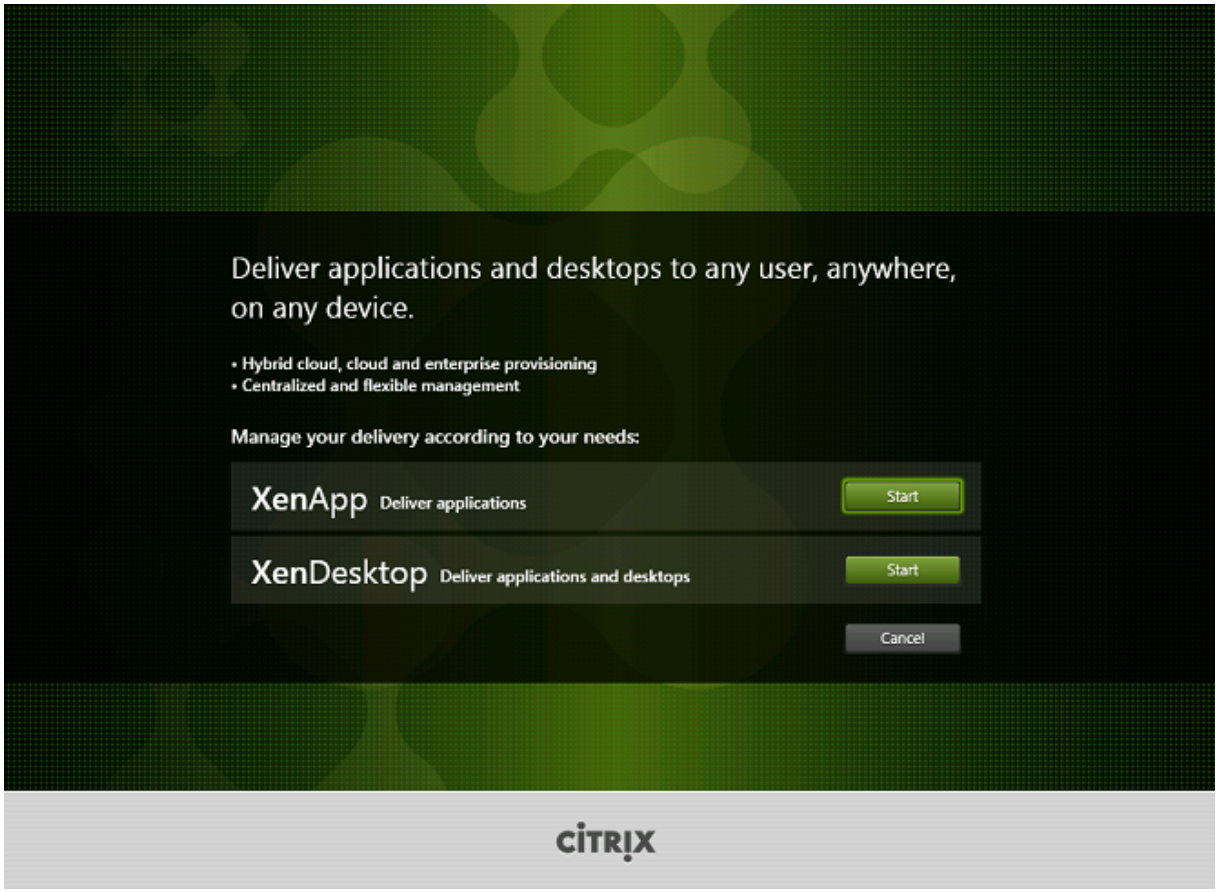
Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die XenApp und XenDesktop-Downloadseite auf. Laden Sie die ISO-Datei für das Produkt herunter.

Entpacken Sie die Datei. Optional können Sie die ISO-Datei auch auf DVD brennen.

Melden Sie sich mit einem lokalen Administratorkonto bei der Maschine an, auf der Sie die Komponenten installieren.

Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit. Wenn das Installationsprogramm nicht automatisch gestartet wird, doppelklicken Sie auf die Anwendung **AutoSelect** oder das bereitgestellte Laufwerk.

Schritt 2. Auswählen des zu installierenden Produkts

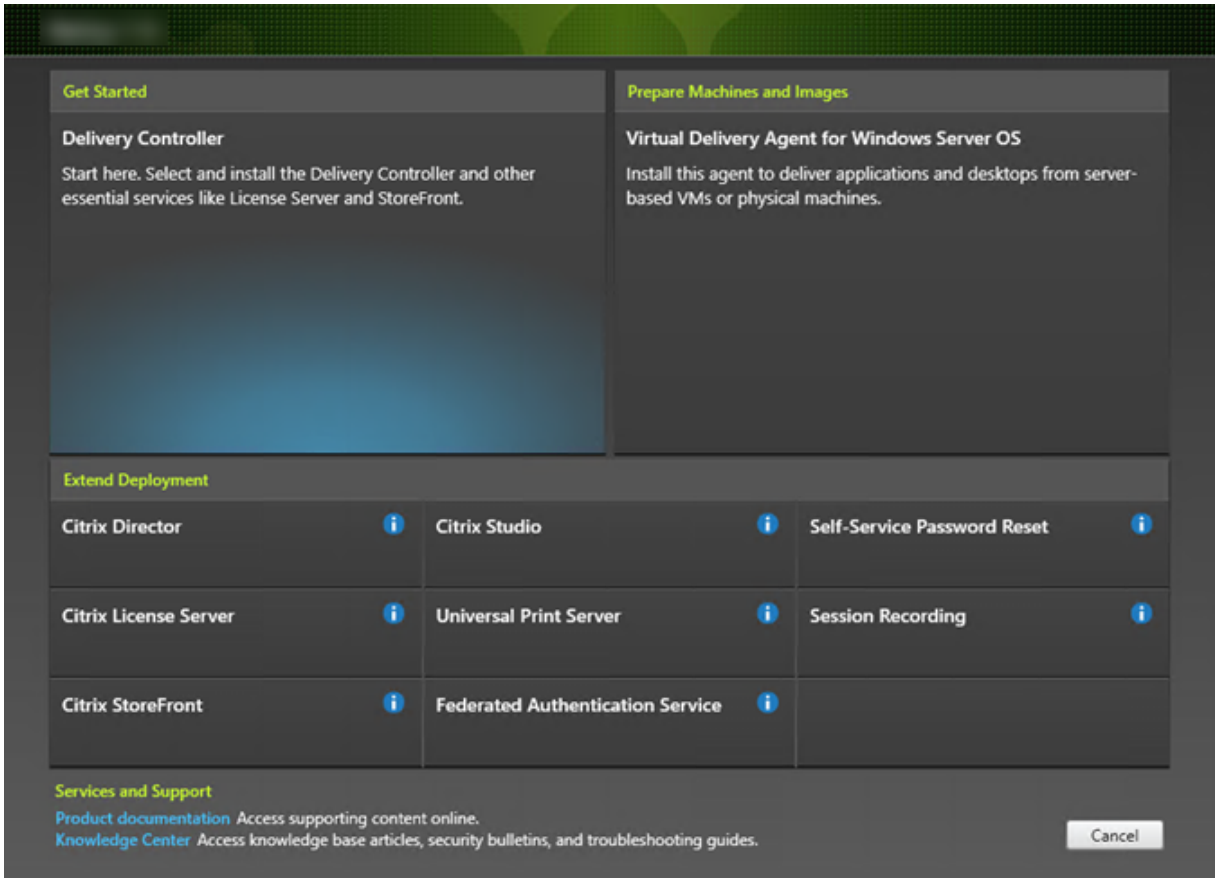


Klicken Sie auf **Start** neben dem zu installierenden Produkt: XenApp oder XenDesktop.

(Wenn auf der Maschine bereits XenApp- oder XenDesktop-Komponenten installiert sind, wird diese Seite nicht angezeigt.)

Befehlszeilenoption: /xenapp zur Installation von XenApp; XenDesktop wird installiert, wenn die Option ausgelassen wird.

Schritt 3. Auswählen der zu installierenden Komponente

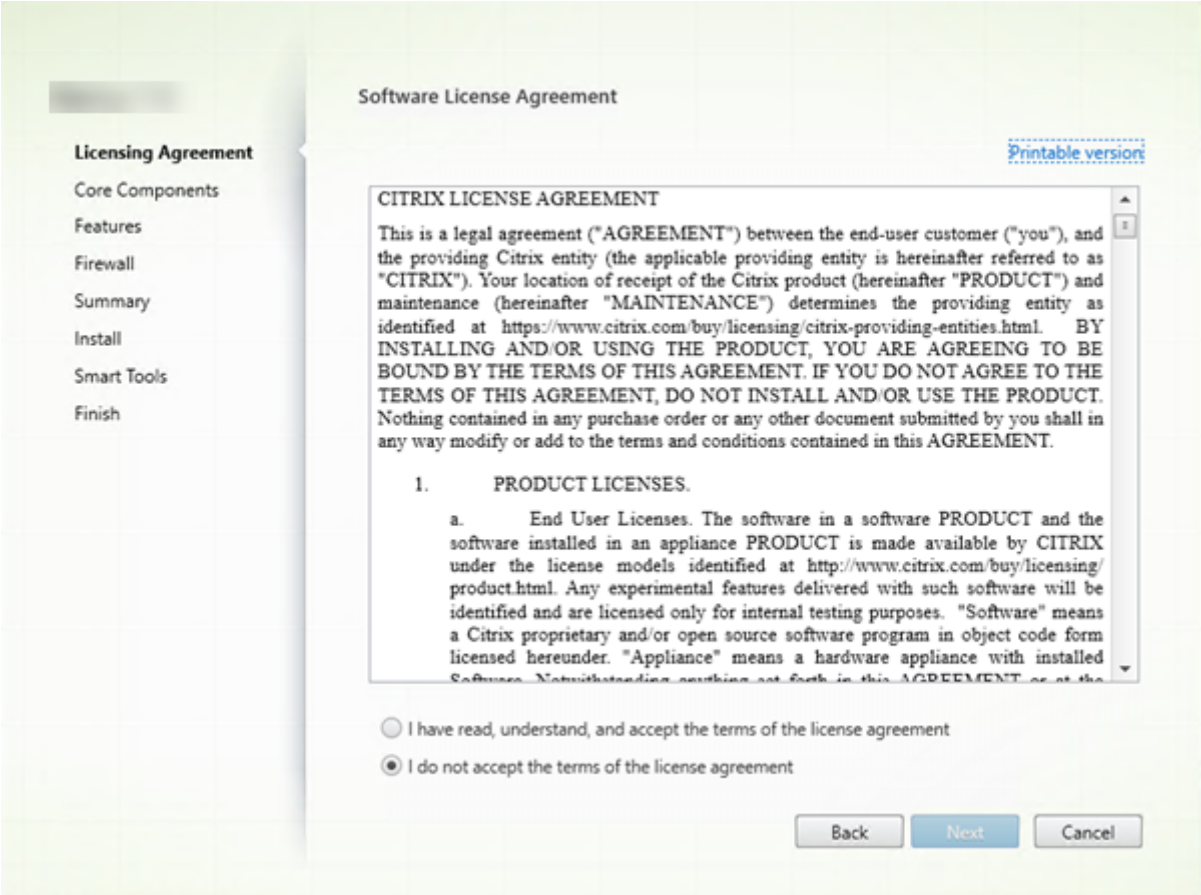


Wenn Sie ganz zu Beginn der Installation stehen, wählen Sie **Delivery Controller**. (Später wählen Sie die spezifischen Komponenten aus, die Sie auf dieser Maschine installieren.)

Wenn Sie bereits einen Controller auf dieser oder einer anderen Maschine installiert haben und eine andere Komponente installieren möchten, wählen Sie die Komponente im Bereich Erweitern der Bereitstellung aus.

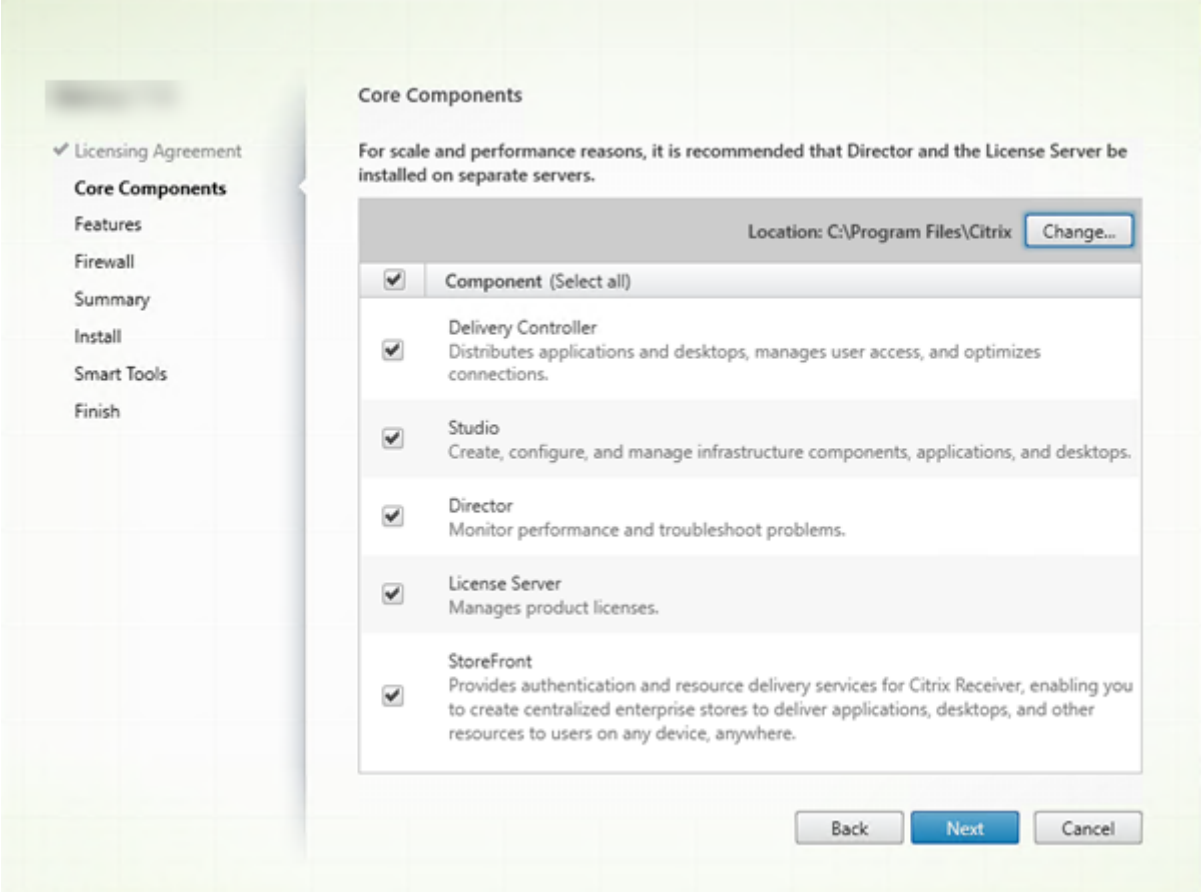
Befehlszeilenoption: /components

Schritt 4. Lesen und akzeptieren der Lizenzvereinbarung



Lesen Sie auf der Seite **Lizenzvereinbarung** die Lizenzvereinbarung und geben Sie an, dass Sie sie gelesen haben und ihr zustimmen. Klicken Sie auf **Weiter**.

Step 5. Auswählen der Komponenten und des Speicherorts für die Installation



Treffen Sie auf der Seite **Kernkomponenten** folgende Auswahl:

- **Speicherort:** Standardmäßig werden die Komponenten in C:\Programme\Citrix installiert. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Wenn Sie einen anderen Speicherort während der Installation angeben, muss dieser Ausführungsberechtigung für den Netzwerkdienst haben.
- **Komponenten:** Standardmäßig sind die Kontrollkästchen aller Kernkomponenten ausgewählt. Die Installation aller Kernkomponenten auf einem Server ist für Machbarkeitsstudien, Test- oder kleine Produktionsbereitstellungen geeignet. Für größere Produktionsumgebungen empfiehlt Citrix die Installation von Director, StoreFront und Lizenzserver auf eigenen Servern.

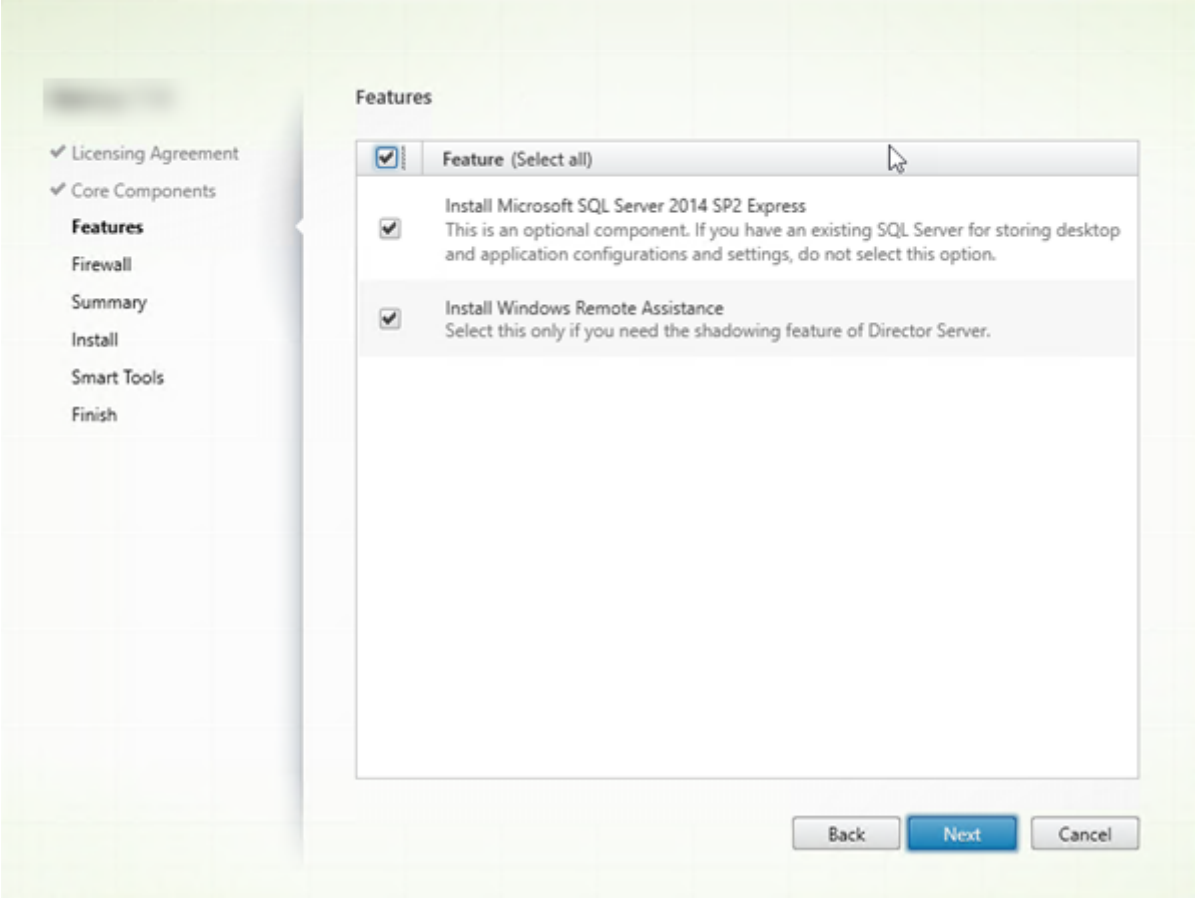
Wählen Sie nur die Komponenten, die Sie auf der Maschine installieren möchten. Nach Abschluss der Installation auf der Maschine können Sie das Installationsprogramm auf anderen Maschinen zum Installieren anderer Komponenten ausführen.

Wenn Sie eine erforderliche Kernkomponente nicht zur Installation auswählen, erscheint eine Warnung. Diese Warnung soll Sie lediglich an die Installation der Komponente erinnern, ihre Installation muss jedoch nicht zwingend auf der aktuellen Maschine erfolgen.

Klicken Sie auf **Weiter**.

Befehlszeilenoptionen: /installdir, /components, /exclude

Schritt 6. Aktivieren oder Deaktivieren von Features



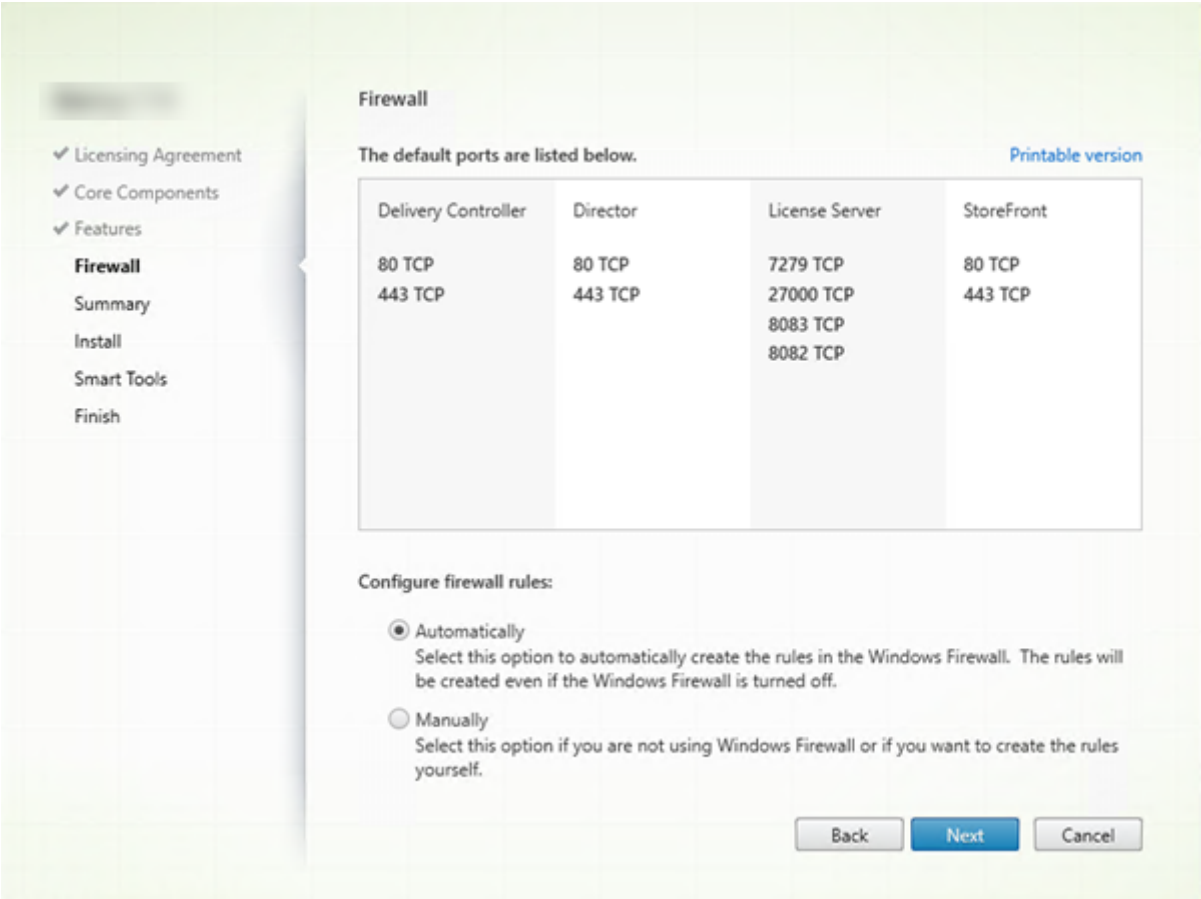
Auf der Seite **Features**:

- Wählen Sie aus, ob Microsoft SQL Server Express zur Verwendung als Sitedatenbank installiert werden soll. Diese Option ist standardmäßig aktiviert. Wenn Sie nicht mit den Datenbanken von XenApp und XenDesktop vertraut sind, lesen Sie die Informationen unter Datenbanken.
- Bei der Installation von Director wird die Microsoft-Remoteunterstützung automatisch installiert. Sie können wahlweise die Spiegelung in der Microsoft-Remoteunterstützung zur Verwendung mit der Director-Benutzerspiegelung aktivieren. Das Aktivieren der Spiegelung öffnet den TCP-Port 3389. Standardmäßig ist dieses Feature aktiviert. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Das Feature wird nur bei der Installation von Director angezeigt.

Klicken Sie auf **Weiter**.

Befehlszeilenoptionen: /nosql (zur Verhinderung der Installation), /no_remote_assistance (zur Verhinderung der Aktivierung)

Schritt 7. automatisches Öffnen der Windows-Firewallports



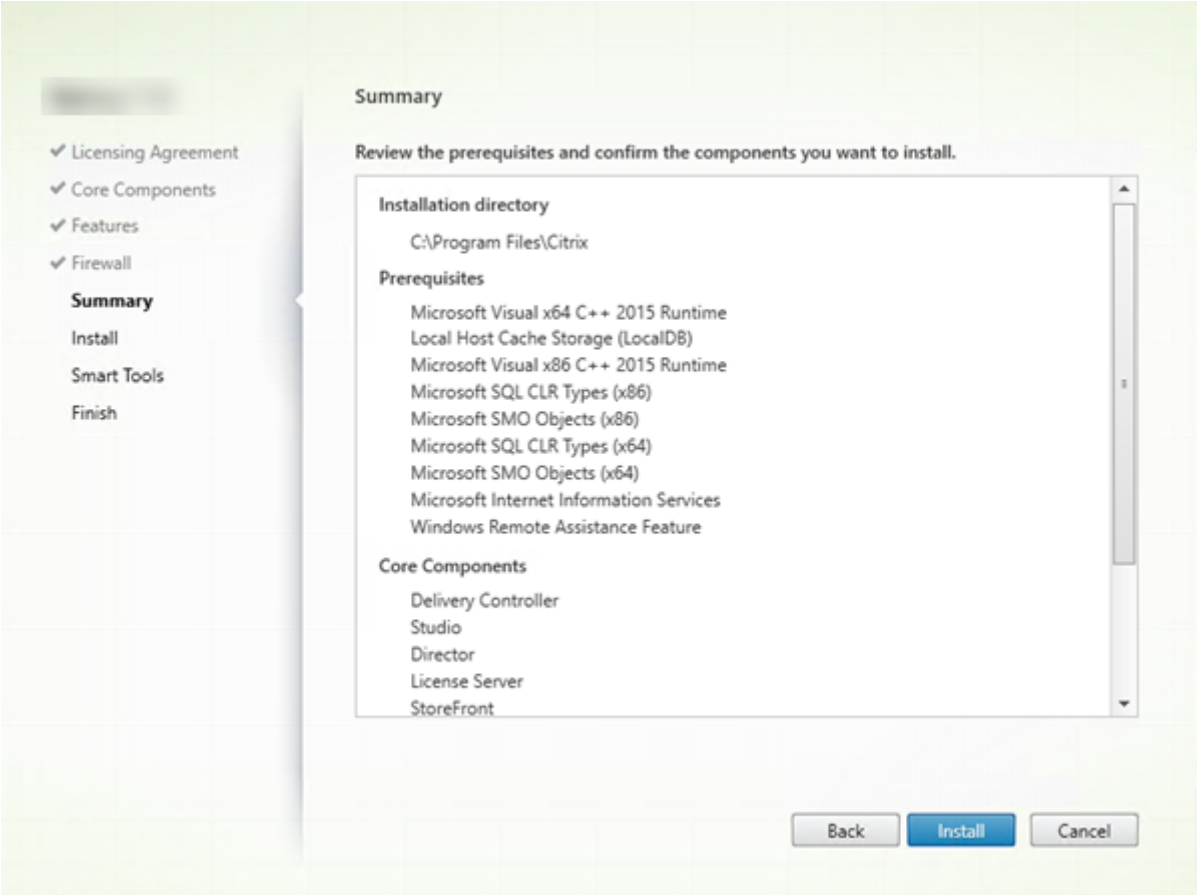
Standardmäßig werden die Ports auf der Seite **Firewall** automatisch geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

Klicken Sie auf **Weiter**.

(Die Abbildung zeigt die Portlisten in einem Szenario, in dem alle Kernkomponenten auf der aktuellen Maschine installiert werden. Diese Art der Installation wird in der Regel nur für Testzwecke durchgeführt.)

Befehlszeilenoption: /configure_firewall

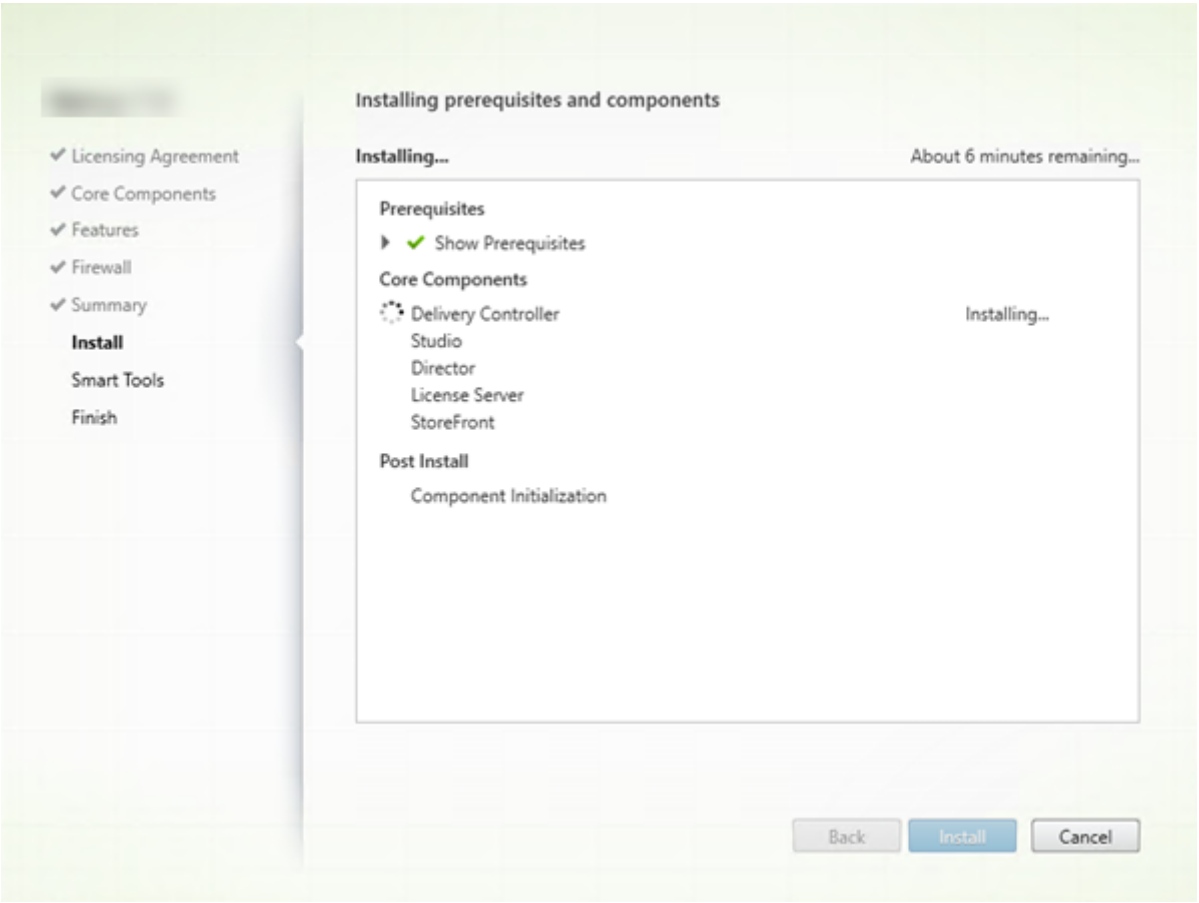
Schritt 8. Überprüfen der Voraussetzungen und Bestätigen der Installation



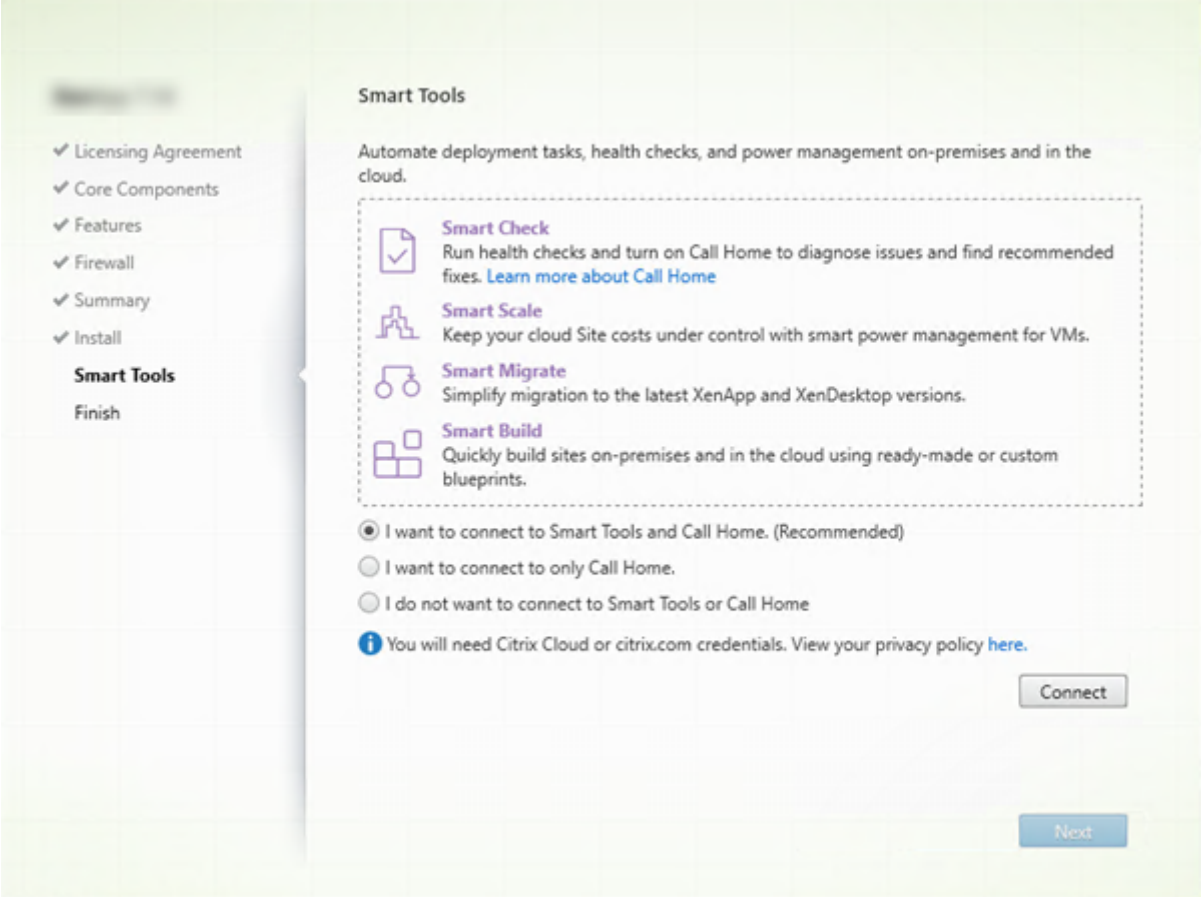
Auf der Seite **Zusammenfassung** wird aufgelistet, was installiert wird. Sie können mit der Schaltfläche Zurück zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern.

Wenn Sie fertig sind, klicken Sie auf **Installieren**.

Der Fortschritt der Installation wird angezeigt.



Schritt 9. Verbindung mit Smart Tools und Call Home



Bei Installation oder Upgrade eines Delivery Controllers enthält die Seite "Smart Tools"folgende Optionen:

- Mit Smart Tools und Call Home Verbindung herstellen: Dies ist die empfohlene Auswahl.
- Nur mit Call Home Verbindung herstellen: Während eines Upgrades wird diese Option nicht angezeigt, wenn Call Home bereits aktiviert ist oder wenn das Installationsprogramm einen Fehler im Zusammenhang mit dem Citrix Telemetriedienst findet.
- Weder mit Smart Tools noch Call Home Verbindung herstellen

Wenn Sie StoreFront (jedoch keinen Controller) installieren, zeigt der Assistent die Seite **Smart Tools** an. Wenn Sie andere Kernkomponenten als StoreFront und Controller installieren, werden die Seiten **Smart Tools** und **Call Home** nicht angezeigt.

Wenn Sie eine Option zur Verbindung mit Smart Tools und/oder Call Home wählen:

1. Klicken Sie auf **Verbinden**.
2. Geben Sie Ihre Citrix oder Citrix Cloud-Anmeldeinformationen an.
3. Wenn Ihre Anmeldeinformationen überprüft sind, wird ein Smart Agent-Zertifikat heruntergeladen. Nach dem erfolgreichen Abschluss dieses Vorgangs wird ein grünes Häkchen neben der

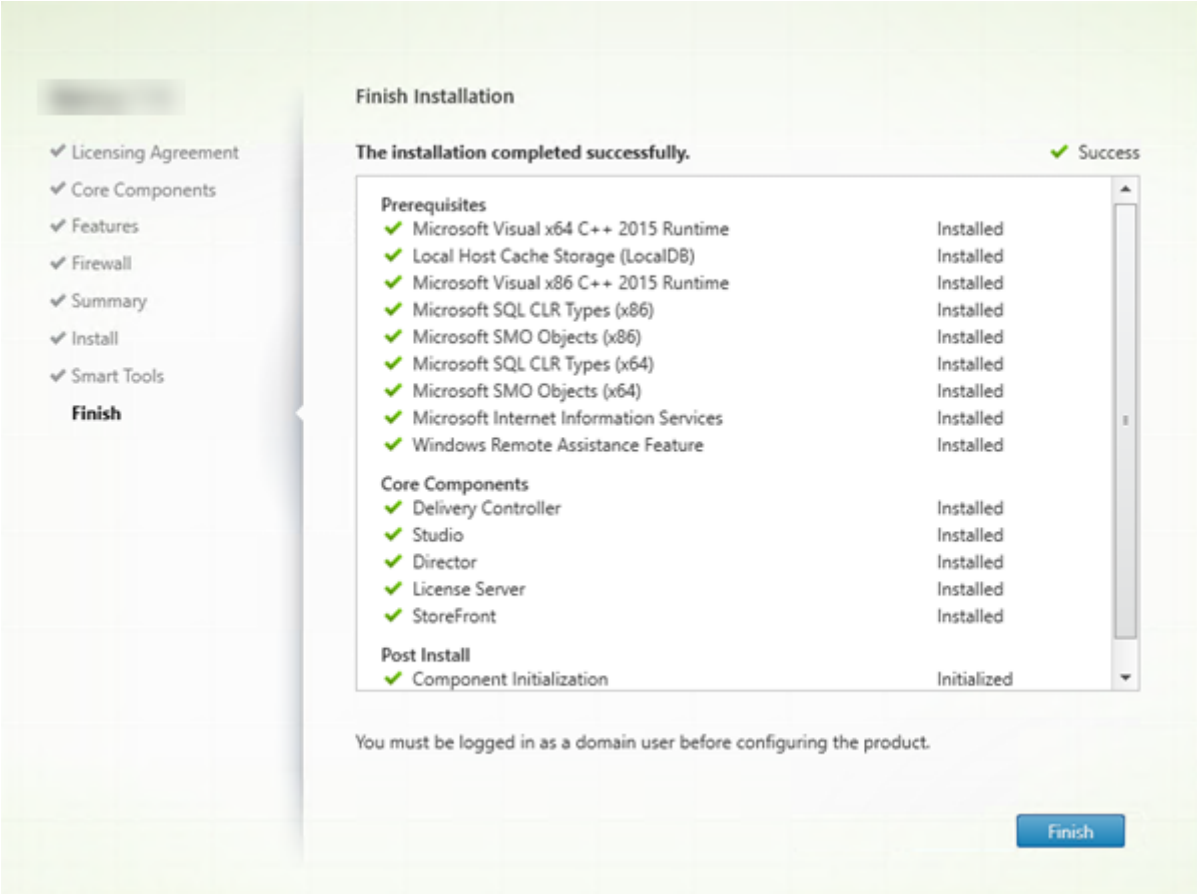
Schaltfläche **Verbinden** angezeigt. Wenn während des Vorgangs ein Fehler auftritt, ändern Sie Ihre Auswahl, sodass **weder mit Smart Tools noch Call Home** eine Verbindung hergestellt wird. Sie können sich später registrieren.

4. Klicken Sie auf **Weiter**, um mit dem Installationsassistenten fortzufahren.

Wenn Sie nicht teilnehmen möchten, klicken Sie auf **Weiter**.

Befehlszeilenoption: / exclude “Smart Tools Agent”(zum Verhindern der Installation)

Schritt 10. Abschließen der Installation



Die Seite **Fertigstellen** zeigt grüne Häkchen für alle Voraussetzungen und Komponenten, die erfolgreich installiert und initialisiert werden konnten.

Klicken Sie auf **Fertig stellen**.

Schritt 11: Installieren der verbleibenden Kernkomponenten auf anderen Maschinen

Wenn Sie alle Kernkomponenten auf einer Maschine installiert haben, fahren Sie mit Nächste Schritte fort. Andernfalls führen Sie das Installationsprogramm auf anderen Maschinen durch, um weitere

Kernkomponenten zu installieren. Sie können auch weitere Controller auf anderen Servern installieren.

Nächste Schritte

Wenn Sie alle erforderlichen Komponenten installiert haben, verwenden Sie Studio zum Erstellen einer Site.

Nach dem Erstellen der Site installieren Sie VDAs.

Sie können Ihre Bereitstellung jederzeit mit dem Produktinstallationsprogramm durch die folgenden Komponenten erweitern:

- Komponente des universellen Druckservers: Starten Sie das Installationsprogramm auf dem Druckerserver. Wählen Sie **Universeller Druckserver** im Bereich "Erweitern der Bereitstellung" . Akzeptieren Sie die Lizenzvereinbarung und fahren Sie fort bis zum Ende des Assistenten. Es sind keine weiteren Optionen auszuwählen. Anweisungen zum Installieren dieser Komponente über die Befehlszeile finden Sie unter Installieren über die Befehlszeile.
- Verbundauthentifizierungsdienst: siehe Verbundauthentifizierungsdienst.
- Self-Service Password Reset Service: siehe Dokumentation zu Self-Service Password Reset Service.

VDAs installieren

January 6, 2023

Es gibt zwei VDA-Typen für Windows-Maschinen: VDAs für Serverbetriebssysteme und VDAs für Desktopbetriebssysteme. Informationen zu VDAs für Linux-Maschinen finden Sie in der Dokumentation zu Linux Virtual Delivery Agent.

> **Wichtig:**
>
> Lesen Sie vor der Installation den Artikel Vorbereiten der Installation. Beispielsweise sollte die Maschine die aktuellen Windows-Updates haben. Wenn erforderliche Updates (etwa KB2919355) nicht vorhanden sind, schlägt die Installation fehl.

Vor der Installation von VDAs müssen Sie die Kernkomponenten installieren. Sie können auch die Site erstellen, bevor Sie die Installation durchführen.

Der vorliegende Abschnitt enthält Informationen zu der Reihenfolge der Schritte mit dem Installationsassistenten bei der Installation eines VDAs. Die entsprechenden Befehle für die Befehlszeile werden ebenfalls angegeben. Weitere Informationen finden Sie unter Installieren über die Befehlszeile.

Wenn eine VDA- oder Delivery Controller-Installation fehlschlägt, wird das Protokoll des fehlerhaften MSI von einem Analysetool analysiert und der exakte Fehlercode angezeigt. Das Tool empfiehlt einen CTX-Artikel, wenn es sich um ein bekanntes Problem handelt. Das Tool sammelt außerdem anonymisierte Daten über den Fehlercode. Diese Daten werden anderen, vom CEIP gesammelten Daten beigefügt. Wenn Sie die Registrierung beim CEIP beenden, werden die gesammelten MSI-Analysedaten nicht mehr an Citrix gesendet.

Schritt 1. Produktsoftware herunterladen und Assistent starten

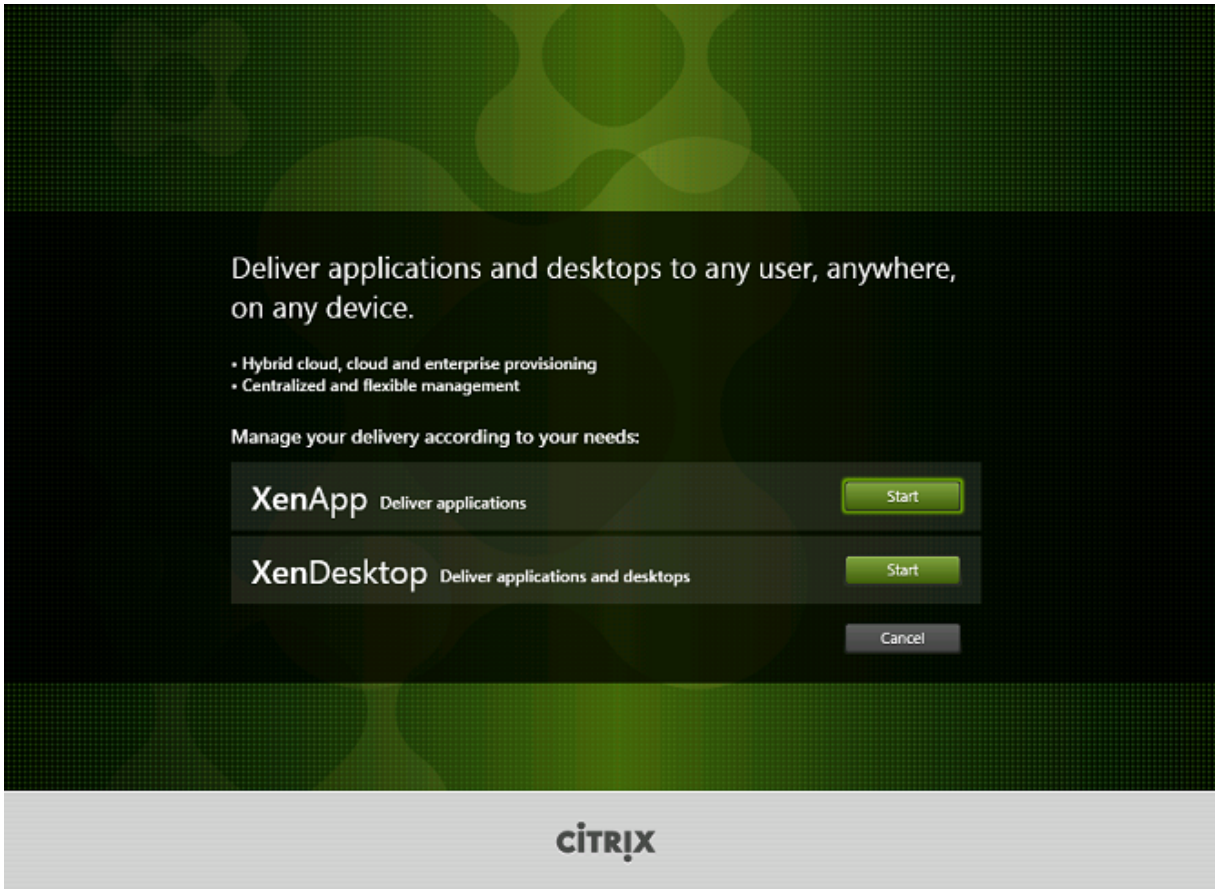
Produktinstallationsprogramm verwenden:

- Wenn Sie das XenApp und XenDesktop-ISO-Image noch nicht heruntergeladen haben:
  - Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die XenApp und XenDesktop-Downloadseite auf. Laden Sie die ISO-Datei für das Produkt herunter.
  - Entpacken Sie die Datei. Optional können Sie die ISO-Datei auch auf DVD brennen.
- Melden Sie sich bei der Maschine oder dem Image, auf der/dem der VDA installiert werden soll, als lokaler Administrator an. Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit. Wenn das Installationsprogramm nicht automatisch gestartet wird, doppelklicken Sie auf die Anwendung **AutoSelect** oder das bereitgestellte Laufwerk.
- Der Installationsassistent wird gestartet.

Eigenständiges Installationspaket verwenden:

- Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die XenApp und XenDesktop-Downloadseite auf. Laden Sie das benötigte Paket:
  - VDAServerSetup.exe: Serverbetriebssystem-VDA <Version>
  - VDAWorkstationSetup.exe: Desktopbetriebssystem-VDA <Version>
  - VDAWorkstationCoreSetup.exe: Desktopbetriebssystem-Kernkomponenten-VDA <Version>
- Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Als Administrator ausführen**.
- Der Installationsassistent wird gestartet.

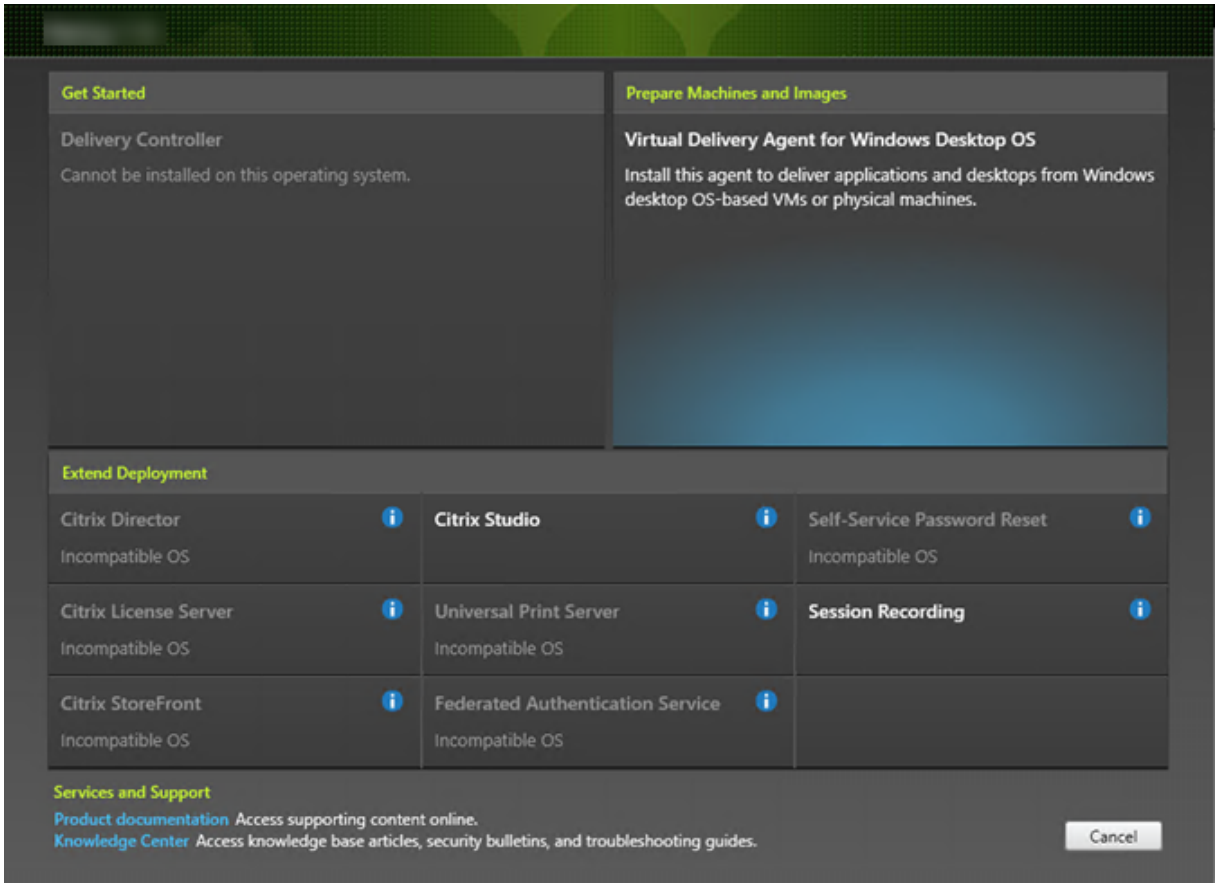
Schritt 2. Zu installierendes Produkt auswählen



Klicken Sie auf **Start** neben dem zu installierenden Produkt: XenApp oder XenDesktop. (Wenn auf der Maschine bereits eine XenApp und XenDesktop-Komponente installiert ist, wird diese Seite nicht angezeigt.)

Befehlszeilenoption: /xenapp zur Installation von XenApp; XenDesktop wird installiert, wenn die Option ausgelassen wird.

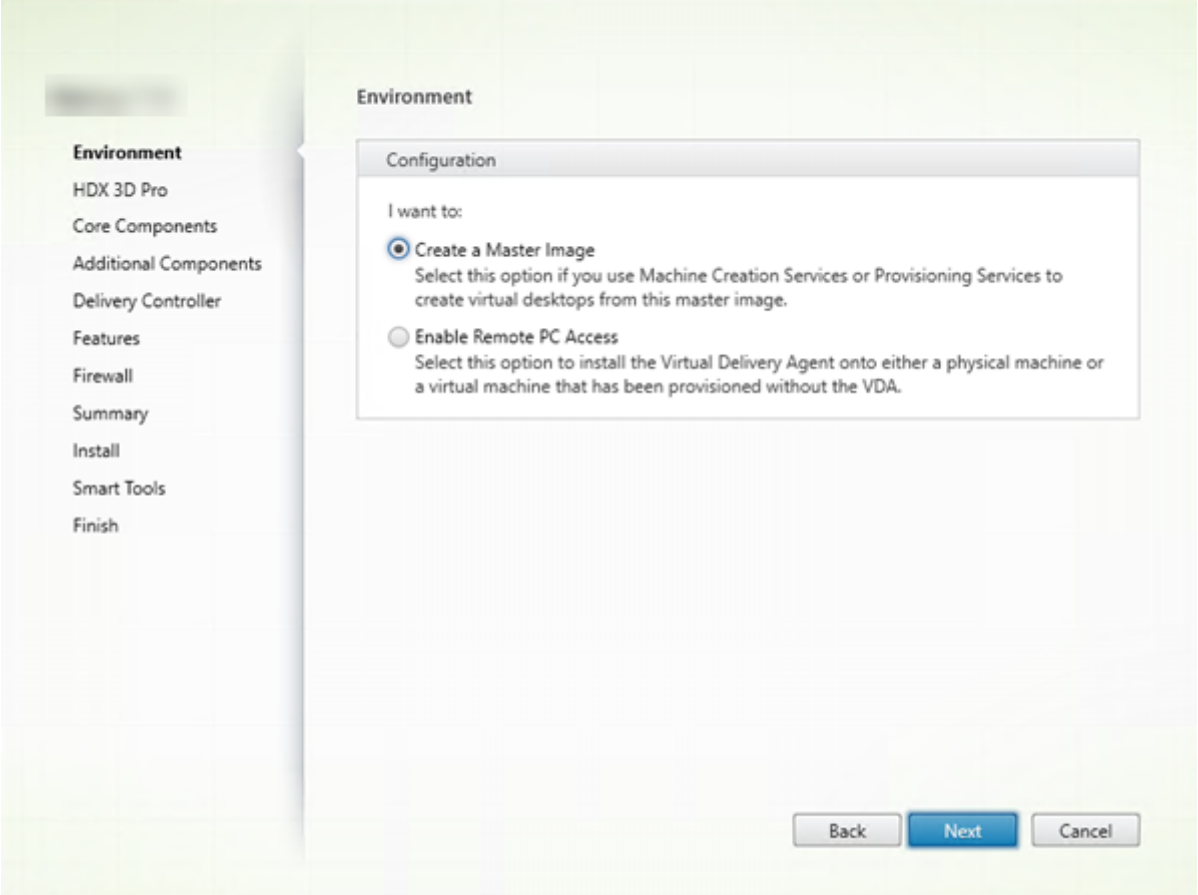
Schritt 3. VDA auswählen



Wählen Sie den Eintrag Virtual Delivery Agent. Das Installationsprogramm weiß, ob ein VDA unter einem Desktop- oder Serverbetriebssystem ausgeführt wird, und bietet daher nur einen VDA des richtigen Typs an.

Wenn das Installationsprogramm beispielsweise auf einer Windows 10-Maschine ausgeführt wird, wird der VDA für Desktopbetriebssysteme angeboten. Der VDA für Serverbetriebssysteme ist nicht verfügbar.

Schritt 4. Art der VDA-Verwendung angeben



Auf der Seite **Umgebung** legen Sie fest, wie der VDA verwendet werden soll. Wählen Sie eine der folgenden Optionen:

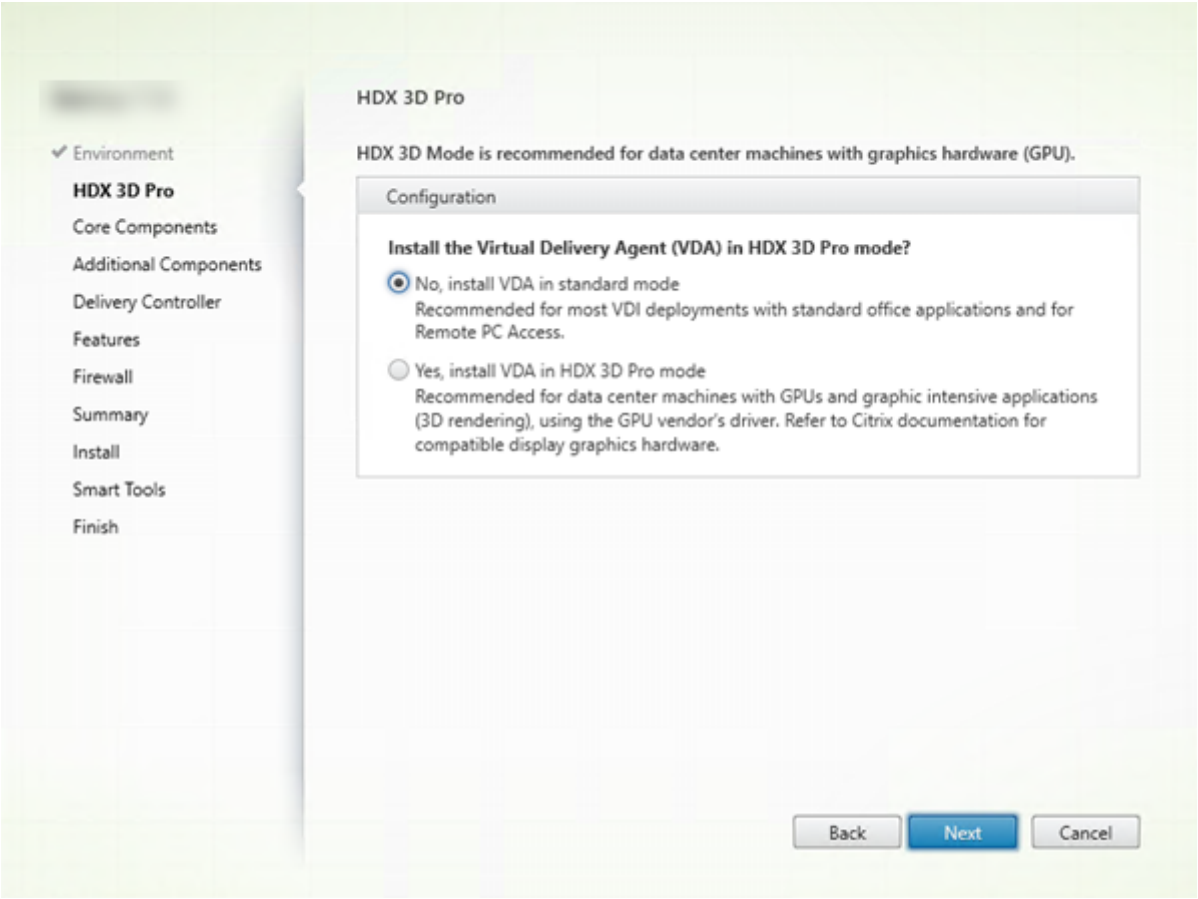
- **Masterimage:** (Standardwert) Der VDA wird auf einem Maschinenimage installiert. Sie verwenden anschließend Citrix Tools (Maschinenerstellungsdienste oder Provisioning Services) zum Erstellen von VMs aus diesem Masterimage.
- **Verbindungen mit einer Servermaschine aktivieren** (wenn die Installation auf einem Server erfolgt) oder **Remote-PC-Zugriff** (bei Installation auf einer Desktopmaschine): Sie installieren den VDA auf einer physischen Maschine oder auf einer ohne VDA bereitgestellten VM. Wenn Sie Remote-PC-Zugriff auswählen, werden die folgenden Komponenten nicht installiert/aktiviert:
  - App-V
  - Profilverwaltung
  - Maschinenidentitätsdienst
  - Personal vDisk

Klicken Sie auf **Weiter**.

Befehlszeilenoptionen: /masterimage, /remotepc

Wenn Sie das Installationsprogramm VDAWorkstationCoreSetup.exe verwenden, wird diese Seite nicht im Assistenten angezeigt und die Befehlszeilenoptionen sind nicht zulässig.

Schritt 5. Auswählen, ob HDX 3D Pro verwendet werden soll



Die Seite **HDX 3D Pro** wird nur angezeigt, wenn Sie einen VDA für Desktopbetriebssysteme installieren.

- Der VDA-Standardmodus wird für die meisten Desktops empfohlen, einschließlich solcher mit aktiviertem Microsoft RemoteFX. Der VDA-Standardmodus ist die Standardeinstellung.
- Der HDX 3D Pro-Modus dient zur Optimierung der Leistung grafikintensiver Programme und Anwendungen sowie Anwendungen mit hohem Multimedia-Anteil. Der HDX 3D Pro-Modus wird empfohlen, wenn die Maschine zur 3D-Wiedergabe auf einen Grafikprozessor zugreift.
- Für Remote-PC-Zugriff ist der VDA normalerweise mit dem VDA-Standardmodus konfiguriert. Für Remote-PC-Zugriff, der mit HDX 3D Pro konfiguriert ist, wird das Ausblenden des Bildschirms für folgende GPUs unterstützt:
  - Intel Iris Pro Graphics und Intel HD Graphics 5300 und höher (Intel Core-Prozessoren der 5. Generation und Intel Core i5-Prozessoren der 6. Generation)

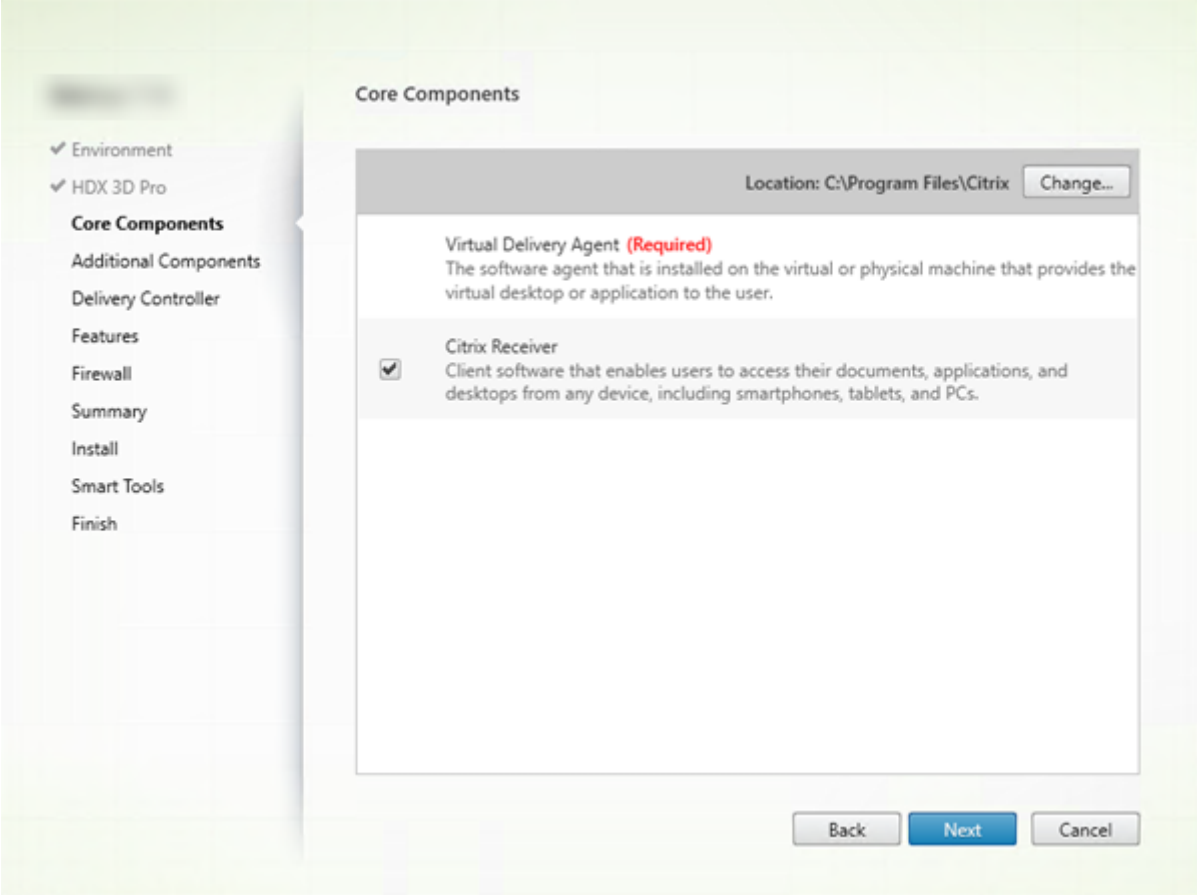
- NVIDIA Quadro- und NVIDIA GRID-GPUs
- AMD RapidFire

Standardmodus	HDX 3D Pro-Modus
Normalerweise am besten für virtuelle Desktops ohne Grafikhardwarebeschleunigung und für Remote-PC-Zugriff geeignet.	Normalerweise am besten geeignet für Desktops in Datencentern mit Grafikhardwarebeschleunigung, wenn nicht mehr als vier Monitore benötigt werden.
Für Remote-PC-Zugriff kann jede GPU verwendet werden. Allerdings mit einigen Abstrichen bei der App-Kompatibilität: Unter **Windows 7, 8 und 8.1** ist GPU-Beschleunigung für DirectX-Featureebenen bis 9.3 möglich. Einige DirectX 10, 11, 12-Anwendungen können u. U. nicht ausgeführt werden, wenn sie kein Fallback auf DirectX 9 tolerieren. **Unter Windows 10** steht die GPU-Beschleunigung für DirectX 10-, 11- und 12-Apps im Fenstermodus zur Verfügung. DX 9-Apps werden über WARP wiedergegeben. DX-Apps können nicht im Vollbildmodus verwendet werden.	Unterstützt GPU-Beschleunigung für alle GPUs. Das Ausblenden der Konsole, nicht standardmäßige Bildschirmauflösungen und echte Unterstützung für mehrere Bildschirme erfordern jedoch NVIDIA GRID, Intel Iris Pro Graphics oder AMD RapidFire Graphics. Verwendet den Grafiktreiber des Herstellers, der die umfassendste Anwendungskompatibilität bietet: **Alle 3D-APIs (DirectX oder OpenGL)**, die die GPU unterstützt. Unterstützung für **Vollbild-3D-App** mit Intel Iris Pro (nur Windows 10), NVIDIA GRID und AMD RapidFire.**Unterstützung für benutzerdefinierte Treibererweiterungen und APIs**. Beispiel: CUDA oder OpenCL.
OpenGL-Anwendungsbeschleunigung in Remotesitzungen, wenn vom GPU-Hersteller unterstützt (derzeit nur NVIDIA).	
Beliebige Monitorauflösungen (Limit hängt von Windows-Betriebssystem und Leistung ab) und bis zu acht Monitore.	Unterstützt bis zu vier Monitore.
H.264-Hardwarecodierung ist mit Intel Iris Pro-Grafikprozessoren verfügbar.	H.264-Hardwarecodierung ist mit NVIDIA-Smartcards verfügbar.

Klicken Sie auf **Weiter**.

Befehlszeilenoption: /enable_hdx_3d_pro

Schritt 6. Auswählen der Komponenten und des Speicherorts für die Installation



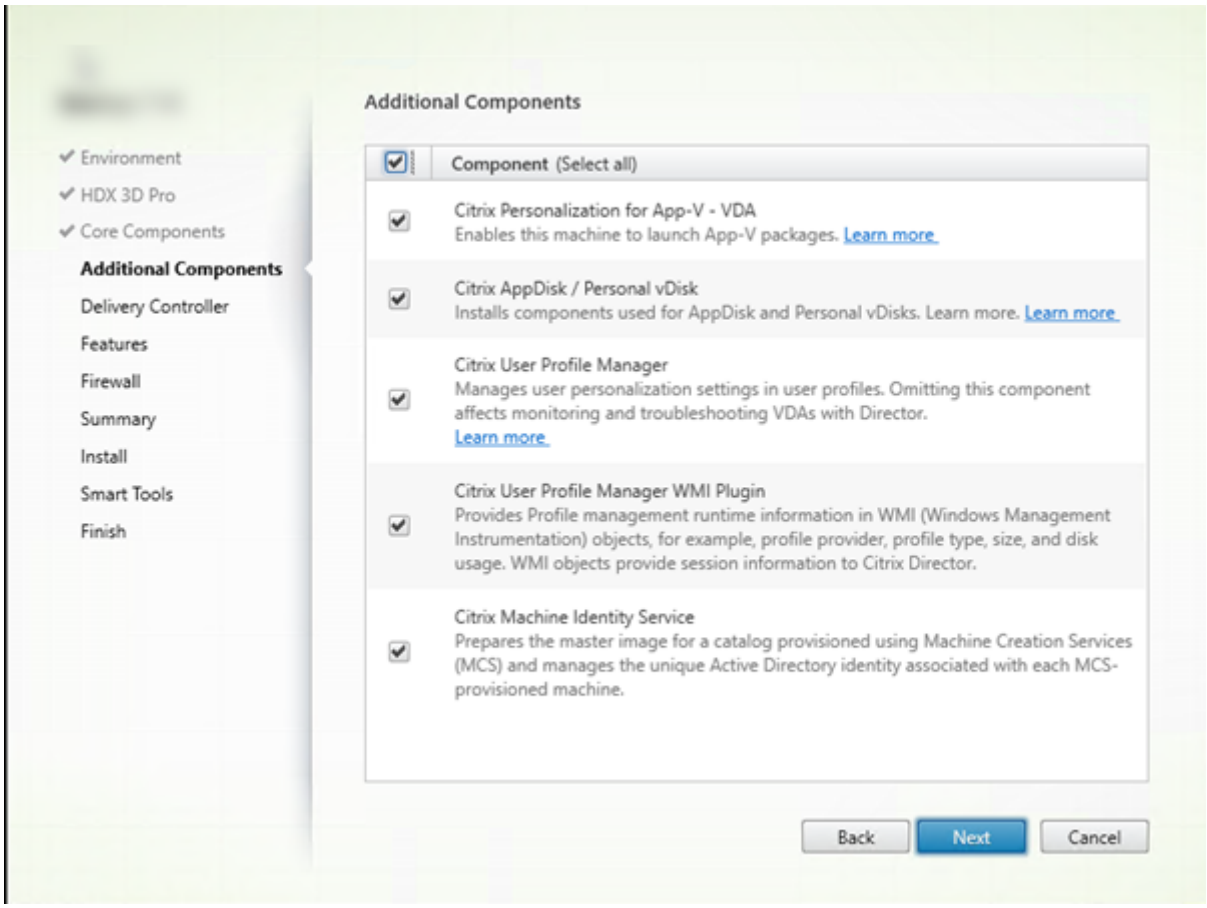
Treffen Sie auf der Seite **Kernkomponenten** folgende Auswahl:

- **Speicherort:** Standardmäßig werden die Komponenten in C:\Programme\Citrix installiert. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Wenn Sie einen anderen Speicherort während der Installation angeben, muss dieser Speicherort Ausführenberechtigung für den Netzwerkdienst haben.
- **Komponenten:** Citrix Receiver für Windows wird standardmäßig mit dem VDA installiert (es sei denn, Sie verwenden das Installationsprogramm VDAWorkstationCoreSetup.exe). Deaktivieren Sie das Kontrollkästchen, wenn Citrix Receiver nicht installiert werden soll. Wenn Sie das Installationsprogramm VDAWorkstationCoreSetup.exe verwenden, wird Citrix Receiver für Windows nie installiert, daher wird dieses Kontrollkästchen nicht angezeigt.

Klicken Sie auf **Weiter**.

Befehlszeilenoptionen: /installdir, "/components vda", um die Installation von Citrix Receiver für Windows zu verhindern

Schritt 7. Installation zusätzlicher Komponenten



Die Seite **Zusätzliche Komponenten** enthält Kontrollkästchen zum Aktivieren oder Deaktivieren der Installation weiterer Features und Technologien mit dem VDA. Die Seite wird in folgenden Fällen nicht angezeigt:

- Bei Verwendung des Installationsprogramms VDAWorkstationCoreSetup.exe. Außerdem sind die Befehlszeilenoptionen für die zusätzlichen Komponenten mit diesem Installationsprogramm nicht gültig.
- Beim Upgrade eines VDAs, wenn alle zusätzlichen Komponenten bereits installiert sind. (Wenn einige zusätzliche Komponenten installiert sind, werden auf der Seite nur diejenigen angezeigt, die noch nicht installiert wurden.)

Citrix Personalisierung für App-V:

Installieren Sie diese Komponente zur Verwendung von Anwendungen aus Microsoft App-V-Paketen. Einzelheiten finden Sie unter App-V.

Befehlszeilenoption: /exclude “Citrix Personalization for App-V –VDA”zum Verhindern der Komponenteninstallation.

Citrix AppDisk / Personal vDisk:

Nur bei Installation von VDAs für Desktopbetriebssysteme auf einer VM zulässig. Installiert die Komponenten für AppDisk und PvD. Weitere Informationen finden Sie unter AppDisks und Personal vDisk.

Befehlszeilenoption: /exclude "Personal vDisk", um die Installation der Komponenten AppDisk und Personal vDisk zu verhindern.

Citrix Profilverwaltung:

Diese Komponente verwaltet die Einstellungen für Benutzeranpassungen in Benutzerprofilen. Einzelheiten finden Sie unter Profilverwaltung.

Das Ausschließen der Citrix Profilverwaltung bei der Installation hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs mit Citrix Director. Auf den Seiten Benutzerdetails und Endpunkt treten Fehler in den Bereichen "Personalisierung"und "Anmeldedauer"auf. Auf den Seiten "Dashboard"und "Trends"werden im Bereich "Durchschnittliche Anmeldedauer"nur Daten für Maschinen angezeigt, auf denen Profilverwaltung installiert ist.

Selbst bei Verwendung der Profilverwaltungslösung eines Drittanbieters empfiehlt Citrix, dass Sie die Citrix Profilverwaltung installieren und ausführen. Das Aktivieren der Citrix Profilverwaltung ist nicht erforderlich.

Befehlszeilenoption: /exclude "Citrix User Profile Manager"zum Verhindern der Komponenteninstallation.

Citrix Profile Management WMI Plug-In:

Dieses Plug-In stellt Laufzeitinformationen zur Profilverwaltung in WMI-Objekten (Windows Management Instrumentation) bereit, z. B. Profilanbieter, Profiltyp, Größe und Datenträgernutzung. WMI-Objekte stellen Sitzungsinformationen für Citrix Director bereit.

Befehlszeilenoption: /exclude "Citrix User Profile Manager WMI Plugin"zum Verhindern der Komponenteninstallation.

Citrix Maschinenidentitätsdienst:

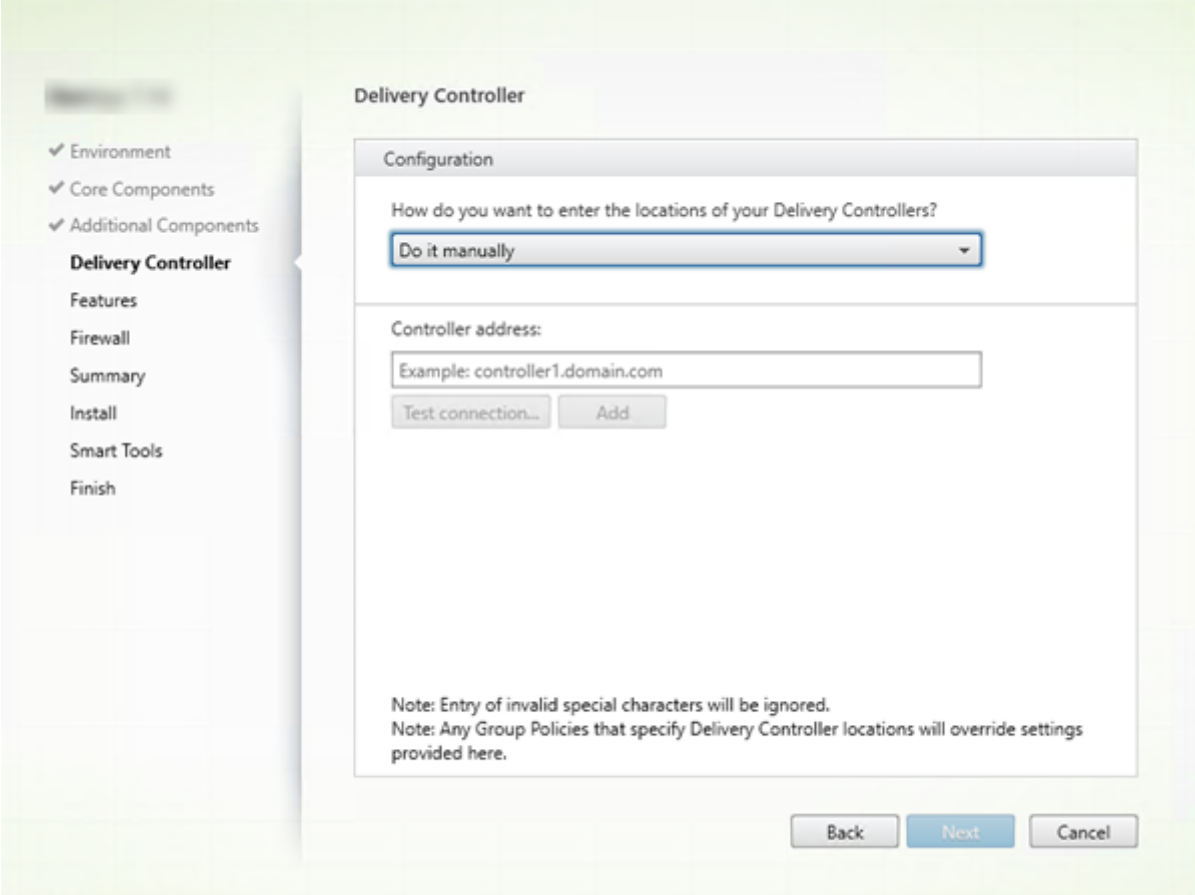
Dieser Dienst bereitet das Masterimage für einen per MCS bereitgestellten Katalog vor. Er verwaltet außerdem die eindeutige Active Directory-Identität jeder bereitgestellten Maschine.

Befehlszeilenoption: /exclude "Machine Identity Service"zum Verhindern der Komponenteninstallation

Standardwerte der grafischen Benutzeroberfläche:

- Wenn Sie auf der Seite **Umgebung** "Masterimage erstellen"auswählen (Schritt 4), werden Elemente auf der Seite **Zusätzliche Komponenten** standardmäßig aktiviert.
- Bei Auswahl von "Remote-PC-Zugriff aktivieren"oder "Verbindungen mit einer Servermaschine aktivieren"auf der Seite **Umgebung** werden auf der Seite **Zusätzliche Komponenten** Elemente standardmäßig deaktiviert.

Schritt 8. Delivery Controller-Adressen



Wählen Sie auf der Seite **Delivery Controller**, wie Sie die Adressen der installierten Controller angeben möchten. Citrix empfiehlt, die Adressen während der VDA-Installation einzugeben (Wahl von "Manuell"). Der VDA kann ohne diese Informationen nicht bei einem Controller registriert werden. Wenn der VDA nicht registriert werden kann, können die Benutzer nicht auf Anwendungen und Desktops auf dem VDA zugreifen.

- **Manuell** (Standard): Geben Sie den FQDN eines installierten Controllers ein und klicken Sie auf **Hinzufügen**. Wenn Sie weitere Controller installiert haben, fügen Sie deren Adressen hinzu.
- **Später (erweitert):** Wenn Sie diese Option auswählen, müssen Sie Ihre Wahl bestätigen, bevor Sie fortfahren können. Zur Angabe von Adressen zu einem späteren Zeitpunkt können Sie entweder das Installationsprogramm erneut ausführen oder die Citrix Gruppenrichtlinie verwenden. Eine entsprechende Erinnerung wird auf der Seite **Zusammenfassung** des Assistenten angezeigt.
- **Standorte aus Active Directory auswählen:** Dies ist nur zulässig, wenn die Maschine zu einer Domäne gehört und der Benutzer ein Domänenbenutzer ist.
- **Automatische Erstellung durch Maschinenerstellungsdienste:** Dies ist nur zulässig, wenn Sie Maschinen mit Maschinenerstellungsdienste bereitstellen.

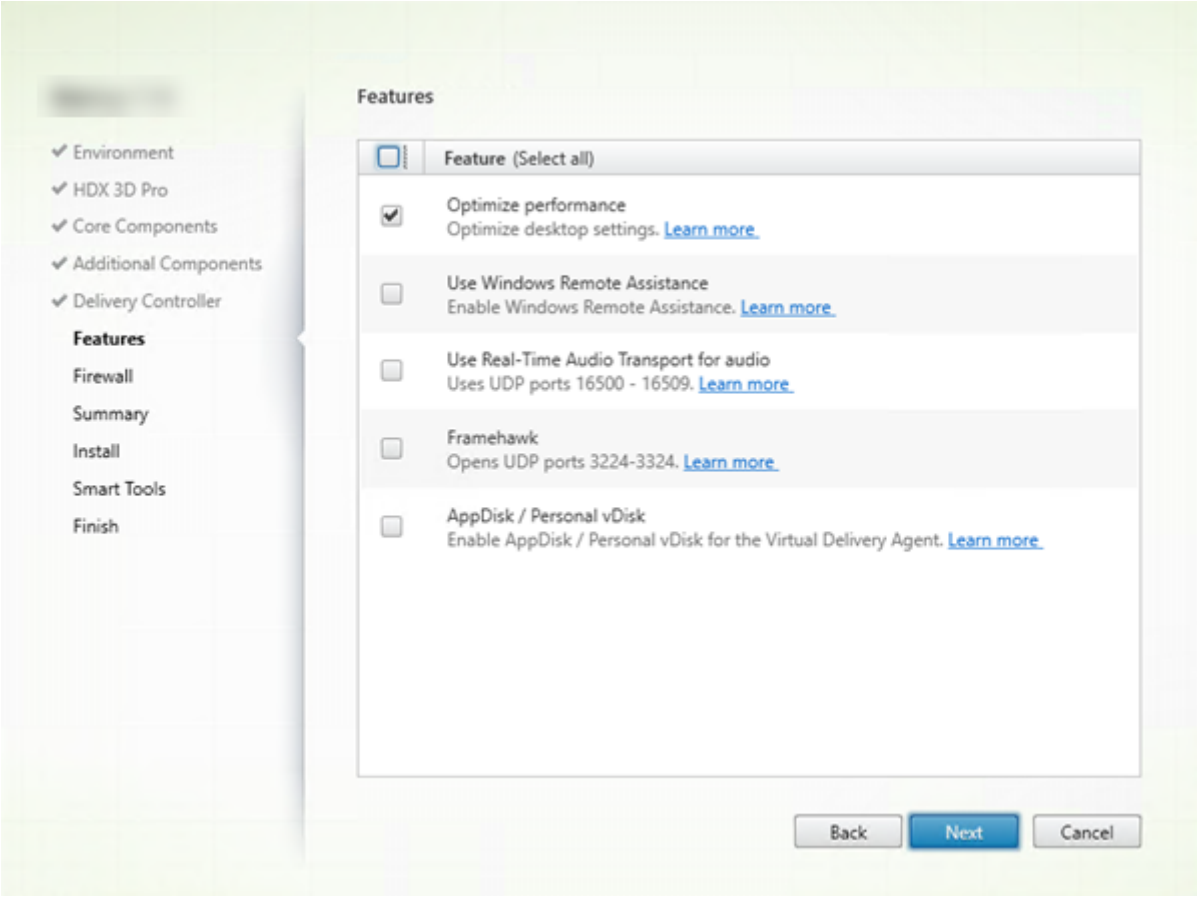
Klicken Sie auf **Weiter**. Wenn Sie “Später (erweitert)”wählen, müssen Sie bestätigen, dass Sie die Controlleradressen später angeben.

Andere Überlegungen

- Die Adresse darf folgende Zeichen nicht enthalten: { | } ~ [\ ] ^ ‘: ; < = > ? & @ ! “# $ % ( ) + / ,
- Wenn Sie Adressen bei der VDA-Installation und in der Gruppenrichtlinie festlegen, haben die Richtlinieneinstellungen Vorrang vor den bei der Installation festgelegten Einstellungen.
- Zur VDA-Registrierung müssen außerdem die Firewallports für die Kommunikation mit dem Controller geöffnet sein. Diese Aktion ist standardmäßig auf der Seite **Firewall** des Assistenten aktiviert.
- Nach der Angabe von Controlleradressen (bei oder nach der VDA-Installation) können Sie das Feature für die automatische Aktualisierung der VDAs verwenden, wenn Controller installiert oder entfernt werden. Einzelheiten dazu, wie VDAs Controller erkennen und sich dort registrieren, finden Sie unter Delivery Controller.

Befehlszeilenoption: /controllers

Schritt 9. Aktivieren oder Deaktivieren von Features



Verwenden Sie auf der Seite **Features** die Kontrollkästchen, um die Features zu aktivieren oder zu deaktivieren, die Sie verwenden möchten.

Leistung optimieren:

Nur bei Installation auf einer VM (nicht auf einem physischen Computer) zulässig. Wenn diese Funktion aktiviert ist (= Standardeinstellung), wird das Optimierungstool für VDAs verwendet, die auf einer VM auf einem Hypervisor ausgeführt werden. Die VM-Optimierung umfasst das Deaktivieren von Offlinedateien, das Deaktivieren der Hintergrunddefragmentierung und die Verkleinerung der Ereignisprotokollgröße. Einzelheiten finden Sie unter CTX224676.

Befehlszeilenoption: /optimize

Wenn Sie das Installationsprogramm VDAWorkstationCoreSetup.exe verwenden, wird dieses Feature nicht im Assistenten angezeigt und die Befehlszeilenoption ist nicht zulässig. Wenn Sie ein anderes Installationsprogramm in einer Remote-PC-Zugriff-Umgebung verwenden, deaktivieren Sie dieses Feature.

Windows-Remoteunterstützung verwenden:

Wenn dieses Feature aktiviert ist, wird die Windows-Remoteunterstützung mit dem Feature zum Spiegeln von Benutzern von Director verwendet. Die Windows-Remoteunterstützung öffnet die dynamischen Ports in der Firewall. (Standard = deaktiviert)

Befehlszeilenoption: /enable_remote_assistance

Echtzeitaudioübertragung für Audio verwenden:

Aktivieren Sie dieses Feature, wenn im Netzwerk häufig VoIP verwendet wird. Das Feature verringert die Latenz und verbessert die Audioresilienz in verlustreichen Netzwerken. Es ermöglicht die Datenübertragung mit RTP über UDP. (Standard = deaktiviert)

Befehlszeilenoption: /enable_real_time_transport

Framehawk:

Wenn dieses Feature aktiviert ist, werden die bidirektionalen UDP-Ports 3224–3324 geöffnet. (Standard = deaktiviert)

Sie können den Portbereich zu einem späteren Zeitpunkt mit der Citrix Richtlinieneinstellung “Portbereich für Framehawk-Anzeigekanal”ändern. In diesem Fall müssen Sie lokale Firewallports öffnen. In allen internen Firewalls (VDA an Citrix Receiver oder NetScaler Gateway) und allen externen Firewalls (NetScaler Gateway an Citrix Receiver) muss ein UDP-Netzwerkpfad geöffnet sein. Wenn Sie NetScaler Gateway bereitstellen, werden Framehawk-Datagramme mit DTLS verschlüsselt (Standard-UDP-Port 443). Weitere Informationen finden Sie unter Framehawk.

Befehlszeilenoption: /enable_framehawk_port

AppDisk und Personal vDisk:

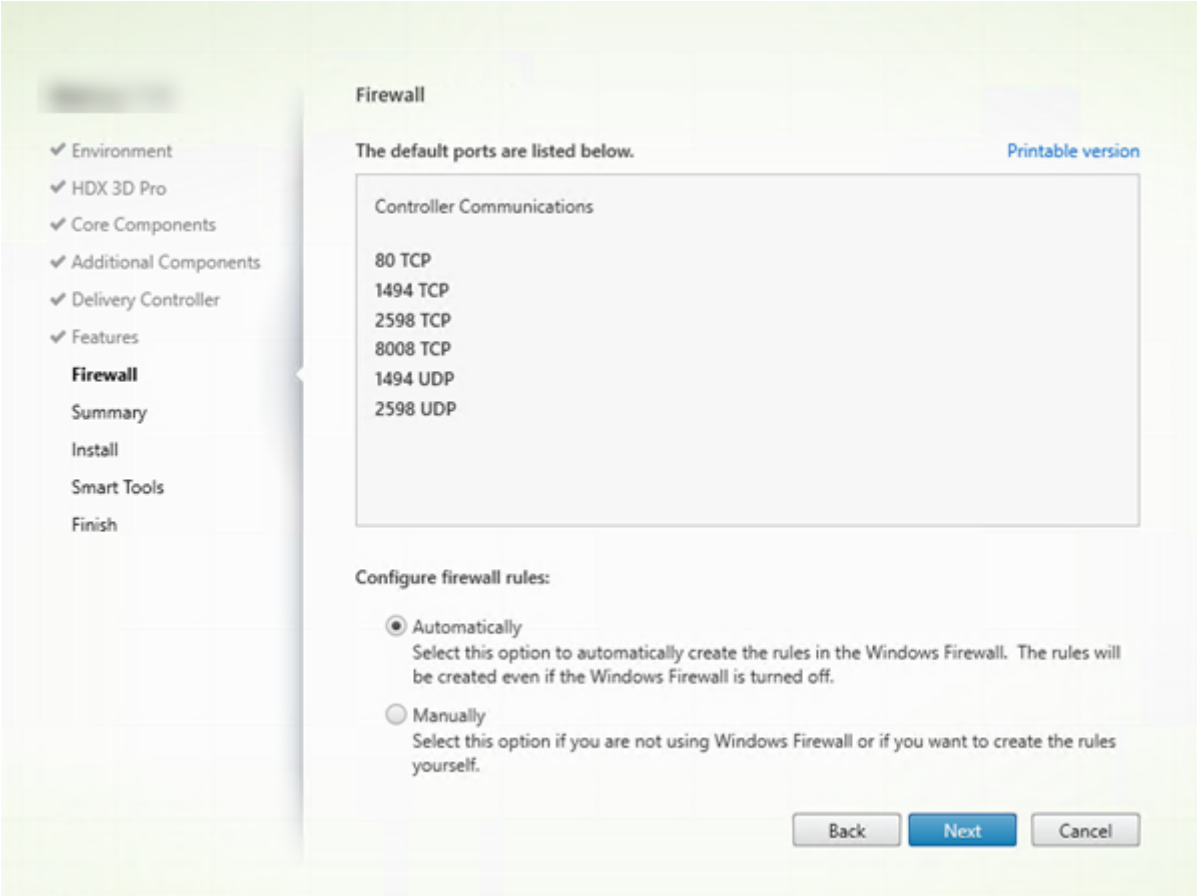
Nur bei Installation von VDAs für Desktopbetriebssysteme auf einer VM zulässig. Das Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen "Citrix AppDisk/Personal vDisk"auf der Seite **Zusätzliche Komponenten** aktiviert wird. Wenn dieses Kontrollkästchen aktiviert ist, können AppDisks und persönliche vDisks verwendet werden. Einzelheiten finden Sie unter AppDisks und Personal vDisk.

Befehlszeilenoption: /baseimage

Wenn Sie das Installationsprogramm VDAWorkstationCoreSetup.exe verwenden, wird dieses Feature nicht im Assistenten angezeigt und die Befehlszeilenoption ist nicht zulässig.

Klicken Sie auf **Weiter**.

Schritt 10. Firewallports

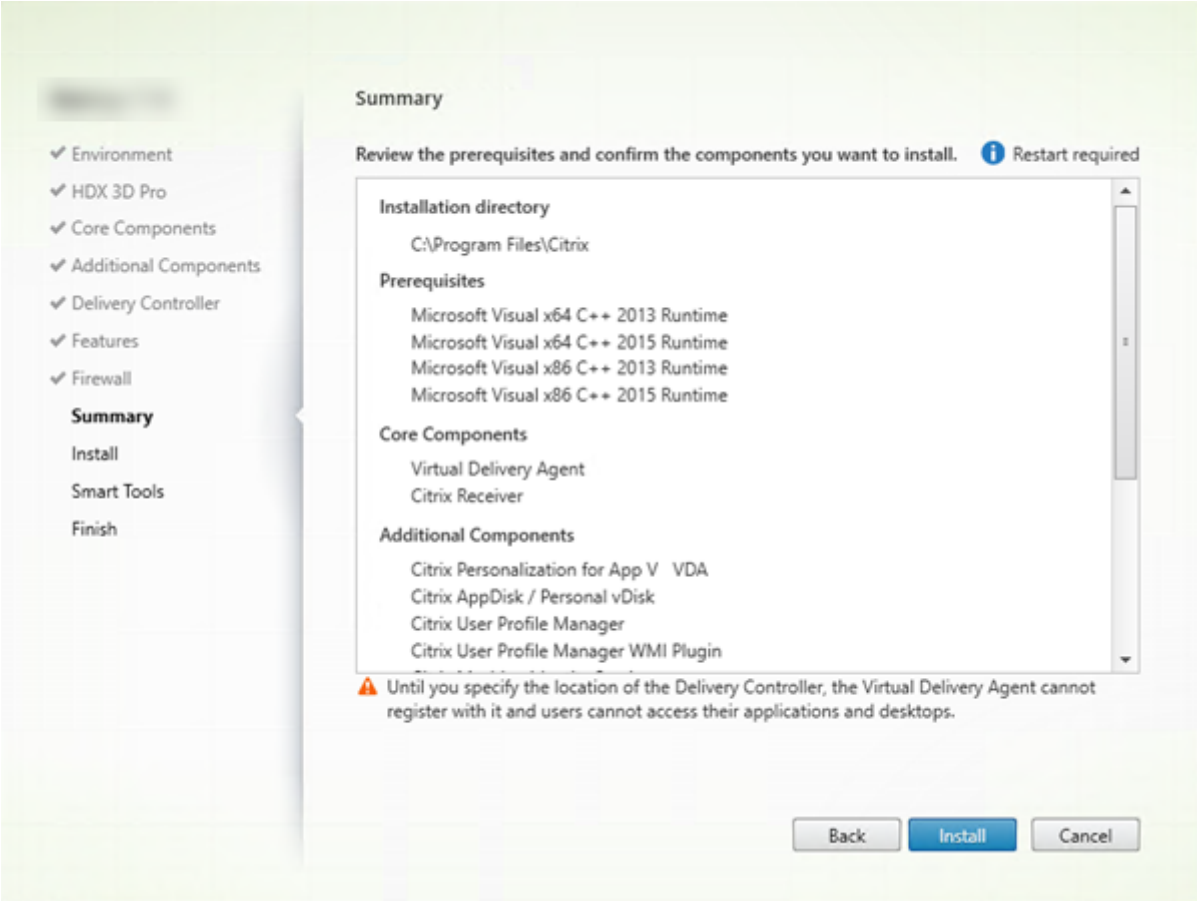


Standardmäßig sind auf der Seite **Firewall** die folgenden Ports geöffnet, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Die Standardeinstellung ist für die meisten Bereitstellungen geeignet. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

Klicken Sie auf **Weiter**.

Befehlszeilenoption: /enable_hdx_ports

Schritt 11. Überprüfen der Voraussetzungen und Bestätigen der Installation

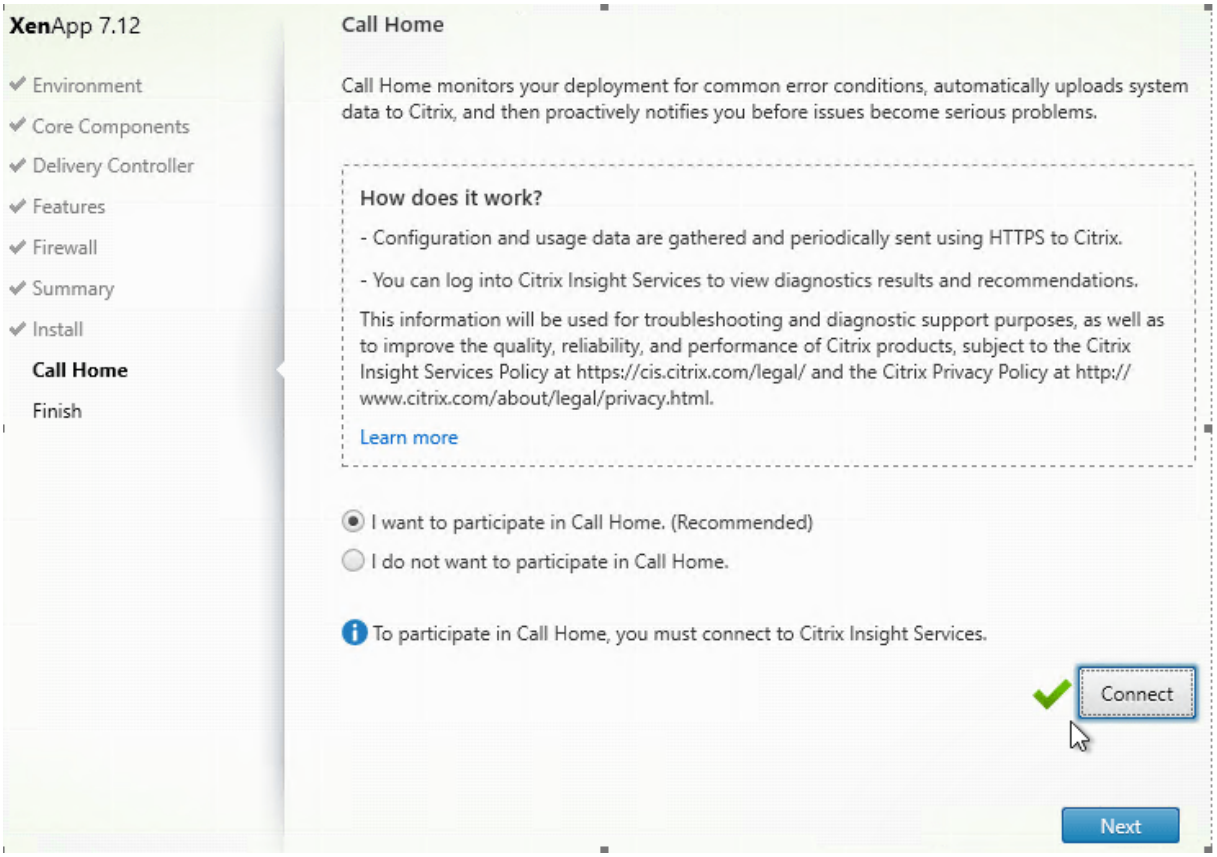


Auf der Seite **Zusammenfassung** wird aufgelistet, was installiert wird. Sie können mit der Schaltfläche Zurück zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern.

Wenn Sie fertig sind, klicken Sie auf **Installieren**.

Wenn erforderliche Software nicht bereits installiert/aktiviert ist wird die Maschine evtl. ein- oder zweimal neu gestartet. Siehe Vorbereiten der Installation.

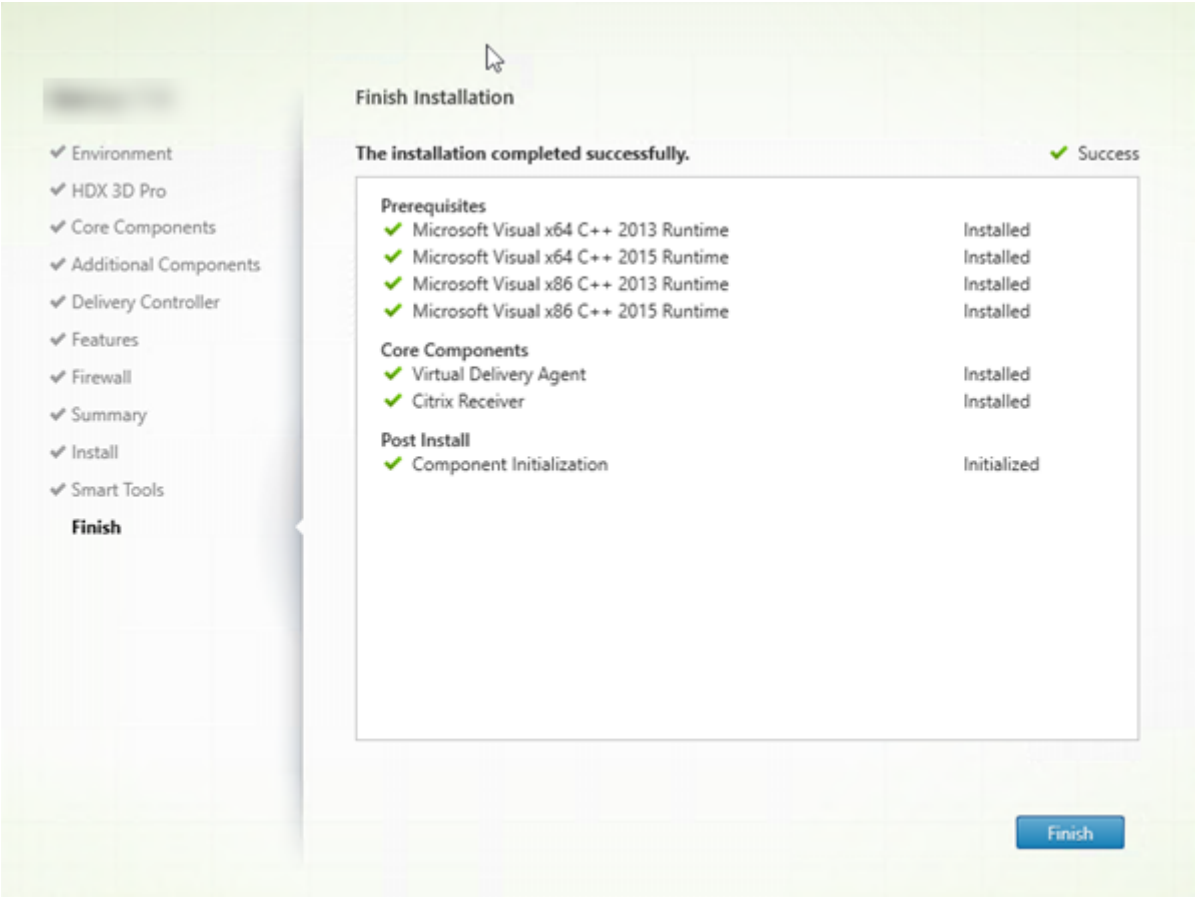
Schritt 12. Teilnahme an Call Home



Geben Sie auf der Seite **Call Home** an, ob Sie bei Call Home teilnehmen möchten. Wenn Sie teilnehmen möchten (Standardeinstellung), klicken Sie auf **Verbinden**. Geben Sie nach Aufforderung die Anmeldeinformationen Ihres Citrix-Kontos ein.

Wenn Ihre Anmeldeinformationen überprüft sind (bzw. wenn Sie nicht teilnehmen), klicken Sie auf **Weiter**.

Schritt 13: Abschließen der Installation



Die Seite **Fertigstellen** zeigt grüne Häkchen für alle Voraussetzungen und Komponenten, die erfolgreich installiert und initialisiert werden konnten.

Klicken Sie auf **Fertig stellen**. Standardmäßig wird die Maschine automatisch neu gestartet. (Sie können den Neustart zwar deaktivieren, doch kann der VDA dann solange nicht verwendet werden, bis ein Neustart erfolgt.)

Installieren weiterer VDAs und Fortsetzen der Konfiguration

Wiederholen Sie die Schritte oben zum Installieren weiterer VDAs auf anderen Maschinen oder Images nach Bedarf.

Wenn alle VDAs installiert sind, starten Sie Studio. Wenn Sie noch keine Site erstellt haben, werden Sie von Studio automatisch zu dieser Aufgabe geleitet. Wenn Sie damit fertig sind, werden Sie von Studio zur Erstellung eines Maschinenkatalogs und anschließend zur Erstellung einer Bereitstellungsgruppe geleitet. Siehe:

- Erstellen einer Site

- Maschinenkataloge erstellen
- Erstellen von Bereitstellungsgruppen

Später können Sie einen installierten VDA auf folgende Weise anpassen:

1. Klicken Sie in Windows im Dialogfeld zum Hinzufügen oder Entfernen von Programmen mit der rechten Maustaste auf **Citrix Virtual Delivery Agent** oder **Citrix Remote PC Access/VDI Core Services VDA**. Klicken Sie auf mit der rechten Maustaste und wählen Sie **Ändern**.
2. Wählen Sie **Virtual Delivery Agent-Einstellungen anpassen**. Wenn das Installationsprogramm gestartet wird, können Sie Folgendes ändern:

- Controlleradressen
- TCP/IP-Port für die Registrierung beim Controller (Standard = 80)
- Automatisches Öffnen der Windows-Firewallports

Problembehandlung

Wenn in der Bereitstellung Microsoft System Center Configuration Manager verwendet wird, schlägt eine VDA-Installation u. U. scheinbar mit Exitcode 3 fehl, obwohl der VDA erfolgreich installiert wird. Sie können diese irreführende Meldung vermeiden, indem Sie die Installation mit einem CMD-Script umschließen oder die Erfolgscodes im Configuration Manager-Paket ändern. Weitere Informationen finden Sie in der Forumsdiskussion auf https://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

In Studio wird im Bereich "Details"für Bereitstellungsgruppen unter Installierte VDA-Version möglicherweise nicht die auf den Maschinen installierte Version angezeigt. In der Maschine wird in Windows unter "Programme und Features"die tatsächliche VDA-Version angezeigt.

Installieren über die Befehlszeile

November 15, 2022

Dieser Artikel gilt für die Installation von Komponenten auf Maschinen mit Windows-Betriebssystem. Informationen zu VDAs für Linux finden Sie in der Dokumentation zum Linux Virtual Delivery Agent.

> **Wichtig:**
>
> In diesem Abschnitt wird die Verwendung von Produktinstallationsbefehlen beschrieben. Lesen Sie vor Beginn jeglicher Installation die Informationen unter Vorbereiten der Installation. Dieser Artikel enthält Beschreibungen der Installationsprogramme.

Sie müssen der Originaladministrator sein oder verwenden Sie **Als Administrator ausführen**, um den Fortschritt der Befehlsausführung und die Rückgabewerte anzuzeigen. Weitere Informationen finden Sie in der Microsoft-Befehlsdokumentation.

Als Ergänzung zu den Installationsbefehlen enthält das Produkt-ISO-Image Beispielskripts zum Installieren, Aktualisieren und Entfernen von VDA-Maschinen in bzw. aus Active Directory. Weitere Informationen finden Sie unter Installieren von VDAs mit Skripts.

Verwenden des Produktinstallationsprogramms

Zugreifen auf die Befehlszeilenschnittstelle des Komplettinstallationsprogramms

1. Laden Sie das Produktpaket von Citrix herunter. Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen.
2. Entpacken Sie die Datei. Optional können Sie die ISO-Datei auch auf DVD brennen.
3. Melden Sie sich mit einem lokalen Administratorkonto am Server an, auf dem Sie die Komponenten installieren.
4. Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit.
5. Führen Sie im Verzeichnis `\x64\XenDesktop Setup` auf dem Medium den entsprechenden Befehl aus.

Installieren von Kernkomponenten

Führen Sie den Befehl `XenDesktopServerSetup.exe` mit den unter Befehlszeilenoptionen zur Installation der Kernkomponenten beschriebenen Optionen aus.

Installieren eines VDAs

Führen Sie den Befehl `XenDesktopVDASetup.exe` mit den unter Befehlszeilenoptionen zur VDA-Installation beschriebenen Optionen aus.

Installieren des universellen Druckservers

Folgen Sie den Anweisungen unter Installieren des universellen Druckservers an der Befehlszeile.

Installieren des Verbundauthentifizierungsdiensts

Citrix empfiehlt die Verwendung der grafischen Oberfläche.

Installieren der Self-Service-Kennwortzurücksetzung

Folgen Sie den Anweisungen in der Dokumentation zum Self-Service-Kennwortzurücksetzungsdienst.

Verwenden eines dedizierten VDA-Installationsprogramms

Zum Zugriff auf die Downloadsite benötigen Sie Citrix Kontoanmeldeinformationen. Für die Installation benötigen Sie erhöhte Administratorprivilegien oder verwenden Sie die Option **Als Administrator ausführen**.

- Laden Sie das benötigte Paket von Citrix herunter.

Name der Komponenten auf der Downloadseite	Name der Installationsdatei
Server OS Virtual Delivery Agent <*Version*>	VDAServerSetup.exe
Desktop OS Virtual Delivery Agent <*Version*>	VDAWorkstationSetup.exe
Desktop OS Core Services Virtual Delivery Agent <*Version*>	VDAWorkstationCoreSetup.exe

- Extrahieren Sie entweder zunächst die Dateien aus dem Paket in ein vorhandenes Verzeichnis und führen Sie dann den Installationsbefehl aus oder führen Sie das Paket direkt aus.

Verwenden Sie zum Extrahieren der Dateien vor der Installation `/extract` mit dem absoluten Pfad, z. B.: `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia` (Das Verzeichnis muss vorhanden sein. Andernfalls schlägt die Extraktion fehl.) Führen Sie dann mit einem separaten Befehl `XenDesktopVdaSetup.exe` in dem Verzeichnis mit dem extrahierten Inhalt aus (im Beispiel oben wäre dies `CitrixVDAInstallMedia`). Verwenden Sie die unter Befehlszeilenoptionen zur VDA-Installation aufgeführten, zulässigen Optionen.

Um das heruntergeladene Paket auszuführen, führen Sie den Namen aus: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` oder `VDAWorkstationCoreSetup.exe`. Verwenden Sie die unter Befehlszeilenoptionen zur VDA-Installation aufgeführten, zulässigen Optionen.

Hinweis für Personen, die mit dem Produktinstallationsprogramm vertraut sind:

- Führen Sie den eigenständigen Installer `VDAServerSetup.exe` aus oder `VDAWorkstationSetup.exe`. Die Verwendung des Befehls ist mit der von `XenDesktopVdaSetup.exe` identisch.
- Das Installationsprogramm `VDAWorkstationCoreSetup.exe` ist anders, da es nur einen Teil der Optionen der anderen Installationsprogramme unterstützt.

Befehlszeilenoptionen zur Installation der Kernkomponenten

Die folgenden Optionen sind bei Installation der Kernkomponenten mit dem Befehl `XenDesktopServerSetup.exe` zulässig. Weitere Informationen zu den Optionen finden Sie unter Installieren der Kernkomponenten.

/components <*component*> [,<*component*>] ...

Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte:

`CONTROLLER`: Controller

`DESKTOPSTUDIO`: Studio

`DESKTOPDIRECTOR`: Director

`LICENSESERVER`: Citrix Lizenzserver

Wenn diese Option ausgelassen wird, werden alle Komponenten installiert (bzw. entfernt, wenn die Option `/remove` ebenfalls angegeben ist).

(In Versionen vor 7.15 LTSR CU6 war StoreFront als Wert gültig. Verwenden Sie ab Version 7.15 LTSR CU6 den dedizierten, unter Installieren von StoreFront aufgeführten StoreFront-Installationsbefehl).

/configure_firewall

Öffnet alle Ports in der Windows-Firewall, die von den installierten Komponenten verwendet werden, wenn der Windows-Firewalldienst ausgeführt wird, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie die Firewall eines Drittanbieters verwenden oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden.

/disableexperiencemetrics

Verhindert das automatische Senden der bei Installation, Upgrade oder Deinstallation erfassten Analysedaten an Citrix.

/exclude

Verhindert die Installation der in geraden Anführungszeichen angegebenen (durch Kommas getrennten) Features, Dienste oder Technologien. Gültige Werte:

`Local Host Cache Storage (LocalDB)`: Verhindert die Installation der für den lokalen Hostcache verwendeten Datenbank. Diese Option hat keine Auswirkungen darauf, ob SQL Server Express zur Verwendung als Sitedatenbank installiert wird.

`Smart Tools Agent`: verhindert die Installation des Citrix Smart Tools Agent.

> **Hinweis:**
>
> Ab CU4 ist Smart Tools nicht mehr im Installationsprogramm enthalten. Smart Tools-Instanzen aus früheren Installationen bleiben ohne Veränderung.

/help oder /h

Zeigt die Hilfe für Befehle an.

/installdir <*directory*>

Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standardeinstellung = `c:\Program Files\Citrix`.

/logpath <*path*>

Speicherort der Protokolldateien. Der angegebene Ordner muss vorhanden sein. Er wird von dem Installationsprogramm nicht erstellt. Standard = `"%TEMP%\Citrix\XenDesktop Installer"`

/ no_remote_assistance

Gilt nur bei der Installation von Director. Deaktiviert das Feature zur Benutzerspiegelung, welches Microsoft-Remoteunterstützung verwendet.

/noreboot

Verhindert einen Neustart nach der Installation. (Bei den meisten Kernkomponenten ist ein Neustart in der Standardeinstellung nicht aktiviert).

/nosql

Verhindert die Installation von Microsoft SQL Server Express auf dem Server, auf dem Sie den Controller installieren. Wenn diese Option ausgelassen wird, wird SQL Server Express zur Verwendung

als Sitedatenbank installiert. Diese Option hat keine Auswirkungen auf die Installation von SQL Server Express LocalDB für den lokalen Hostcache.

/quiet oder /passive

Während der Installation wird keine Benutzeroberfläche angezeigt. Der einzige Hinweis auf den Installationsvorgang ist im Windows Task-Manager. Wenn diese Option ausgelassen wird, wird die grafische Oberfläche gestartet.

/remove

Entfernt die mit `/components` angegebenen Kernkomponenten.

/removeall

Entfernt alle installierten Kernkomponenten.

/sendexperiencemetrics

Sendet automatisch bei Installation, Upgrade oder Deinstallation erfasste Analysedaten an Citrix. Wenn diese Option ausgelassen wird (oder `/disableexperiencemetrics` angegeben wird), werden Analysedaten lokal erfasst, aber nicht automatisch gesendet.

/tempdir <*directory*>

Das Verzeichnis, das die temporären Dateien während der Installation enthält. Standard = C:\Windows\Temp.

/xenapp

Installiert XenApp. Wenn diese Option ausgelassen wird, wird XenDesktop installiert.

Beispiele: Installieren der Kernkomponenten

Mit dem folgenden Befehl werden ein XenDesktop-Controller, Studio, die Citrix Lizenzierung und SQL Server Express auf einem Server installiert. Für die Komponentenkommunikation erforderliche Firewallports werden automatisch geöffnet.


```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller
,desktopstudio,licenseserver /configure_firewall
```

Mit dem folgenden Befehl werden ein XenApp-Controller, Studio und SQL Server Express auf dem Server installiert. Für die Komponentenkommunikation erforderliche Firewallports werden automatisch geöffnet.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

Befehlszeilenoptionen zur VDA-Installation

Die folgenden Optionen sind für einen oder mehrere der folgenden Befehle gültig: `XenDesktopVDASetup.exe`, `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` oder `VDAWorkstationCoreSetup.exe`.

/baseimage

Nur bei Installation von VDAs für Desktopbetriebssysteme auf einer VM zulässig. Ermöglicht die Verwendung von persönlichen vDisks mit einem Masterimage. Einzelheiten finden Sie unter Personal vDisk.

Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden.

/components <*component*>[,<*component*>]

Durch Trennzeichen getrennte Liste der zu installierenden oder zu entfernenden Komponenten. Gültige Werte:

`VDA`: Virtual Delivery Agent

`PLUGINS`: Citrix Receiver für Windows (`CitrixReceiver.exe`)

Beispiel: Um den VDAs ohne Citrix Receiver zu installieren, geben Sie `/components vda` an.

Wenn diese Option ausgelassen wird, werden alle Komponenten installiert.

Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden. Mit dem Installationsprogramm kann Citrix Receiver nicht installiert werden.

/controllers "*<controller>* [*<controller>*] [...]"

Durch Leerzeichen getrennte FQDNs der Controller, mit denen VDA kommunizieren kann; von geraden Anführungszeichen umschlossen. Geben Sie nicht sowohl die Option `/site_guid` als auch die Option `/controllers` an.

/disableexperiencemetrics

Verhindert das automatische Senden der bei Installation, Upgrade oder Deinstallation erfassten Analysedaten an Citrix.

/enable_framehawk_port

Öffnet die von Framehawk verwendeten UDP-Ports. Standard = false

/enable_hdx_3d_pro

Installiert den VDA im HDX 3D Pro-Modus.

/enable_hdx_ports

Öffnet die erforderlichen Ports in der Windows-Firewall für den VDA und aktivierte Features (mit Ausnahme von Windows-Remoteunterstützung), wenn die Windows-Firewall erkannt wird (selbst wenn sie nicht aktiviert ist). Wenn Sie eine andere oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

Um UDP-Ports zu öffnen, die der adaptive HDX-Transport verwendet, geben Sie zusätzlich zu `/enable_hdx_udp_ports` die Option `/enable_hdx_ports` an.

/enable_hdx_udp_ports

Öffnet die für den adaptiven HDX-Transport erforderlichen UDP-Ports in der Windows-Firewall, wenn der Windows-Firewalldienst erkannt wird, selbst wenn die Firewall nicht aktiviert ist. Wenn Sie eine andere oder keine Firewall verwenden, müssen die Ports manuell geöffnet werden. Weitere Informationen zu Ports finden Sie unter Netzwerkports.

Um andere Ports zu öffnen, die der VDA verwendet, geben Sie die Option `/enable_hdx_ports` und die Option `/enable_hdx_udp_ports` an.

/enable_real_time_transport

Aktiviert oder deaktiviert die Verwendung von UDP für Audiopakete (Real-Time Audio Transport für Audio). Das Aktivieren dieses Features kann die Audioleistung verbessern. Verwenden Sie die Option /enable_hdx_ports, wenn Sie möchten, dass die UDP-Ports automatisch bei Erkennung des Windows-Firewalldiensts geöffnet werden.

/enable_remote_assistance

Aktiviert das Spiegelungsfeature in der Microsoft-Remoteunterstützung für die Verwendung mit Director. Wenn Sie diese Option angeben, öffnet die Windows-Remoteunterstützung die dynamischen Ports in der Firewall.

/exclude "*<component>*"["*<component>*"]

Verhindert die Installation der in geraden Anführungszeichen angegebenen (durch Kommas getrennten) optionalen Komponenten. Beispiel: Installieren oder Aktualisieren eines VDAs auf einem Image, das nicht mit MCS verwaltetet werden soll, erfordert keine Personal vDisk- oder Maschinenidentitätsdienstkomponenten. Gültige Werte:

- Personal vDisk
- Machine Identity Service
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Citrix Universal Print Client
- Citrix Telemetry Service
- Citrix Personalization for App-V - VDA

Ausschließen der Citrix User Profilverwaltung aus der Installation (mit der Option /exclude "Citrix User Profile Manager") hat Auswirkungen auf die Überwachung und Problembehandlung von VDAs mit Citrix Director. Auf den Seiten **Benutzerdetails** und **Endpunkt** treten Fehler in den Bereichen **Personalisierung** und **Anmeldedauer** auf. Auf den Seiten **Dashboard** und **Trends** werden im Bereich **Durchschnittliche Anmeldedauer** nur Daten für Maschinen angezeigt, auf denen die Profilverwaltung installiert ist.

Selbst bei Verwendung der Profilverwaltungslösung eines Drittanbieters empfiehlt Citrix, dass Sie die Citrix Profilverwaltung installieren und ausführen. Die Citrix Profilverwaltung muss nicht aktiviert werden.

Diese Option ist ungültig, wenn Sie das Installationsprogramms VDAWorkstationCoreSetup.exe verwenden. Das Installationsprogramm schließt viele dieser Elemente automatisch aus.

/h oder /help

Zeigt die Hilfe für Befehle an.

/hdxflashv2only

Verhindert zur Erhöhung der Sicherheit die Installation der Legacy-Binärdateien der Flash-Umleitung.

Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

/installdir <*directory*>

Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Standardeinstellung = `c:\Program Files\Citrix`.

/logpath <*path*>

Speicherort der Protokolldateien. Der angegebene Ordner muss vorhanden sein. Er wird von dem Installationsprogramm nicht erstellt. Standard = `"%TEMP%\Citrix\XenDesktop Installer"`

Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

/masterimage

Gilt nur für die Installation von VDAs auf einer VM. Richtet VDA als Masterimage ein.

Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden.

/no_mediafoundation_ack

Bestätigt, dass Microsoft Media Foundation nicht installiert ist und mehrere HDX-Multimediafeatures nicht installiert werden und nicht funktionieren. Wenn diese Option ausgelassen wird und Media Foundation nicht installiert ist, schlägt die VDA-Installation fehl. Bei den meisten unterstützten Windows-Editionen ist Media Foundation bereits installiert. Eine Ausnahme bilden die N-Editionen.

/nocitrixwddm

Gilt nur für Windows 7-Maschinen, die keine WDDM-Treiber enthalten. Deaktiviert die Installation des Citrix WDDM-Treibers.

Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

/nodesktopexperience

Gilt nur für die Installation von VDAs für Serverbetriebssysteme. Verhindert das Aktivieren der Enhanced Desktop Experience. Dieses Feature wird auch über die Citrix Richtlinieneinstellung Enhanced Desktop Experience gesteuert.

/noreboot

Verhindert einen Neustart nach der Installation. Der VDA kann erst nach einem Neustart verwendet werden.

/noresume

Wenn während einer Installation ein Maschinenneustart erforderlich ist, wird das Installationsprogramm automatisch fortgesetzt, sobald der Neustart abgeschlossen ist. Um den Standardwert zu überschreiben, geben Sie `/noresume` an. Dies kann hilfreich sein, wenn Sie das Medium neu laden müssen oder während einer automatischen Installation Informationen erfassen möchten.

/optimize

Gilt nur für die Installation von VDAs auf einer VM. Aktiviert die Optimierung für VDAs, die auf einer VM auf einem Hypervisor ausgeführt werden. Die VM-Optimierung umfasst das Deaktivieren von Offlinedateien, das Deaktivieren der Hintergrunddefragmentierung und die Verkleinerung der Ereignisprotokollgröße. Geben Sie diese Option nicht für Remote-PC-Bereitstellungen an. Weitere Informationen finden Sie unter CTX224676.

/portnumber <*port*>

Gilt nur, wenn die Option `/reconfig` angegeben wurde. Portnummer für die Kommunikation zwischen VDA und dem Controller. Der zuvor konfigurierte Port wird deaktiviert, es sei denn, es handelt sich um Port 80.

/quiet oder /passive

Während der Installation wird keine Benutzeroberfläche angezeigt. Der einzige Hinweis auf den Installations- und Konfigurationsvorgang ist im Windows Task-Manager. Wenn diese Option ausgelassen wird, wird die grafische Oberfläche gestartet.

/reconfigure

Passt die zuvor konfigurierten VDA-Einstellungen an, wenn der Befehl mit den Optionen `/portnumber`, `/controllers` oder `/enable_hdx_ports` verwendet wird. Wenn Sie diese Option ohne die Option `/quiet` angeben, wird die grafische Oberfläche zum Anpassen von VDA gestartet.

/remotepc

Gilt nur für Remote-PC-Zugriff-Bereitstellungen. Verhindert die Installation der folgenden Komponenten unter einem Desktopbetriebssystem:

- Citrix Personalisierung für App-V
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plug-In
- Maschinenidentitätsdienst
- Personal vDisk

Diese Option ist ungültig, wenn Sie das Installationsprogramms `VDAWorkstationCoreSetup.exe` verwenden. Das Installationsprogramm schließt diese Komponenten automatisch aus.

/remove

Entfernt die mit `/components` angegebenen Komponenten.

/removeall

Entfernt alle installierten VDA-Komponenten.

/sendexperiencemetrics

Sendet automatisch bei Installation, Upgrade oder Deinstallation erfasste Analysedaten an Citrix. Wenn diese Option ausgelassen wird (oder die Option `/disableexperiencemetrics` angegeben wird), werden Analysedaten lokal erfasst, aber nicht automatisch gesendet.

/servervdi

Installiert einen VDA für Desktopbetriebssysteme auf einem unterstützten Windows-Server. Lassen Sie diese Option aus, wenn Sie einen VDA für Serverbetriebssysteme auf einem Windows-Server installieren. Lesen Sie vor dem Verwenden dieser Option Server-VDI.

Verwenden Sie diese Option nur mit dem VDA-Installationsprogramm für das vollständige Produkt. Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

/site_guid <*guid*>

GUID (Globally Unique Identifier) der Website Active Directory Organisationseinheit (OU). Dabei wird ein virtueller Desktop einer Site zugeordnet, wenn Active Directory für die Discovery verwendet wird (das Feature für automatische Updates ist die empfohlene und Discovery-Standardmethode). Die Site-GUID ist eine Site-Eigenschaft, die in Studio angezeigt wird. Geben Sie nicht sowohl die Option `/site_guid` als auch die Option `/controllers` an.

/tempdir <*directory*>

Das Verzeichnis für die temporären Dateien während der Installation. Standardeinstellung = `c:\Windows\Temp`.

Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

/virtualmachine

Gilt nur für die Installation von VDAs auf einer VM. Überschreibt das Erkennen einer physischen Maschine durch den Installer. Dabei werden BIOS-Informationen an die VMs weitergegeben, sodass sie als physische Maschinen erscheinen.

Diese Option ist bei der grafischen Oberfläche nicht verfügbar.

Beispiele: Installieren eines VDAs

Installieren eines VDAs mit dem Komplettinstallationsprogramm

Mit dem folgenden Befehl wird ein VDA für Desktopbetriebssysteme und Citrix Receiver am Standardspeicherort auf einer VM installiert. VDA wird als Masterimage verwendet. Der VDA registriert sich anfänglich am Controller auf dem “Contr-Main”genannten Server in der Domäne “mydomain”und verwendet Personal vDisks, das Optimierungsfeature und die Windows-Remoteunterstützung.


```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,
plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /
optimize /masterimage /baseimage /enable_remote_assistance
```

Installation eines Desktopbetriebssystem-VDAs mit dem eigenständigen Installationsprogramm VDAWorkstationCoreSetup

Mit dem folgenden Befehl wird ein Kernkomponenten-VDA unter einem Desktopbetriebssystem zur Verwendung in einer Remote-PC-Zugriff- oder VDI-Bereitstellung installiert. Citrix Receiver und andere, nicht zu den Kernkomponenten gehörenden Dienste werden nicht installiert. Die Adresse eines Controllers wird automatisch angegeben und die Ports der Windows-Firewall werden automatisch geöffnet. Der Administrator steuert die Neustarts.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

Anpassen eines VDAs über die Befehlszeile

Nachdem VDA installiert wurde, können Sie einige Einstellungen anpassen. Führen Sie auf dem Produktmedium im `\x64\XenDesktop Setup`-Verzeichnis den Befehl `XenDesktopVdaSetup .exe` aus und legen Sie dabei eine oder mehrere der folgenden, unter Befehlszeilenoptionen zur VDA-Installation beschriebenen Optionen fest:

- `/reconfigure` (zum Anpassen des VDAs erforderlich)
- `/h` oder `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber` Port
- `/enable_hdx_ports`

Installieren des universellen Druckservers über die Befehlszeile

Führen Sie einen der folgenden Befehle auf jedem Druckserver aus:

- Auf einem unterstützten 32-Bit-Betriebssystem: Führen im Verzeichnis `\x86\Universal Print Server\` auf dem Citrix Installationsmedium `UpsServer_x86.msi` aus.
- Auf einem unterstützten 64-Bit-Betriebssystem: Führen im Verzeichnis `\x64\Universal Print Server\` auf dem Citrix Installationsmedium `UpsServer_x64.msi` aus.

Nach der Installation des universellen Druckservers auf den Druckservern konfigurieren Sie diesen anhand der Anweisungen unter Bereitstellen von Druckern.

Installieren von VDAs mit Skripts

August 18, 2021

Dieser Artikel gilt für die Installation von VDAs auf Maschinen mit Windows-Betriebssystem. Informationen zu VDAs für Linux finden Sie in der Dokumentation zum Linux Virtual Delivery Agent.

Das Installationsmedium enthält Beispielskripts, um Virtual Delivery Agents (VDAs) für Maschinen in Active Directory zu installieren, zu aktualisieren oder zu entfernen. Sie können die Skripts auch auf einzelne Maschinen anwenden und sie zum Verwalten von Masterimages einsetzen, die von den Maschinenerstellungsdiensten und Provisioning Services verwendet werden.

Erforderliche Zugriffsberechtigungen:

- Für die Skripts ist Lesezugriff für "Jeder"auf der Netzwerkfreigabe erforderlich, auf der der VDA-Installationsbefehl ist. Der Installationsbefehl lautet beim vollständigen Produkt-ISO-Image "XenDesktopVdaSetup.exe"und beim eigenständigen Installationsprogramm "VDAWorkstationSetup.exe"bzw. "VDAServerSetup.exe".
- Die Protokolldetails werden auf jeder lokalen Maschine gespeichert. Sollen die Ergebnisse zentral zur Überprüfung und Analyse protokolliert werden, benötigen die Skripts Lese- und Schreibzugriff auf der Netzwerkfreigabe für "Jeder".

Um die Ergebnisse der Skriptausführung zu überprüfen, müssen Sie die zentrale Protokollfreigabe untersuchen. Erfasst werden das Skriptprotokoll, das Installationsprogrammprotokoll und die MSI-Installationsprotokolle. Jeder Installations- oder Deinstallationsvorgang wird in einem Ordner mit Zeitstempel aufgezeichnet. Am Präfix "PASS"oder "FAIL"im Ordnertitel ist das Ergebnis der Vorgangs ersichtlich. Sie können herkömmliche Verzeichnissuchprogramme verwenden, um eine fehlerhafte Installation oder Deinstallation im zentralen Protokoll zu finden. Diese Tools bieten eine Alternative zur lokalen Suche auf den Zielmaschinen.

> **Wichtig:**
>
> Vor Beginn einer Installation führen Sie die unter Vorbereiten der Installation beschriebenen Schritte durch.

Installieren oder Aktualisieren von VDAs mit dem Skript

1. Suchen Sie das Beispielskript InstallVDA.bat im Ordner \Support\AdDeploy\ auf dem Installationsmedium. Citrix empfiehlt, dass Sie ein Backup der ursprünglichen Skriptdatei anlegen,

bevor Sie sie ändern.

2. Bearbeiten Sie das Skript:

   - Geben Sie die Version des zu installierenden VDA an: SET DESIREDVERSION. Beispielsweise kann Version 7 als 7.0 angegeben werden. Der vollständige Wert findet sich auf dem Installationsmedium in der Datei ProductVersion.txt (z. B. 7.0.0.3018). Eine vollständige Übereinstimmung ist jedoch nicht erforderlich.
   - Geben Sie die Netzwerkfreigabe an, wo das Installationsprogramm aufgerufen wird. Verweisen Sie auf den Stamm (den höchsten Punkt) der Struktur. Die geeignete Version des Installationsprogramms (32 Bit oder 64 Bit) wird automatisch aufgerufen, wenn das Skript ausgeführt wird. Beispiel: SET DEPLOYSHARE=\\fileserver1\share1.
   - Geben Sie optional einen Netzwerkfreigabeort zum Speichern der zentralen Protokolle an. Beispiel: SET LOGSHARE=\\fileserver1\log1.
   - Geben Sie die VDA-Konfigurationsoptionen an. Weitere Informationen finden Sie unter Installieren über die Befehlszeile. Die Optionen /quiet und /noreboot sind standardmäßig im Skript enthalten und sind erforderlich: SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT.

3. Weisen Sie mit den Startskripts für Gruppenrichtlinien das Skript der Organisationseinheit zu, die die Maschinen enthält. Diese Organisationseinheit sollte nur Maschinen enthalten, auf denen Sie VDA installieren möchten. Wenn die Maschinen in dieser Organisationseinheit neu gestartet werden, wird das Skript auf allen ausgeführt. Ein VDA wird auf jeder Maschine installiert, deren Betriebssystem unterstützt wird.

Entfernen von VDAs mit dem Skript

1. Besorgen Sie sich das Beispielskript UninstallVDA.bat aus \Support\AdDeploy\ auf dem Installationsmedium. Citrix empfiehlt, dass Sie ein Backup der ursprünglichen Skriptdatei anlegen, bevor Sie sie ändern.
2. Bearbeiten Sie das Skript.

   - Geben Sie die Version des zu entfernenden VDA an: SET CHECK_VDA_VERSION. Beispielsweise kann Version 7 als 7.0 angegeben werden. Der vollständige Wert findet sich auf dem Installationsmedium in der Datei ProductVersion.txt (z. B. 7.0.0.3018). Eine vollständige Übereinstimmung ist jedoch nicht erforderlich.
   - Geben Sie optional einen Netzwerkfreigabeort zum Speichern der zentralen Protokolle an.

3. Weisen Sie mit den Startskripts für Gruppenrichtlinien das Skript der Organisationseinheit zu, die die Maschinen enthält. Diese Organisationseinheit sollte nur Maschinen enthalten, von denen Sie VDA entfernen möchten. Wenn die Maschinen in dieser Organisationseinheit neu gestartet werden, wird das Skript auf allen ausgeführt. Der VDA wird von jeder Maschine entfernt.

Problembehandlung

Das Skript generiert interne Protokolldateien, die den Skriptausführungsverlauf beschreiben. Das Skript kopiert das Protokoll Kickoff_VDA_Startup_Skript innerhalb von Sekunden nachdem die Bereitstellung auf der Maschine gestartet wurde in die zentrale Protokollfreigabe. Sie können überprüfen, ob der Prozess funktioniert. Wird dieses Protokoll nicht in die zentrale Protokollfreigabe kopiert, untersuchen Sie zur Problembehandlung die lokale Maschine. Das Skript platziert zwei Debugprotokolldateien im Ordner% temp% auf jeder Maschine:

- Kickoff_VDA_Startup_Script_<DateTimeStamp>.log
- VDA_Install_ProcessLog_<DateTimeStamp>.log

Überprüfen Sie diese Protokolle, um Folgendes für das Skript sicherzustellen:

- Es wird wie erwartet ausgeführt.
- Das Zielbetriebssystem wird korrekt erkannt.
- Der Verweis auf ROOT von DEPLOYSHARE ist korrekt konfiguriert (enthält die Datei "AutoSelect.exe").
- Die Authentifizierung bei den Freigaben DEPLOYSHARE und LOG ist möglich.

Installieren von VDAs mit SCCM

December 5, 2023

Übersicht

Die VDA-Installation verläuft in zwei Phasen:

- Installieren der Voraussetzungen
- Installieren des VDAs

Zum erfolgreichen Bereitstellen des VDAs mit Microsoft SCCM (System Center Configuration Manager) oder einem ähnlichen Softwareverteilungstool empfiehlt Citrix, diese Phasen separat auszuführen. Installieren Sie also erst die Voraussetzungen mit ihrem Installationsprogramm und dann den VDA mit einem VDA-Installationsprogramm, anstatt Voraussetzungen und VDA gemeinsam mit dem VDA-Installationsprogramm zu installieren.

Identifizieren von Anforderungen und Definieren der Tasksequenz

Vor der VDA-Installation müssen zunächst die Voraussetzungen auf der Maschine installiert werden. Welche Voraussetzungen erforderlich sind, kann je nach VDA-Version variieren. Weitere Informationen finden Sie in den Systemanforderungen für die zu installierende VDA-Version:

- Aktuelles Release von Citrix Virtual Apps and Desktops
- Citrix Virtual Apps and Desktops 1912 LTSR
- XenApp und XenDesktop 7.15 LTSR

Ob diese Voraussetzungen installiert werden müssen, kann ebenfalls zwischen Umgebungen variieren, je nachdem, was bereits auf den Zielmaschinen vorhanden ist und welches Betriebssystem genutzt wird. Bevor Sie Skripts oder Tasksequenzen erstellen, müssen Sie die spezifischen Anforderungen Ihrer Umgebung verstehen (z. B., welche Voraussetzungen installiert werden müssen). Anschließend können Sie die Tasksequenz korrekt definieren.

Tipp: Eine gute Möglichkeit zum Sammeln dieser Informationen ist die manuelle Installation des VDAs auf einer Maschine in der Umgebung. Dabei sehen Sie, welche Voraussetzungen bei der VDA-Installation erforderlich sind und installiert sein müssen.

Die Installationsdateien für die VDA-Voraussetzungen sind im Installationsmedium für Citrix Virtual Apps and Desktops (oder XenApp und XenDesktop) im Ordner **Support** enthalten. Verwenden Sie diese Dateien, um sicherzustellen, dass Sie die richtige Version der Voraussetzungen installieren.

Neustarts

Wie viele Neustarts während der Installation der Voraussetzungen und des VDA erforderlich sind, hängt von der Umgebung ab. Beispielsweise kann ein Neustart für ausstehende Updates oder es können Neustarts von früheren Softwareinstallationen erforderlich sein. Außerdem müssen Dateien, die zuvor von anderen Prozessen gesperrt wurden, möglicherweise aktualisiert werden.

- Prüfen Sie bei der manuellen Installation, welche Voraussetzungen einen Neustart auslösen.
- Optionale Komponenten im VDA-Installationsprogramm (z. B. Citrix User Profile Manager, Citrix Files) können einen Neustart erfordern. Prüfen Sie bei der manuellen Installation, welche Komponenten einen Neustart auslösen.

Definieren der Tasksequenz

Nachdem Sie alle Voraussetzungen und Neustarts erfasst haben, führen Sie folgende Schritte mit dem SCCM Task Sequencer aus:

1. Erstellen Sie separate SCCM-Aufträge für die Installation jeder Voraussetzung. Dadurch können Probleme oder Fehler, die bei der Bereitstellung auftreten, leichter isoliert werden. Dies erleichtert die Problembehandlung.
2. Erstellen Sie den VDA-Installationsauftrag. Führen Sie diesen Auftrag erst aus, nachdem alle Voraussetzungen erfolgreich installiert sind. Hierfür gibt es zwei Möglichkeiten:
    - Prüfen Sie mit dem SCCM-Client, ob die GUIDs der Voraussetzungen vorhanden sind.
    - Machen Sie den VDA-Installationsauftrag abhängig von den Aufträgen der Voraussetzungen.

Beispiel einer SCCM-Installationssequenz

Dies ist ein Beispiel für eine SCCM-Installationssequenz. Denken Sie daran: Ihre Voraussetzungsversionen können sich je nach zu installierender VDA-Version unterscheiden.

1. SCCM JOB1: Microsoft .NET Framework 4.8
2. SCCM JOB2: Microsoft Visual C++ 2017 Runtime (32-Bit and 64-Bit)
3. SCCM JOB3: VDA-Installation
    a) Verwenden Sie den jeweils erforderlichen VDA-Installationsbefehl. Fügen Sie die Optionen `/quiet`, `/noreboot` und `/noresume` hinzu. (Durch die Option `/noresume` kann die Installation fortgesetzt werden, ohne erst auf die interaktive Anmeldung zu warten. So kann SCCM den Installationsvorgang steuern.)
    b) Achten Sie auf Rückgabecodes.
        - `0`: Erfolg, Installation abgeschlossen, Neustart erforderlich.
        - `3`: Erfolg, Installation nicht abgeschlossen, Neustart erforderlich.
        - `8`: Erfolg, Installation abgeschlossen, Neustart erforderlich.
    c) Starten Sie die Maschine neu.
    d) Bei Rückgabecode 3 wiederholen Sie Schritt 3a.

Weitere Informationen zu Rückgabecodes finden Sie unter Citrix-Installationsrückgabecodes.

Beispiele für VDA-Installationsbefehle

Die verfügbaren Installationsoptionen variieren je nach verwendetem Installationsprogramm. Weitere Informationen zu Befehlszeilenoptionen finden Sie in den folgenden Artikeln. (Bereitgestellte Links führen zum aktuellen Release von Citrix Virtual Apps and Desktops. Wenn Sie eine LTSR-Produktversion verwenden, lesen Sie die entsprechenden LTSR-Artikel.)

- Installieren von VDAs
- Installieren über die Befehlszeile

Installationsbefehle für Remote-PC-Zugriff

- Der folgende Befehl verwendet das Kernkomponenten-VDA-Installationsprogramm für Einzelsitzungs-OS (eigenständiger Installer `VDAWorkstationCoreSetup.exe`):

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.
  com" /enable_hdx_ports /noresume /noreboot
  ```

- Der folgende Befehl verwendet das vollständige VDA-Installationsprogramm für Einzelsitzungs-OS (eigenständiger Installer `VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /controllers "control.
  domain.com" /enable_hdx_ports /noresume /noreboot
  ```

Installationsbefehl für dedizierte VDI

- Der folgende Befehl verwendet das vollständige VDA-Installationsprogramm für Einzelsitzungs-OS (eigenständiger Installer `VDAWorkstationSetup.exe`):

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers "
  control.domain.com" /enable_hdx_ports /optimize /enable_remote_assistance
   /noresume /noreboot
  ```

Erstellen einer Site

August 18, 2021

Eine *Site* ist der Name, den Sie einer XenApp- oder XenDesktop-bereitstellung geben. Sie umfasst die Delivery Controller und andere Kernkomponenten, Virtual Delivery Agents (VDAs), Verbindungen mit Hosts, Maschinenkataloge und Bereitstellungsgruppen. Sie erstellen die Site nach der Installation der Kernkomponenten und bevor Sie den ersten Maschinenkatalog und die erste Bereitstellungsgruppe erstellen.

Beim Erstellen einer Site werden Sie automatisch für das Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) registriert. Im Rahmen des CEIP werden anonyme Statistiken und Nutzungsinformationen gesammelt und an Citrix gesendet. Das erste Datenpaket wird rund sieben Tage nach dem Erstellen der Site an Citrix gesendet. Sie können Ihre Registrierung nach der Siteerstellung jederzeit ändern. Wählen Sie im Studio-Navigationsbereich zunächst **Konfiguration**, anschließend die Registerkarte "Produktsupport"und folgen Sie den Anweisungen. Einzelheiten finden Sie unter https://more.citrix.com/XD-CEIP.

Der Benutzer, der eine Site erstellt, wird zu deren Volladministrator. Weitere Informationen finden Sie unter Delegierte Administration.

Lesen Sie den Artikel, bevor Sie den Assistenten zum Erstellen der Site starten.

Erstellen einer Site

Öffnen Sie Studio, falls es nicht geöffnet ist. Sie werden automatisch zu der Aktion zum Starten des Assistenten für die Siteerstellung geführt. Die Seiten des Assistenten decken folgende Elemente der Konfiguration ab:

Name und Typ der Site

Es stehen zwei Sitetypen zur Auswahl:

- **Site für Anwendungs- und Desktopbereitstellung**. Wenn Sie eine Anwendungs- und Desktopbereitstellungssite erstellen, haben Sie die Wahl zwischen einer vollständigen Bereitstellung (empfohlen) oder einer leeren Site. Leere Sites sind nur teilweise konfiguriert und werden normalerweise von erfahrenen Administratoren erstellt.
- **Remote-PC-Zugriff-Site**. Sites dieses Typs ermöglichen Benutzern den Remotezugriff auf ihre Büro-PCs über eine sichere Verbindung.

Wenn Sie zu diesem Zeitpunkt eine Bereitstellung für die Anwendungs- und Desktopbereitstellung erstellen, können Sie eine Remote-PC-Zugriff-Bereitstellung später hinzufügen. Ebenso können Sie einer Remote-PC-Zugriff-Bereitstellung später eine vollständige Bereitstellung hinzufügen.

Geben Sie einen Namen für die Site ein. Wenn die Site erstellt ist, wird ihr Name oben im Navigationsbereich von Studio angezeigt: **Citrix Studio** (*Sitename*).

Datenbanken

Die Seite **Datenbanken** enthält Optionen zum Einrichten der Site-, der Standort-, der Überwachungs- und der Konfigurationsprotokollierungsdatenbank. Informationen zu Anforderungen für die Datenbanken und zu deren Einrichtung finden Sie unter Datenbanken.

Wenn Sie die SQL Server Express-Software zur Verwendung als Sitedatenbank installieren, wird nach der Installation der Software ein Neustart ausgeführt. Der Neustart wird nicht ausgeführt, wenn Sie die SQL Server Express-Software zur Verwendung als Sitedatenbank nicht installieren.

Wenn Sie nicht die Standardoption SQL Server Express verwenden, stellen Sie sicher, dass die SQL Server-Software auf den Maschinen installiert ist, bevor Sie eine Site erstellen. Unter Systemanforderungen werden die unterstützten Versionen aufgeführt.

Wenn Sie bereits die Controller-Software auf anderen Servern installiert haben und der Site weitere Controller hinzufügen möchten, können Sie dies über diese Seite tun. Wenn Sie Skripts für die Einrichtung der Datenbanken generieren möchten, fügen Sie die Controller vor dem Generieren der Skripts hinzu.

Lizenzierung

Überlegen Sie, ob Sie vorhandene Lizenzen verwenden möchten oder das 30-tägige kostenlose Probeabo, bei dem die Lizenzdateien später hinzugefügt werden können. Sie können Lizenzdateien auch über den Assistenten für die Siteerstellung hinzufügen oder herunterladen. Weitere Informationen finden Sie in der Dokumentation für die Lizenzierung.

Geben Sie die Lizenzserveradresse im folgenden Format an: *name*:[*port*]. Der Name muss ein FQDN, NetBIOS-Name oder eine IP-Adresse sein. FQDN wird empfohlen. Wenn Sie die Portnummer auslassen, ist der Standardport 27000. Klicken Sie auf **Verbinden**. Sie können erst mit der nächsten Seite des Assistenten fortfahren, wenn eine Verbindung zum Lizenzserver hergestellt wurde.

Energieverwaltung (nur Remote-PC-Zugriff)

Siehe Remote-PC-Zugriff.

Hostverbindung, Netzwerk und Speicher

Wenn Sie für die Bereitstellung von Anwendungen und Desktops VMs auf einem Hypervisor oder in einer Cloud verwenden möchten, können Sie optional die erste Verbindung mit diesem Host erstellen. Sie können außerdem Speicher- und Netzwerksressourcen für die Verbindung festlegen. Nach dem Erstellen der Site können Sie diese Verbindung und Ressourcen ändern und weitere Verbindungen erstellen. Weitere Informationen finden Sie unter Verbindungen und Ressourcen.

Seite "Verbindung": siehe Informationsquellen zum Verbindungstyp.

- Wenn Sie keine VMs auf einem Hypervisor oder in einer Cloud verwenden (oder Studio für die Verwaltung von auf dedizierten Blade-PCs gehosteten Desktops verwenden), wählen Sie als Verbindungstyp **Keine**.
- Wenn Sie eine Remote-PC-Zugriff-Site konfigurieren und Wake-On-LAN verwenden möchten, wählen Sie als Typ **Microsoft System Center Configuration Manager**.

Geben Sie außerdem an, ob Sie Citrix Tools (z. B. Maschinenerstellungsdienste) oder andere Tools zum Erstellen von VMs verwenden möchten.

Seite "Speicher"und "Netzwerk": Informationen über Speichertypen und Verwaltungsmethoden finden Sie unter Hostspeicher, Speicherverwaltung und Speicherauswahl.

Weitere Features

Sie können Features zum Anpassen der Site auswählen. Wenn Sie das Kontrollkästchen eines Elements aktivieren, wird ein Dialogfeld zur Konfiguration angezeigt.

AppDNA-Integration Gilt, wenn Sie AppDisks verwenden und AppDNA installiert haben. Die AppDNA-Integration ermöglicht die Analyse von Anwendungen auf AppDisks. Sie können dann Kompatibilitätsprobleme untersuchen und beheben. Weitere Informationen finden Sie unter AppDisks.

App-V-Veröffentlichung Aktivieren Sie dieses Feature, wenn Sie Anwendungen aus Microsoft App-V-Paketen auf App-V-Servern verwenden. Geben Sie die URL für den App-V-Verwaltungsserver und die URL und Portnummer des App-V-Veröffentlichungsservers an.

Wenn Sie nur Anwendungen von App-V-Paketen in Netzwerkfreigaben verwenden, brauchen Sie das Feature nicht auszuwählen.

Sie können das Feature auch später in Studio aktivieren, deaktivieren und konfigurieren. Weitere Informationen finden Sie unter App-V.

Remote-PC-Zugriff

Informationen über Remote-PC-Zugriffsbereitstellungen finden Sie unter Remote-PC-Zugriff.

Wenn Sie das Wake-On-LAN-Feature verwenden, führen Sie vor dem Erstellen der Site die entsprechende Konfiguration in Microsoft System Center Configuration Manager durch. Weitere Informationen finden Sie unter Microsoft System Center Configuration Manager.

Für das Erstellen einer Remote-PC-Zugriff-Site gilt Folgendes:

- Wenn Sie Wake-On-LAN verwenden, geben Sie die Adresse, Anmeldeinformationen und Verbindungsinformationen für Microsoft System Center Configuration Manager auf der Seite **Energieverwaltung** an.
- Geben Sie Benutzer oder Benutzergruppen auf der Seite **Benutzer** an. Benutzer werden nicht automatisch hinzugefügt. Geben Sie außerdem Maschinenkonten (Domänen- oder OU-Konten) auf der Seite **Maschinenkonten** an.

  Zum Hinzufügen von Benutzern klicken Sie auf **Benutzer hinzufügen**. Wählen Sie Benutzer und Benutzergruppen aus und klicken Sie dann auf **Benutzer hinzufügen**.

  Zum Hinzufügen von Maschinenkonten klicken Sie auf **Maschinenkonten hinzufügen**. Wählen Sie die Maschinenkonten aus und klicken Sie dann auf **Maschinenkonten hinzufügen**. Klicken

Sie auf **Organisationseinheiten hinzufügen**. Wählen Sie die Domäne und die Organisationseinheiten und geben Sie an, ob Elemente in Unterordnern eingeschlossen werden sollen. Klicken Sie auf **Organisationseinheiten hinzufügen**.

Beim Erstellen einer Remote-PC-Zugriff-Site wird automatisch ein Maschinenkatalog erstellt. Der Maschinenkatalog enthält alle Maschinenkonten, die Sie im Assistenten für die Siteerstellung hinzugefügt haben. Es wird automatisch eine Bereitstellungsgruppe erstellt. Sie enthält alle Benutzer und Gruppen, die Sie hinzugefügt haben.

Zusammenfassung

Auf der letzten Seite des Assistenten für die Siteerstellung wird eine Zusammenfassung der von Ihnen angegebenen Informationen angezeigt. Verwenden Sie die Schaltfläche **Zurück**, wenn Sie etwas ändern möchten. Wenn Sie fertig sind, klicken Sie auf **Erstellen**, um die Siteerstellung zu starten.

Testen einer Sitekonfiguration

Zum Durchführen der Tests, nachdem Sie die Site erstellt haben, wählen Sie **Citrix Studio (*Sitename*)** oben im Navigationsbereich. Klicken Sie im mittleren Bereich auf **Site testen**. Sie können einen HTML-Bericht der Testergebnisse für die Site anzeigen.

Der Sitetest kann auf Controllern unter Windows Server 2016 fehlschlagen. Der Fehler tritt auf, wenn eine lokale SQL Server Express-Instanz für die Sitedatenbank verwendet wird und der SQL Server Browser-Dienst nicht gestartet wurde. Führen Sie zur Vermeidung dieses Fehlers die folgenden Schritte aus.

1. Aktivieren Sie den SQL Server Browser-Dienst (falls erforderlich) und starten Sie ihn.
2. Starten Sie den SQL Server-Dienst (SQLEXPRESS) neu.

Problembehandlung

Nach der Konfiguration der Site können Sie Studio installieren und über MMC als Snap-In auf einer Remotemaschine hinzufügen. Wenn Sie später versuchen, das Snap-In zu entfernen, reagiert MMC möglicherweise nicht mehr. Starten Sie als Workaround MMC neu.

Erstellen von Maschinenkatalogen

August 18, 2021

Sammlungen von physischen oder virtuellen Maschinen werden als Einheit in einem sogenannten Maschinenkatalog verwaltet. Alle Maschinen in einem Maschinenkatalog haben den gleichen Betriebssystemtyp: Server oder Desktop. Ein Katalog mit Serverbetriebssystemmaschinen kann entweder Windows- oder Linux-Maschinen enthalten, nicht aber beides.

Nach dem Erstellen der Site werden Sie von Studio zur Erstellung des ersten Maschinenkatalogs geführt. Nach dem Erstellen des ersten Maschinenkatalogs werden Sie in Studio durch das Erstellen der ersten Bereitstellungsgruppe geführt. Später können Sie den erstellten Katalog ändern und weitere Kataloge erstellen.

Übersicht

Wenn Sie einen Katalog virtueller Maschinen erstellen, geben Sie an, wie diese VMs bereitgestellt werden sollen. Sie können Citrix Tools, z. B. Maschinenerstellungsdienste (MCS) oder Provisioning Services (PVS) verwenden. Alternativ können Sie eigene Tools verwenden.

- Wenn Sie Maschinen mit Provisioning Services (PVS) erstellen, lesen Sie die zugehörige Dokumentation.
- Bei Verwendung von Maschinenerstellungsdiensten (MCS) stellen Sie ein Masterimage (bzw. einen Snapshot) zum Erstellen identischer virtueller Maschinen im Katalog bereit. Vor dem Erstellen des Katalogs verwenden Sie die Tools des Hypervisors oder Clouddiensts zum Erstellen und Konfigurieren des Masterimages. Dazu gehört auch die Installation eines Virtual Delivery Agents (VDA) auf dem Image. Dann erstellen Sie den Maschinenkatalog in Studio. Sie wählen das Image (bzw. einen Image-Snapshot) und geben die Anzahl der in dem Katalog zu erstellenden VMs und weitere Informationen an.
- Selbst wenn Sie die Maschinen bereits haben, d. h. keine Masterimages verwenden müssen, erstellen Sie mindestens einen Maschinenkatalog.

Beim Erstellen des ersten Maschinenkatalogs mit MCS oder PVS verwenden Sie die Hostverbindung, die Sie beim Erstellen der Site konfiguriert haben. Nach dem Erstellen des ersten Maschinenkatalogs und der ersten Bereitstellungsgruppe können Sie die Informationen über diese Verbindung ändern und weitere Verbindungen erstellen.

Nach Abschließen des Assistenten zum Erstellen von Maschinenkatalogen werden automatisch Tests ausgeführt, um sicherzustellen, dass der Katalog richtig konfiguriert wurde. Wenn die Tests abgeschlossen sind, können Sie einen Testbericht anzeigen. Sie können die Tests jederzeit über Studio ausführen.

Nur bei lokalen Bereitstellungen: Beim Erstellen des ersten Maschinenkatalogs mit MCS oder PVS verwenden Sie die Hostverbindung, die Sie beim Erstellen der Site konfiguriert haben. Nach dem Erstellen des ersten Maschinenkatalogs und der ersten Bereitstellungsgruppe können Sie die Informationen über diese Verbindung ändern und weitere Verbindungen erstellen.

Wenn Sie einen Katalog direkt mit dem PowerShell-SDK erstellen, können Sie alternativ zu einem Image bzw. einem Snapshot eine Hypervisorvorlage (VMTemplate) angeben.

VDA-Registrierung

Ein VDA muss bei einem Delivery Controller (lokale Bereitstellungen) bzw. Cloud Connector (Citrix Cloud-Bereitstellungen) registriert sein, damit er beim Start gebrokerter Sitzungen in die Auswahl kommt. Nicht registrierte VDAs können eine mangelnde Auslastung verfügbarer Ressourcen zur Folge haben. Es gibt eine Reihe von Gründen, warum ein VDA nicht registriert sein könnte. Viele können vom Administrator behandelt werden. Studio bietet Informationen zur Problembehandlung im Assistenten zum Erstellen von Maschinenkatalogen und nach dem Hinzufügen von Maschinen eines Katalogs zu einer Bereitstellungsgruppe.

Im Assistenten zum Erstellen von Maschinenkatalogen wird nach dem Hinzufügen vorhandener Maschinen in der Liste der Computerkontonamen angezeigt, ob die einzelnen Maschinen zum Hinzufügen zu dem Katalog geeignet sind. Zeigen Sie auf das Symbol neben jeder Maschine, um Informationen dazu einzublenden.

Wenn die Nachricht eine problematische Maschine identifiziert, können Sie diese Maschine entweder entfernen (über die Schaltfläche **Entfernen**) oder die Maschine hinzufügen. Wird beispielsweise gemeldet, dass die Maschineninformationen nicht abgerufen werden konnten (z. B. weil die Maschine nie registriert wurde), können Sie die Maschine auf Wunsch dennoch hinzufügen.

Informationen zu Meldungen zur Funktionsebene finden Sie unter VDA-Versionen und Funktionsebenen.

Weitere Informationen zur Fehlerbehebung bei der VDA-Registrierung finden Sie unter CTX136668.

Überblick über die Katalogerstellung mit MCS

Nachdem Sie Informationen im Assistenten zum Erstellen von Maschinenkatalogen eingegeben haben, erfolgen die nachfolgend aufgeführten Standardaktionen in MCS.

- Wenn Sie ein Masterimage anstelle eines Snapshots ausgewählt haben, erstellt MCS einen Snapshot.
- MCS erstellt eine vollständige Kopie des Snapshots und fügt diese an jedem in der Hostverbindung definierten Speicherort hinzu.
- MCS fügt Active Directory Maschinen hinzu, wodurch eindeutige Identitäten erstellt werden.
- MCS erstellt die im Assistenten angegebene Anzahl VMs mit jeweils zwei Datenträgern. Neben den beiden Datenträgern wird jeweils ein Master am gleichen Speicherort gespeichert. Wenn Sie mehrere Speicherorte definiert haben, werden an jedem die folgenden Datenträgertypen erstellt:

  - Vollständige Kopie des Snapshots (siehe oben); diese ist schreibgeschützt und wird von allen gerade erstellten VMs gemeinsam genutzt.
  - Eine eindeutige 16-MB-Identitätsdisk, durch die jede VM eine eindeutige Identität erhält. Jede VM erhält eine Identitätsdisk.
  - Ein eindeutiger differenzierender Datenträger zum Speichern der auf der VM erfolgten Schreibvorgänge. Dieser Datenträger ist, sofern dies vom Hostspeicher unterstützt wird, für schlanke Speicherzuweisung geeignet und kann bei Bedarf auf die maximale Größe des Masterimages anwachsen. Jede VM erhält einen differenzierenden Datenträger. Der differenzierende Datenträger enthält die im Lauf von Sitzungen gemachten Änderungen. Er ist für dedizierte Desktops permanent. Für gepoolte Desktops wird er nach jedem Neustart gelöscht und neu erstellt.

Alternativ können Sie beim Erstellen von VMs für statische Desktops auf der Seite **Maschinen** des Assistenten zum Erstellen von Maschinenkatalogen Thick Clones (vollständige Kopie) festlegen. Thick Clones erfordern keine Beibehaltung des Masterimages in jedem Datenspeicher. Jede VM hat ihre eigene Datei.

Vorbereiten eines Masterimages auf dem Hypervisor bzw. im Clouddienst

Informationen über das Erstellen von Verbindungen mit Hypervisors und Cloudanbietern finden Sie unter Verbindungen und Ressourcen.

Das Masterimage enthält das Betriebssystem, nicht virtualisierte Anwendungen, den VDA und andere Software.

Nützliche Info:

- Masterimages werden ggf. auch als Klonimage, Golden Image, Basis-VM oder Basisimage bezeichnet. Hosthersteller und Clouddienstanbieter verwenden andere Bezeichnungen.
- Wenn Sie PVS verwenden, können Sie entweder ein Masterimage oder einen physischen Computer als Masterzielgerät verwenden. In Provisioning Services wird für Images eine andere Terminologie verwendet als in MCS. Einzelheiten finden Sie in der Provisioning Services-Dokumentation.
- Stellen Sie sicher, dass der Hypervisor oder Clouddienst über genügend Prozessoren, Arbeitsspeicher und Datenspeicher für die erstellten Maschinen verfügt.
- Konfigurieren Sie die für Desktops und Anwendungen benötigte Menge an Festplattenspeicher. Dieser Wert kann später nicht mehr geändert werden (auch nicht im Maschinenkatalog).
- Bei Remote-PC-Zugriff-Maschinenkatalogen werden keine Masterimages verwendet.
- Hinweise zur Aktivierung von Microsoft-Schlüsselverwaltungsserver bei Verwendung der Maschinenerstellungsdienste: Wenn Ihre Bereitstellung 7.x-VDAs mit einem XenServer 6.1- oder 6.2-Host, einem vSphere-Host oder einem Microsoft System Center Virtual Machine Manager-Host enthält, müssen Sie kein manuelles Rearm für Microsoft Windows oder Microsoft

Office durchführen. Wenn die Bereitstellung einen 5.x-VDA mit einem XenServer 6.0.2-Host enthält, lesen Sie CTX128580.

- Installieren und konfigurieren Sie die folgende Software auf dem Masterimage:
  - Integrationstools für den Hypervisor (z. B. XenServer-Tools, Hyper-V-Integrationsdienste oder VMware-Tools). Wenn Sie diesen Schritt auslassen, funktionieren die Anwendungen und Desktops unter Umständen nicht richtig.
  - Einen VDA: Citrix empfiehlt die Installation der neuesten Version, damit die neuesten Features verfügbar sind. Wird kein VDA auf dem Masterimage installiert, schlägt die Katalogerstellung fehl.
  - Tools von Drittanbietern, zum Beispiel Antivirensoftware oder Agents zur elektronischen Softwareverteilung. Konfigurieren Sie Dienste mit den für Benutzer und Maschinentyp geeigneten Einstellungen (z. B. Featureupdates).
  - Anwendungen von Drittanbietern, die Sie nicht virtualisieren möchten. Citrix empfiehlt, dass Sie Anwendungen virtualisieren. Die Virtualisierung von Anwendungen senkt Kosten, denn das Masterimage muss nach dem Hinzufügen oder Neukonfigurieren einer Anwendung nicht aktualisiert werden. Außerdem belegen weniger installierte Anwendungen weniger Platz auf Masterimage-Festplatten, wodurch Speicherkosten eingespart werden.
  - App-V-Clients mit den empfohlenen Einstellungen, wenn Sie App-V-Anwendungen veröffentlichen möchten. Der App-V-Client ist bei Microsoft erhältlich.
  - Wenn Sie MCS verwenden und Microsoft Windows in lokalisierter Version ausführen möchten, installieren Sie die Gebietsschemas und Sprachpakete. Wenn ein Snapshot beim Provisioning erstellt wird, verwenden die bereitgestellten VMs die installierten Gebietsschemas und Sprachpakete.

> **Wichtig:**
>
> Wenn Sie PVS oder MCS verwenden, führen Sie auf den Masterimages nicht Sysprep aus.

Vorbereiten eines Masterimages

1. Erstellen Sie mit dem Verwaltungstool des Hypervisors ein Masterimage und installieren Sie dann das Betriebssystem sowie alle Service Packs und Updates. Geben Sie die Anzahl der vCPUs an. Sie können den vCPU-Wert auch festlegen, wenn Sie den Maschinenkatalog mit PowerShell erstellen. Beim Erstellen eines Maschinenkatalogs mit Studio können Sie die Anzahl der vCPUs nicht angeben. Konfigurieren Sie die für Desktops und Anwendungen benötigte Menge an Festplattenspeicher. Dieser Wert kann später nicht mehr geändert werden (auch nicht im Maschinenkatalog).
2. Stellen Sie sicher, dass die Festplatte am Gerätestandort 0 verbunden ist. Dieser Standort ist in den meisten Standardmasterimagevorlagen automatisch konfiguriert; in einigen benutzerdefinierten Vorlagen ist dies jedoch nicht unbedingt der Fall.

3. Installieren und konfigurieren Sie die oben aufgeführte Software auf dem Masterimage.
4. Bei Verwendung von PVS erstellen Sie eine VHD-Datei für die vDisk von Ihrem Masterzielgerät, bevor Sie das Masterzielgerät in eine Domäne einbinden. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
5. Wenn Sie MCS nicht verwenden, fügen Sie das Masterimage der Domäne hinzu, zu der die Anwendungen und Desktops gehören. Stellen Sie sicher, dass das Masterimage auf dem Host verfügbar ist, auf dem die Maschinen erstellt werden. Wenn Sie MCS verwenden, ist das Hinzufügen des Masterimages zu einer Domäne nicht erforderlich. Die bereitgestellten Maschinen werden Mitglied der im Assistenten zum Erstellen von Maschinenkatalogen angegebenen Domäne.
6. Citrix empfiehlt, dass Sie einen Snapshot des Masterimages erstellen und benennen, damit es künftig identifiziert werden kann. Wenn Sie ein Masterimage anstelle eines Snapshots beim Erstellen eines Maschinenkatalogs angeben, erstellt Studio automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

Vorbereiten eines Masterimages für GPU-fähige Maschinen auf XenServer

Wenn Sie für Ihre Hostinginfrastruktur XenServer verwenden, benötigen GPU-fähige Maschinen ein dediziertes Masterimage. Diese VMs erfordern Videotreiber, die GPUs unterstützen. Konfigurieren Sie GPU-fähige Maschinen, damit die VM Software verwenden kann, die die GPU für Vorgänge verwendet.

1. Erstellen Sie in XenCenter eine VM mit Standard-VGA sowie Netzwerken und einer vCPU.
2. Aktualisieren Sie die VM-Konfiguration so, dass die GPU (entweder Passthrough oder vGPU) verwendet werden kann.
3. Installieren Sie ein unterstütztes Betriebssystem und aktivieren Sie RDP.
4. Installieren Sie XenServer-Tools und NVIDIA-Treiber.
5. Deaktivieren Sie die VNC-Verwaltungskonsole (Virtual Network Computing), um die Leistung zu optimieren, und starten Sie anschließend die VM neu.
6. Sie werden aufgefordert, RDP zu verwenden. Installieren Sie mit RDP den VDA und starten Sie dann die VM neu.
7. Optional können Sie einen Snapshot der VM erstellen und als Vorlage für andere GPU-Masterimages verwenden.
8. Installieren Sie mit RDP kundenspezifische Anwendungen, die in XenCenter konfiguriert werden und GPU-Funktionen verwenden.

Erstellen eines Maschinenkatalogs mit Studio

Bevor Sie den Assistenten zum Erstellen von Maschinenkatalogen starten, lesen Sie diesen Abschnitt, damit Sie wissen, welche Optionen Sie auswählen und welche Informationen Sie angeben müssen.

Wenn Sie ein Masterimage verwenden, vergewissern Sie sich vor dem Erstellen des Maschinenkatalogs, dass auf dem Image ein VDA installiert ist.

In Studio:

- Wenn Sie eine Site, jedoch noch keinen Maschinenkatalog erstellt haben, führt Studio Sie zum richtigen Startpunkt zur Erstellung eines Maschinenkatalogs.
- Wenn Sie bereits einen Maschinenkatalog erstellt haben und einen weiteren erstellen möchten, wählen Sie im Studio-Navigationsbereich **Maschinenkataloge**. Wählen Sie im Aktionsbereich die Option **Maschinenkatalog erstellen**.

Der Assistent führt Sie durch die nachfolgend beschriebenen Einstellungen. Die angezeigten Assistentenseiten können sich je nach der von Ihnen vorgenommenen Auswahl unterscheiden.

Betriebssystem

Jeder Katalog enthält nur Maschinen eines Typs:

- **Serverbetriebssystem:** Ein Katalog für Serverbetriebssysteme bietet gehostete, freigegebene Desktops und Anwendungen. Auf den Maschinen können die unterstützten Versionen von Windows oder Linux ausgeführt werden, ein Katalog kann jedoch nur Windows- oder Linux-Maschinen enthalten. Informationen zu Linux finden Sie in der Dokumentation zu Linux-VDAs.
- **Desktopbetriebssystem:** Ein Katalog für Desktopbetriebssysteme bietet VDI-Desktops und -Anwendungen, die diversen Benutzern zugewiesen werden können.
- **Remote-PC-Zugriff:** Ein Remote-PC-Zugriff-Katalog bietet Benutzern Remotezugriff auf ihre physischen Büro-Desktopmaschinen. Bei Remote-PC-Zugriff wird VPN nicht für die Sicherheit benötigt.

Maschinenverwaltung

Diese Seite wird nicht angezeigt, wenn Sie einen Katalog für Remote-PC-Zugriff-Maschinen erstellen.

Auf der Seite **Maschinenverwaltung** wird angegeben, wie die Maschinen verwaltet und mit welchem Tool sie bereitgestellt werden.

Wählen Sie, ob für Maschinen in dem Katalog die Energieverwaltung über Studio ausgeführt werden soll.

- Maschinen mit Energieverwaltung über Studio oder über eine Cloudumgebung bereitgestellte Maschinen (z. B. VM oder Blade-PC). Diese Option ist nur verfügbar, wenn bereits eine Verbindung zu einem Hypervisor oder Cloudservice konfiguriert wurde.
- Maschinen ohne Energieverwaltung über Studio (z. B. physische Maschinen).

Wenn Sie angegeben haben, dass die Energieverwaltung der Maschinen über Studio oder die Maschinenbereitstellung über eine Cloudumgebung erfolgen soll, wählen Sie aus, welches Tool für die Erstellung von VMs verwendet werden soll.

- **Citrix Maschinenerstellungsdienste (MCS):** verwendet ein Masterimage zum Erstellen und Verwalten virtueller Maschinen. Bei Maschinenkatalogen in Cloudumgebungen wird MCS verwendet. MCS ist für physische Maschinen nicht verfügbar.
- **Citrix Provisioning Services (PVS):** Verwaltet Zielgeräte als Gerätesammlung. Eine als Image eines Masterzielgeräts erstellte PVS-vDisk liefert Desktops und Anwendungen. Diese Option ist für Cloudbereitstellungen nicht verfügbar.
- **Sonstiges:** Ein Tool, das Maschinen verwaltet, die bereits im Rechenzentrum sind. Citrix empfiehlt die Verwendung von Microsoft System Center Configuration Manager oder einer anderen Drittanbieteranwendung, um sicherzustellen, dass die Maschinen im Katalog konsistent sind.

Desktoptypen (Desktoperfahrung)

Diese Seite wird nur angezeigt, wenn Sie einen Maschinenkatalog mit Desktopbetriebssystemmaschinen erstellen.

Auf der Seite **Desktoperfahrung** wird festgelegt, was bei jeder Benutzeranmeldung passiert. Wählen Sie eine der folgenden Optionen aus:

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

Wenn Sie beim Anmelden eine Verbindung mit einem statischen Desktop herstellen möchten, wird der Bildschirm **Gerätesammlung** angezeigt. Wenn Sie diesen Verbindungstyp einrichten, zeigt der Katalog die Personal vDisk im Benutzerdatenfeld unter dem Maschinentyp an.

Masterimage

Diese Seite wird nur angezeigt, wenn Sie VMs mit MCS erstellen.

Wählen Sie die Verbindung mit dem Host-Hypervisor oder Clouddienst und anschließend den zuvor erstellten Snapshot bzw. die zuvor erstellte virtuelle Maschine. Beim Erstellen des ersten Maschinenkatalogs ist nur die Verbindung verfügbar, die Sie beim Erstellen der Site konfiguriert haben.

Nicht vergessen:

- Wenn Sie MCS (oder PVS) verwenden, führen Sie auf den Masterimages nicht Sysprep aus.
- Wenn Sie ein Masterimage anstelle eines Snapshots angeben, erstellt Studio automatisch einen Snapshot, der jedoch nicht umbenannt werden kann.

Stellen Sie sicher, dass auf dem Masterimage die aktuelle VDA-Version installiert ist, damit Sie die neuesten Produktfeatures verwenden können. Ändern Sie nicht den Standardwert für die Mindestversion des VDAs. Wenn Sie eine ältere VDA-Version verwenden müssen, lesen Sie den Abschnitt VDA-Versionen und Funktionsebenen.

Eine Fehlermeldung wird angezeigt, wenn Sie einen Snapshot oder eine VM auswählen, der bzw. die nicht mit dem zuvor im Assistenten ausgewählten Tool zur Maschinenverwaltung kompatibel ist.

Cloudplattformen/-dienste

Wenn Sie VMs über eine Cloudplattform bzw. einen Clouddienst hosten (z. B. Azure Resource Manager, Nutanix oder Amazon Web Services), kann der Assistent zum Erstellen von Maschinenkatalogen zusätzliche Seiten für den spezifischen Host umfassen.

Einzelheiten finden Sie unter Informationen zu Verbindungstypen.

Gerätesammlung

Diese Seite wird nur angezeigt, wenn Sie VMs mit PVS erstellen. Sie enthält die Gerätesammlungen und Geräte, die noch keinem Katalog hinzugefügt wurden.

Wählen Sie die gewünschten Gerätesammlungen. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.

Maschinen

Diese Seite wird nicht angezeigt, wenn Sie einen Katalog für Remote-PC-Zugriff-Maschinen erstellen.

Der Titel der Seite hängt von der Auswahl ab, die Sie auf der Seite **Maschinenverwaltung** getroffen haben: **Maschinen**, **Virtuelle Maschinen** oder **VMs und Benutzer**.

Bei Verwendung von MCS führen Sie folgende Schritte aus:

- Legen Sie fest, wie viele virtuelle Maschinen erstellt werden sollen.
- Wählen Sie die Menge Arbeitsspeicher in MB, die jede VM haben soll.
- **Wichtig:** Jede erstellte VM hat eine Festplatte. Deren Größe wird im Masterimage festgelegt. Sie können die Festplattengröße im Katalog nicht ändern.
- Wenn Sie auf der Seite **Desktoperfahrung** festgelegt haben, dass die Änderungen der Benutzer an statischen Desktops auf separaten Personal vDisks gespeichert werden sollen, geben Sie deren Größe in Gigabyte und den Laufwerksbuchstaben an.
- Wenn Ihre Bereitstellung mehrere Zonen enthält, können Sie eine Zone für den Katalog wählen.

- Wenn Sie VMs mit statischen Desktops erstellen, wählen Sie einen Kopiermodus für die VMs. Siehe Kopiermodus für virtuelle Maschinen.
- Wenn Sie VMs mit zufälligen Desktops und ohne persönliche vDisks erstellen, können Sie einen Cache für temporäre Daten auf jeder Maschine konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines Cache für temporäre Daten.

Bei Verwendung von PVS führen Sie folgende Schritte aus:

Auf der Seite **Geräte** werden die Geräte in der Gerätesammlung aufgelistet, die Sie auf der vorherigen Seite des Assistenten ausgewählt haben. Auf dieser Seite können Sie keine Maschinen hinzufügen oder entfernen.

Bei Verwendung anderer Tools führen Sie folgende Schritte aus:

Fügen Sie eine Liste der Active Directory-Computerkontonamen hinzu (bzw. importieren Sie eine). Sie können den Active Directory-Kontonamen von VMs nach dem Hinzufügen bzw. Importieren ändern. Wenn Sie im Assistenten auf der Seite **Desktoperfahrung** statische Computer angegeben haben, können Sie optional den Active Directory-Benutzernamen für jede hinzugefügte VM angeben.

Nachdem Sie Namen hinzugefügt oder importiert haben, können Sie mit der Schaltfläche **Entfernen** Namen aus der Liste löschen, während Sie noch auf dieser Assistentenseite sind.

Bei der Verwendung von PVS oder anderer Tools (nicht MCS) führen Sie folgende Schritte aus:

Ein Symbol und eine QuickInfo für jede hinzugefügte (bzw. importierte oder aus einer PVS-Gerätesammlung stammende) Maschine lassen solche Maschinen erkennen, die dem Katalog möglicherweise nicht hinzugefügt oder nicht bei einem Delivery Controller registriert werden können. Einzelheiten finden Sie unter VDA-Versionen und Funktionsebenen.

Kopiermodus für virtuelle Maschinen

Über den auf der Seite **Maschinen** ausgewählten Kopiermodus wird festgelegt, ob MCS Thin Clones (Schnellkopien) oder Thick Clones (vollständige Kopien) des Masterimages erstellen soll. Standardmäßig werden Thin Clones erstellt.

- Thin Clones bieten eine effizientere Speichernutzung und eine schnellere Maschinenerstellung.
- Thick Clones bieten eine bessere Unterstützung für Datenwiederherstellung und Migration, jedoch ggf. bei geringeren IOPS nach Maschinenerstellung.

VDA-Versionen und Funktionsebenen

Die Funktionsebene eines Katalogs steuert, welche Produktfeatures den Maschinen in dem Katalog zur Verfügung stehen. Zur Verwendung von Features, die in neueren Produktversionen eingeführt

wurden ist u. U. ein neuer VDA erforderlich. Das Festlegen einer Funktionsebene stellt den Maschinen in dem Katalog alle mit der entsprechenden Version (und höheren Versionen, wenn die Funktionsebene nicht geändert wird) eingeführten Features zur Verfügung. In dem Katalog enthaltene Maschinen mit einer älteren VDA-Version können dann allerdings nicht registriert werden.

In einer Dropdownliste am unteren Rand der Seite **Maschinen** (bzw. **Geräte**) kann die VDA-Mindestebene zur erfolgreichen Registrierung und somit die Mindestfunktionsebene des Katalogs festgelegt werden. Bei lokalen Bereitstellungen ist standardmäßig die aktuelle Funktionsebene ausgewählt. Wenn Sie der Citrix Empfehlung folgen, von VDAs und Kernkomponenten immer die aktuelle Version zu installieren bzw. immer ein Upgrade auf die aktuelle Version durchzuführen, müssen Sie diese Auswahl nicht ändern. Wenn Sie jedoch ältere VDAs weiterverwenden müssen, wählen Sie hier den richtigen Wert.

Ein XenApp- und XenDesktop-Release enthält möglicherweise keine neue VDA-Version oder der neue VDA hat keine Auswirkungen auf die Funktionsebene. In diesem Fall kann die Funktionsebene auf eine VDA-Version hinweisen, die älter ist als die installierten bzw. aktualisierten Komponenten. Beispiel: XenApp und XenDesktop 7.15 LTSR enthält zwar einen VDA der Version 7.15, die Standardfunktionsebene (7.9 oder später) ist jedoch weiterhin die aktuelle. Nach der Installation bzw. einem Upgrade der Komponenten von Version 7.9–7.14 auf 7.15 LTSR ist daher keine Änderung der Funktionsebene erforderlich.

In Citrix Cloud-Bereitstellungen verwendet Studio eine Standardfunktionsebene, die älter sein kann als die aktuelle.

Die Auswahl der Funktionsebene hat Auswirkungen auf die darüber aufgeführten Maschinen. Eine QuickInfo neben jedem Listeneintrag gibt an, ob der VDA der Maschine mit dem Katalog auf der gewählten Funktionsebene kompatibel ist.

Erfüllt ein VDA einer Maschine die ausgewählte Mindestfunktionsebene nicht, wird eine entsprechende Meldung angezeigt. Sie können den Assistenten fortsetzen, doch betroffene Maschinen werden in der Regel keine Registrierung bei einem Controller durchführen können. Alternativen in diesem Fall:

- Entfernen Sie Maschinen mit älteren VDAs aus der Liste, führen Sie ein Upgrade der VDAs durch und fügen Sie die Maschinen dann erneut hinzu.
- Wählen Sie eine niedrigere Funktionsebene. Es besteht dann allerdings kein Zugriff auf die neuesten Produktfeatures.

Eine Meldung wird außerdem angezeigt, wenn eine Maschine den falschen Typ aufweist und deshalb dem Katalog nicht hinzugefügt werden konnte. Beispiele wären das Hinzufügen einer Servermaschine zu einem Desktopbetriebssystemkatalog oder das Hinzufügen einer für die zufällige Zuteilung erstellten Maschine zu einem Katalog mit statischen Maschinen.

Konfigurieren eines Cache für temporäre Daten

Das lokale Zwischenspeichern temporärer Daten auf VMs ist optional. Sie können den temporären Datencache auf Maschinen aktivieren, wenn Sie MCS zum Verwalten gepoolter (nicht dedizierter) Maschinen in einem Katalog verwenden. Wenn für einen Katalog eine Verbindung verwendet wird, durch die die Speicherung temporärer Daten festgelegt ist, können Sie bei der Katalogerstellung den temporäre Datencache aktivieren und konfigurieren.

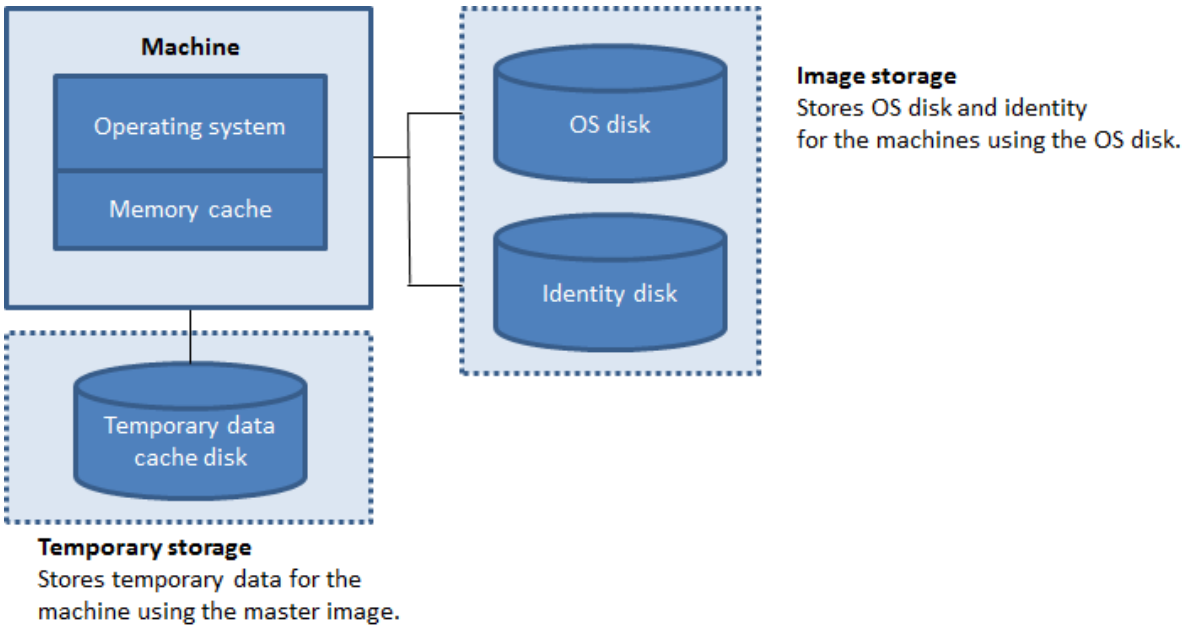
Zum Aktivieren der Zwischenspeicherung temporärer Daten muss der VDA auf jeder Maschine in dem ausgewählten Katalog mindestens in Version 7.9 vorliegen.

Beim Erstellen der Verbindung für den Katalog geben Sie an, ob die temporären Daten in einem freigegebenen oder dem lokalen Speicher abgelegt werden sollen. Einzelheiten hierzu finden Sie unter Verbindungen und Ressourcen. Das Aktivieren und Konfigurieren des temporären Caches im Katalog enthält zwei Kontrollkästchen und Werte: **Dem Cache zugewiesener Speicher (MB)** und **Größe des Datenträgercache (GB)**. Die Standardwerte unterscheiden sich je nach Verbindungstyp. Die Standardwerte sind in den meisten Fällen ausreichen. Allerdings muss der für Folgendes erforderliche Speicherplatz berücksichtigt werden:

- Von Windows selbst erstellte temporäre Datendateien, einschließlich der Windows-Auslagerungsdatei
- Benutzerprofildaten
- ShareFile-Daten, die mit Benutzersitzungen synchronisiert werden
- Gegebenenfalls von einem Sitzungsbenutzer erstellte oder kopierte Daten und alle Anwendungen, die Benutzer möglicherweise sitzungsintern installieren

Windows gestattet nicht, dass für eine Sitzung deutlich mehr Cache verwendet wird, als es freien Speicherplatz auf dem ursprünglichen Masterimage gibt, über das die Maschinen des Maschinenkatalogs bereitgestellt werden. Es ergibt beispielsweise keinen Sinn, eine Cachegröße von 20 GB festzulegen, wenn auf dem Masterimage nur 10 GB freier Speicherplatz verfügbar sind.

Wenn Sie das Kontrollkästchen **Größe des Datenträgercache** aktivieren, werden temporäre Daten zunächst in den Speichercache geschrieben. Wenn der Speichercache seinen konfigurierten Grenzwert erreicht (= Wert für **Dem Cache zugewiesener Speicher**), werden die ältesten Daten zum temporären Datencache-Datenträger verschoben.



Der Speichercache ist Teil der Gesamtspeichermenge auf jeder Maschine. Wenn Sie das Kontrollkästchen **Dem Cache zugewiesener Speicher** aktivieren, sollten Sie daher die Gesamtspeichergröße auf jeder Maschine erhöhen.

Wenn Sie das Kontrollkästchen **Dem Cache zugewiesener Speicher** deaktivieren und das Kontrollkästchen **Größe des Datenträgercache** aktiviert lassen, werden temporäre Daten direkt auf den Cachedatenträger geschrieben, wobei ein minimale Menge an Speichercache verwendet wird.

Das Ändern der **Datenträgercachegröße** vom Standardwert kann sich auf die Leistung auswirken. Die Größe muss gemäß den Anforderungen der Benutzer und der Maschinenlast gewählt werden.

> **Wichtig:**
>
> Wenn auf dem Datenträgercache nicht mehr genügend Speicherplatz vorhanden ist, wird die Sitzung des Benutzers unbrauchbar.

Wenn Sie das Kontrollkästchen **Größe des Datenträgercache** deaktivieren, wird kein Datenträgercache erstellt. Geben Sie in diesem Fall für **Dem Cache zugewiesener Speicher** einen Wert an, der groß genug ist, um alle temporären Daten zu speichern. Dies ist nur möglich, wenn große Mengen an RAM für die Zuweisung zu jeder VM verfügbar sind.

Wenn Sie beide Kontrollkästchen deaktivieren, werden temporäre Daten nicht zwischengespeichert, sondern für jede VM auf den differenzierenden Datenträger (im Betriebssystemspeicher) geschrieben. (Dies ist die Provisioning-Aktion in Releases vor 7.9.)

Aktivieren Sie die Zwischenspeicherung nicht, wenn ein Katalog zum Erstellen von AppDisks verwendet werden soll.

Diese Funktion ist nicht verfügbar, wenn eine Nutanix-Hostverbindung verwendet wird.

Die Cachewerte für einen Maschinenkatalog können nach dessen Erstellung nicht geändert werden.

Netzwerkkarten

Diese Seite wird nicht angezeigt, wenn Sie einen Katalog für Remote-PC-Zugriff-Maschinen erstellen.

Wenn Sie mehrere Netzwerkkarten verwenden möchten, weisen Sie jeder ein virtuelles Netzwerk zu. Sie können beispielsweise einer Karte ein bestimmtes sicheres Netzwerk und einer anderen ein häufiger verwendetes Netzwerk zuweisen. Auf dieser Seite können Sie auch Netzwerkkarten hinzufügen und entfernen.

Maschinenkonten

Diese Seite wird nur angezeigt, wenn Sie einen Katalog für Remote-PC-Zugriff-Maschinen erstellen.

Geben Sie die hinzuzufügenden Active Directory-Maschinenkonten oder Organisationseinheiten an, die Benutzern oder Benutzergruppen entsprechen. Verwenden Sie keinen Schrägstrich (/) in Namen von Organisationseinheiten.

Sie können eine zuvor konfigurierte Energieverwaltungsverbindung auswählen oder die Energieverwaltung nicht verwenden. Wenn Sie die Energieverwaltung verwenden möchten, jedoch noch keine geeignete Verbindung konfiguriert wurde, können Sie die Verbindung später erstellen und dann die Energieverwaltungseinstellungen des Maschinenkatalogs entsprechend bearbeiten.

Computerkonten

Diese Seite wird nur angezeigt, wenn Sie VMs mit MCS erstellen.

Jede Maschine im Maschinenkatalog benötigt ein Active Directory-Computerkonto. Geben Sie an, ob neue Konten erstellt oder vorhandene Konten verwendet werden sollen, und geben Sie den Speicherort für diese Konten an.

- Wenn Sie neue Konten erstellen, müssen Sie Zugang zu einem Domänenadministratorkonto für die Domäne haben, in der die Maschinen residieren werden.

Legen Sie für die zu erstellenden Maschinen das Kontobenennungsschema mit Hashmarkierungen zur Kennzeichnung der Platzierung sequenzieller Zahlen bzw. Buchstaben fest. Verwenden Sie keinen Schrägstrich (/) in Namen von Organisationseinheiten. Namen dürfen nicht mit einer Zahl beginnen. Beispiel: Das Benennungsschema “PC-Vertrieb-##”(und Aktivierung von 0-9) bewirkt eine Benennung der Computerkonten als “PC-Vertrieb-01”, “PC-Vertrieb-02”, “PC-Vertrieb-03”usw.

- Wenn Sie bestehende Konten verwenden, navigieren Sie zu den Konten oder klicken Sie auf **Importieren** und geben Sie eine CSV-Datei mit den Kontonamen an. Die importierte Datei muss folgendes Format haben:

```
[ADComputerAccount]
ADcomputeraccountname.domain
...
<!--NeedCopy-->
```

Stellen Sie sicher, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Da diese Konten von Studio verwaltet werden, gestatten Sie Studio, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort (muss für alle Konten gleich sein) an.

Bei Katalogen mit physischen oder vorhandenen Maschinen wählen Sie vorhandene Konten aus oder importieren Sie diese, und weisen Sie jeder Maschine sowohl ein Active Directory-Computerkonto als auch ein Benutzerkonto zu.

Bei Maschinen, die mit PVS erstellt wurden, werden Computerkonten für Zielgeräte anders verwaltet. Weitere Informationen hierzu finden Sie in der Dokumentation zu Provisioning Services.

Zusammenfassung, Name und Beschreibung

Überprüfen Sie auf der Seite **Zusammenfassung** des Assistenten die von Ihnen angegebenen Informationen. Geben Sie einen Namen und eine Beschreibung für den Katalog ein. Diese Informationen werden in Studio angezeigt.

Klicken Sie nach dem Überprüfen der Informationen auf **Fertig** um die Katalogerstellung zu starten.

Problembehandlung

Citrix empfiehlt, Protokolle zu erstellen, um die Arbeit des Supportteams zu unterstützen. Verwenden Sie das Verfahren in diesem Abschnitt, um Protokolldateien zu generieren:

1. Erstellen Sie auf dem Masterimage den folgenden Registrierungsschlüssel mit dem Wert 1 (als DWORD-Wert (32-Bit)):

   ```
   HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING
   ```

2. Fahren Sie das Masterimage herunter und erstellen Sie einen neuen Snapshot.
3. Führen Sie den folgenden Befehl auf dem Delivery Controller aus:

   ```
   Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
    -Value $True
   ```

4. Erstellen Sie einen neuen Katalog basierend auf diesem Snapshot.

5. Nachdem die Vorbereitungs-VM auf dem Hypervisor erstellt wurde, melden Sie sich an und extrahieren folgende Dateien aus dem Stammverzeichnis von Laufwerk C:\:
   - Image-prep.log
   - PvsVmAgentLog.txt
6. Fahren Sie die Maschine herunter. Dabei wird ein Fehler gemeldet.
7. Führen Sie den folgenden PowerShell-Befehl aus, um das automatische Herunterfahren der Image-Vorbereitungsmaschinen erneut zu aktivieren:

   ```
   Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdo
   ```

Verwalten von Maschinenkatalogen

November 9, 2020

Einführung

Sie können Maschinen in Maschinenkatalogen hinzufügen und entfernen, zusätzlich zum Umbenennen, Ändern der Maschinenbeschreibungen und Verwalten der Active Directory-Computerkonten des Katalogs.

Zur Verwaltung von Katalogen gehören ggf. auch die Aktualisierung des Betriebssystems und der Antivirensoftware der enthaltenen Maschinen, ein Upgrade des Betriebssystems und Änderungen an der Konfiguration.

- Maschinenkataloge mit gepoolt-zufälligen Maschinen, die mit Maschinenerstellungsdiensten (MCS) erstellt wurden, pflegen Sie, indem Sie das Masterimage des Katalogs aktualisieren. Nachdem die Masterimages aktualisiert wurden, aktualisieren Sie die Maschinen. Mit diesem Prozess können Sie eine große Anzahl Maschinen effizient aktualisieren. Bei mit Provisioning Services erstellten Maschinen werden Updates über die vDisk verteilt. Weitere Informationen finden Sie in der Dokumentation zu Provisioning Services.
- Bei Katalogen mit statischen (permanent zugewiesenen) oder Remote-PC-Zugriff-Maschinen verwalten Sie Updates an den Maschinen der Benutzer Studio-extern entweder einzeln oder zusammen mit Bereitstellungssoftware von Drittanbietern.

Weitere Informationen zum Erstellen und Verwalten von Verbindungen mit Hosthypervisors und Clouddiensten finden Sie unter Verbindungen und Ressourcen.

Informationen zu persistenten Instanzen

Beim Update eines MCS-Katalogs, der mit persistenten, also dedizierten Instanzen, erstellt wurde, verwenden alle neu für den Katalog erstellten Maschinen das aktualisierte Bild. Bereits vorhandene Instanzen verwenden weiterhin die ursprüngliche Instanz. Dafür muss das Masterimage mit PowerShell-Befehlen aktualisiert werden. Weitere Informationen finden Sie im Knowledge Center-Artikel CTX129205.

Das Update eines Images wird für jeden anderen Katalogtyp auf die gleiche Weise durchgeführt. Beachten Sie Folgendes:

- Bei persistenten Datenträgerkatalogen werden die bereits vorhandenen Maschinen nicht auf das neue Image aktualisiert. Alle neu dem Katalog hinzugefügten Maschinen verwenden aber das neue Image.
- Bei nichtpersistenten Datenträgerkatalogen wird das Maschinenimage aktualisiert, wenn die Maschine das nächste Mal zurückgesetzt wird.
- Bei persistenten Maschinenkatalogen werden durch das Update des Images auch die Kataloginstanzen aktualisiert, die es verwenden.
- Bei nichtpersistenten Katalogen müssen Images in separaten Katalogen sein, wenn Sie unterschiedliche Images für verschiedene Maschinen brauchen.

Hinzufügen von Maschinen im Maschinenkatalog

Vorbereitungen:

- Stellen Sie sicher, dass der Virtualisierungshost (Hypervisor oder Clouddienstanbieter) genügend Prozessoren, Arbeitsspeicher und Speicher zur Unterbringung der zusätzlichen Maschinen hat.
- Stellen Sie sicher, dass Sie genügend ungenutzte Active Directory-Computerkonten haben. Wenn Sie bestehende Konten verwenden, können Sie nur so viele Maschinen erstellen, wie Sie Konten haben.
- Wenn Sie Active Directory-Computerkonten für die zusätzlichen Maschinen mit Studio erstellen, müssen Sie die erforderlichen Domänenadministratorrechte haben.

Hinzufügen von Maschinen zum Maschinenkatalog

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Maschinenkatalog und dann im Bereich **Aktionen** die Option **Maschinen hinzufügen**.
3. Legen Sie die Anzahl der hinzuzufügenden virtuellen Maschinen fest.
4. Gibt es nicht genügend Active Directory-Konten für die Zahl der VMs, die Sie hinzufügen möchten, wählen Sie die Domäne und den Speicherort, an dem Konten erstellt werden

sollen. Legen Sie ein Kontobenennungsschema mit Hashmarkierungen zur Kennzeichnung der Platzierung sequenzieller Zahlen bzw. Buchstaben fest. Verwenden Sie keinen Schrägstrich (/) in Namen von Organisationseinheiten. Namen dürfen nicht mit einer Zahl beginnen. Beispiel: Das Benennungsschema "PC-Vertrieb-##"(und Aktivieren von 0-9) bewirkt eine Benennung der Computerkonten als "PC-Vertrieb-01", "PC-Vertrieb-02", "PC-Vertrieb-03"usw.

5. Wenn Sie bestehende Active Directory-Konten verwenden, navigieren Sie zu den Konten oder klicken Sie auf **Importieren** und geben Sie eine CSV-Datei mit Kontonamen an. Stellen Sie sicher, dass Sie ausreichend Konten für die hinzuzufügenden Maschinen haben. Studio verwaltet diese Konten. Gestatten Sie Studio, die Kennwörter für alle Konten zurückzusetzen, oder geben Sie das Kontokennwort (muss für alle Konten gleich sein) an.

Die Maschinen werden in einem Hintergrundprozess erstellt, der beim Erstellen einer großen Zahl von Maschinen lange dauern kann. Die Maschinenerstellung wird fortgesetzt, selbst wenn Sie Studio schließen.

Löschen von Maschinen aus einem Maschinenkatalog

Wenn Sie eine Maschine aus einem Maschinenkatalog löschen, können Benutzer nicht mehr darauf zugreifen. Vergewissern Sie sich vor dem Löschen daher, dass folgende Bedingungen erfüllt sind:

- Die Benutzerdaten wurden gesichert oder werden nicht mehr benötigt.
- Alle Benutzer sind abgemeldet. Durch das Aktivieren des Wartungsmodus wird verhindert, dass neue Verbindungen mit einer Maschine hergestellt werden.
- Die Maschinen sind ausgeschaltet.

Löschen von Maschinen aus einem Maschinenkatalog

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Bereich **Aktionen** die Option **Maschinen anzeigen**.
3. Wählen Sie eine oder mehrere Maschinen und dann im Bereich **Aktionen** die Option **Löschen**.

Wählen Sie aus, ob die Maschinen wirklich gelöscht werden sollen. Falls ja, geben Sie an, ob die zugehörigen Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen.

Ändern einer Maschinenkatalogbeschreibung oder der Remote-PC-Zugriff-Einstellungen

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Bereich **Aktionen** die Option **Maschinenkatalog bearbeiten**.

3. Nur bei Remote-PC-Zugriff-Katalogen: Auf der Seite **Energieverwaltung** können Sie die Energieverwaltungseinstellungen ändern und eine Energieverwaltungsverbindung auswählen. Verwenden Sie die Seite **Organisationseinheiten** zum Hinzufügen und Entfernen von Active Directory-Organisationseinheiten.
4. Ändern Sie auf der Seite **Beschreibung** die Beschreibung des Maschinenkatalogs.

Umbenennen von Maschinenkatalogen

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Bereich **Aktionen** die Option **Maschinenkatalog umbenennen**.
3. Geben Sie den neuen Namen ein.

Verschieben eines Maschinenkatalogs in eine andere Zone

Wenn eine Bereitstellung mehrere Zonen enthält, können Sie Maschinenkataloge von Zone zu Zone verschieben.

Wenn Sie einen Maschinenkatalog aus dem Hypervisor oder Clouddienst mit den zugehörigen VMs in eine andere Zone verschieben, kann sich dies negativ auf die Leistung auswirken.

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Bereich **Aktionen** die Option **Verschieben**.
3. Wählen Sie die Zone aus, in die Sie den Katalog verschieben möchten.

Löschen von Maschinenkatalogen

Vor dem Löschen eines Katalogs müssen Sie Folgendes sicherstellen:

- Alle Benutzer sind abgemeldet und es werden keine getrennten Sitzungen ausgeführt.
- Der Wartungsmodus ist für alle Maschinen in dem Katalog aktiviert, damit keine neuen Verbindungen hergestellt werden können.
- Alle Maschinen in dem Katalog sind ausgeschaltet.
- Der Katalog ist keiner Bereitstellungsgruppe zugeordnet. Das heißt, keine Bereitstellungsgruppe enthält Maschinen aus dem Katalog.

Löschen eines Maschinenkatalogs

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Katalog und dann im Bereich **Aktionen** die Option **Maschinenkatalog löschen**.

3. Geben Sie an, ob die Maschinen in dem Katalog gelöscht werden sollen. Falls ja, geben Sie an, ob die zugehörigen Active Directory-Computerkonten beibehalten, deaktiviert oder gelöscht werden sollen.

Verwalten von Active Directory-Computerkonten in einem Maschinenkatalog

Zum Verwalten von Active Directory-Konten in einem Maschinenkatalog haben Sie folgende Möglichkeiten:

- Freigeben nicht verwendeter Maschinenkonten durch Entfernen von Active Directory-Computerkonten aus Desktopbetriebssystem- und Serverbetriebssystemmaschinenkatalogen. Diese Konten können dann für andere Maschinen verwendet werden.
- Hinzufügen von Konten, damit beim Hinzufügen weiterer Maschinen zum Katalog Computerkonten bereit stehen. Verwenden Sie keinen Schrägstrich (/) in Namen von Organisationseinheiten.

Verwalten von Active Directory-Konten

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Maschinenkatalog und dann im Bereich **Aktionen** die Option **Active Directory-Konten** verwalten.
3. Entscheiden Sie, ob Sie Computerkonten hinzufügen oder löschen möchten. Wenn Sie Konten hinzufügen, geben Sie an, wie mit den Kennwörtern verfahren werden soll: Setzen Sie entweder alle zurück oder geben Sie ein für alle Konten geltendes Kennwort ein. Sie können die Kennwörter zurückzusetzen, wenn Sie die aktuellen Kennwörter nicht kennen. Zum Zurücksetzen von Kennwörtern müssen Sie die entsprechende Berechtigung haben. Wenn Sie ein Kennwort eingeben, wird das Kennwort von Konten beim Importieren geändert. Wenn Sie ein Konto löschen, legen Sie fest, ob das Konto in Active Directory beibehalten, deaktiviert oder gelöscht werden soll.

Sie können auch angeben, ob Active Directory-Konten beibehalten, deaktiviert oder gelöscht werden sollen, wenn Sie Maschinen aus einem Katalog entfernen oder einen Katalog löschen.

Aktualisieren von Maschinenkatalogen

Citrix empfiehlt, vor dem Durchführen von Updates von Maschinen in einem Katalog Kopien oder Snapshots der Masterimages zu speichern. In der Datenbank wird von jedem Masterimage eines Maschinenkatalogs ein historischer Datensatz beibehalten. Bei Problemen mit Updates, die auf den Benutzerdesktops bereitgestellt wurden, können Sie das Masterimage auf die vorherige Version

zurücksetzen und die Downtime für Benutzer minimieren. Masterimages dürfen nicht gelöscht, verschoben oder umbenannt werden, da ansonsten Kataloge nicht auf ihre Verwendung zurückgesetzt werden können.

Bei Maschinenkatalogen, die Provisioning Services verwenden, müssen Sie eine neue vDisk veröffentlichen, um Änderungen auf den Katalog anzuwenden. Informationen hierzu finden Sie in der Dokumentation zu Provisioning Services.

Nachdem eine Maschine aktualisiert wurde, wird sie automatisch neu gestartet.

Aktualisieren oder Erstellen eines Masterimages

Bevor Sie einen Maschinenkatalog aktualisieren, aktualisieren Sie zunächst ein vorhandenes Masterimage oder erstellen Sie eins auf dem Hypervisor.

1. Erstellen Sie auf dem Hypervisor bzw. im Clouddienst einen Snapshot der aktuellen VM und geben Sie diesem einen aussagekräftigen Namen. Der Snapshot kann notfalls zur Wiederherstellung (Rollback) der Maschinen in dem Katalog verwendet werden.
2. Falls erforderlich, schalten Sie das Masterimage ein und melden Sie sich an.
3. Installieren Sie Updates bzw. nehmen Sie die erforderlichen Änderungen am Masterimage vor.
4. Wenn das Masterimage eine persönliche vDisk verwendet, aktualisieren Sie den Bestand.
5. Schalten Sie die virtuelle Maschine aus.
6. Erstellen Sie einen Snapshot der VM und geben Sie diesem einen aussagekräftigen Namen, der bei der Aktualisierung des Katalogs in Studio erkannt wird. Obwohl Studio einen Snapshot erstellen kann, empfiehlt Citrix, dass Sie einen Snapshot mit der Hypervisor-Verwaltungskonsole erstellen und dann den Snapshot in Studio auswählen. Dadurch können Sie statt eines automatisch erstellten Namens einen aussagekräftigen Namen und eine Beschreibung zuweisen. Bei GPU-Masterimages können Sie das Masterimage nur über die XenServer XenCenter-Konsole ändern.

Aktualisieren des Katalogs

Vorbereiten und Verteilen des Updates auf allen Maschinen in einem Katalog

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie einen Maschinenkatalog und dann im Bereich **Aktionen** die Option **Maschinen aktualisieren**.
3. Wählen Sie auf der Seite **Masterimage** den Host und das Masterimage aus, das Sie verwenden möchten.
4. Legen Sie auf der Seite **Rolloutstrategie** fest, wann die Aktualisierung der Maschinen im Maschinenkatalog erfolgen soll: beim nächsten Herunterfahren oder sofort. Details hierzu finden Sie weiter unten.

5. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und klicken Sie auf **Fertig stellen**. Jede Maschine wird nach erfolgter Aktualisierung automatisch neu gestartet. Ein VDA im Wartungsmodus kann nicht neu gestartet werden.

Wenn Sie einen Katalog direkt mit dem PowerShell-SDK anstelle von Studio aktualisieren, können Sie alternativ zu einem Image bzw. einem Image-Snapshot eine Hypervisorvorlage (VMTemplates) angeben.

Rolloutstrategie Das Imageupdate beim nächsten Herunterfahren wirkt sich sofort auf alle nicht in Verwendung befindliche Maschinen aus, d. h. auf Maschinen ohne aktive Benutzersitzung. In Verwendung befindliche Systeme erhalten das Update bei Beenden der aktiven Sitzung. Beachten Sie Folgendes:

- Neue Sitzungen können erst gestartet werden, wenn das Update auf einer Maschine abgeschlossen ist.
- Desktopbetriebssystemmaschinen werden, wenn sie nicht in Verwendung sind bzw. keine Benutzer angemeldet sind, sofort aktualisiert.
- Bei Serverbetriebssystemen mit untergeordneten Maschinen werden keine automatischen Neustarts durchgeführt. Sie müssen manuell heruntergefahren und neu gestartet werden.

> *Tipp:*
>
> Zum Beschränken der Anzahl neu gestarteter Maschine können Sie die erweiterten Einstellungen für eine Hostverbindung verwenden. Über diese Einstellungen können Sie die für einen Katalog durchgeführten Aktionen ändern. Erweiterte Einstellungen variieren je nach Hypervisor.

Wenn Sie das Image sofort aktualisieren, konfigurieren Sie eine Zeit und Benachrichtigungen für die Verteilung.

- **Verteilungszeit:** Sie können festlegen, dass alle Maschinen gleichzeitig aktualisiert werden oder die Gesamtzeitdauer zum Beginnen des Updates aller Maschinen im Katalog angeben. Ein interner Algorithmus bestimmt, wann welche Maschine während dieses Zeitraums aktualisiert und neu gestartet wird.
- **Benachrichtigung:** Wählen Sie in der Dropdownliste “Benachrichtigung”links aus, ob auf den Maschinen eine Meldung angezeigt werden soll, bevor ein Update beginnt. In der Standardeinstellung wird keine Meldung angezeigt. Wenn Sie festlegen, dass 15 Minuten vor dem Update eine Meldung angezeigt wird, können Sie in der rechten Dropdownliste vorgeben, dass die Meldung alle fünf Minuten nach der Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt. Sofern Sie kein gleichzeitiges Update aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine zu der von dem internen Algorithmus berechneten Zeit vor dem Update angezeigt.

Rollback eines Updates

Nach Bereitstellung eines aktualisierten/neuen Masterimages können Sie diese mit einem Rollback rückgängig machen. Dies kann erforderlich sein, wenn Probleme bei den aktualisierten Maschinen auftreten. Bei einem Rollback werden die Maschinen in dem Katalog auf das letzte funktionierende Image zurückgesetzt. Neue Features, die das neue Image erfordern, stehen dann nicht mehr zur Verfügung. Bei einem Rollback einer Maschine ist ein Neustart erforderlich.

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie den Maschinenkatalog aus und wählen Sie dann im Bereich **Aktionen** die Option **Rollback für Maschinenupdate**.
3. Legen Sie fest, wann das ältere Masterimage auf die Maschinen angewendet werden soll (gemäß den Rollout-Anweisungen oben).

Das Rollback wird nur auf Maschinen angewendet, die zurückgesetzt werden müssen. Benutzer von Maschinen, die nicht mit dem neuen/aktualisierten Masterimage aktualisiert wurden (z. B. weil sie sich nicht abgemeldet hatten), erhalten keine Meldung und müssen sich nicht abmelden.

Durchführen eines Upgrades eines Maschinenkatalogs und Rückgängigmachen eines Upgrades

Aktualisieren Sie den Maschinenkatalog nach dem Upgrade der VDAs auf den Maschinen auf eine neuere Version. Citrix empfiehlt das Upgrade aller VDAs auf die aktuelle Version, damit Zugriff auf alle neuen Features besteht.

Upgradevorbereitung:

- Wenn Sie Provisioning Services verwenden, aktualisieren Sie die VDA-Version. Die Provisioning Konsole behält die VDA-Version nicht bei. Provisioning Services kommuniziert direkt mit dem XenApp- und XenDesktop -Setupassistenten, um die VDA-Version im erstellten Katalog festzulegen.
- Starten Sie die aktualisierten Maschinen, damit sie sich bei dem Controller registrieren. Auf diese Weise kann Studio feststellen, dass die Maschinen im Maschinenkatalog aktualisiert werden müssen.

Durchführen des Upgrades eines Maschinenkatalogs

1. Wählen Sie im **Studio**-Navigationsbereich **Maschinenkataloge**.
2. Wählen Sie den Katalog aus. Auf der Registerkarte **Details** im unteren Bereich werden Versionsinformationen angezeigt.
3. Wählen Sie **Katalog aktualisieren**. Wenn Studio erkennt, dass für den Katalog ein Upgrade erforderlich ist, wird eine Meldung angezeigt. Folgen Sie den Anweisungen. Kann eine Maschine

nicht aktualisiert werden, wird eine Meldung mit einer Erläuterung der Ursache des Problems angezeigt. Citrix empfiehlt, dass Sie alle Maschinenprobleme beheben, bevor Sie den Maschinenkatalog aktualisieren, damit alle Maschinen einwandfrei funktionieren.

Wenn das Katalogupgrade abgeschlossen ist, können Sie Maschinen auf ihren vorherigen Zustand zurücksetzen, indem Sie den Maschinenkatalog und dann im Bereich **Aktionen** die Option **Rückgängig machen** wählen.

Problembehandlung

Empfehlungen für Maschinen mit einem unbekannten Energiezustand finden Sie unter CTX131267.

Erstellen von Bereitstellungsgruppen

August 18, 2021

Eine Bereitstellungsgruppe ist eine Sammlung von Maschinen aus einem oder mehreren Maschinenkatalogen. Die Bereitstellungsgruppe gibt an, welche Benutzer diese Maschinen verwenden können und welche Anwendungen bzw. Desktops für diese Benutzer verfügbar sein sollen.

Das Erstellen einer Bereitstellungsgruppe ist nach dem Erstellen einer Site und eines Maschinenkatalogs der nächste Schritt beim Konfigurieren der Bereitstellung. Später können Sie die anfänglichen Einstellungen der ersten Bereitstellungsgruppe ändern und weitere Bereitstellungsgruppen erstellen. Es gibt Features und Einstellungen, die Sie nur beim Bearbeiten einer Bereitstellungsgruppe, nicht aber beim Erstellen konfigurieren können.

Beim Erstellen einer Remote-PC-Zugriff-Site wird automatisch eine Bereitstellungsgruppe namens **Remote-PC-Zugriff-Desktops** erstellt.

Erstellen einer Bereitstellungsgruppe

1. Wenn Sie eine Site und einen Maschinenkatalog, jedoch noch keine Bereitstellungsgruppe erstellt haben, führt Studio Sie zum richtigen Startpunkt für die Erstellung einer Bereitstellungsgruppe. Wenn Sie bereits eine Bereitstellungsgruppe erstellt haben und eine weitere erstellen möchten, wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** und dann im Aktionsbereich **Bereitstellungsgruppe erstellen**.
2. Der Assistent zum Erstellen von Bereitstellungsgruppen wird mit der **Einführungsseite** gestartet, die Sie für zukünftige Starts des Assistenten deaktivieren können.
3. Der Assistent führt Sie durch die nachfolgend beschriebenen Seiten. Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur letzten Seite gelangen.

Schritt 1. Maschinen

Wählen Sie einen Maschinenkatalog und die Anzahl der Maschinen, die Sie aus dem Katalog verwenden möchten.

Nützliche Info:

- Mindestens eine Maschine in dem ausgewählten Katalog muss unbenutzt bleiben.
- Ein Maschinenkatalog kann in mehreren Bereitstellungsgruppen angegeben werden, eine Maschine kann jedoch nur in einer Bereitstellungsgruppe verwendet werden.
- Eine Bereitstellungsgruppe kann Maschinen aus mehreren Maschinenkatalogen verwenden, diese Kataloge müssen allerdings Maschinen desselben Typs enthalten (Serverbetriebssystemmaschinen oder Desktopbetriebssystemmaschinen oder Remote-PC-Zugriff-Maschinen). Sie können also in einer Bereitstellungsgruppe nicht verschiedene Maschinentypen mischen. Umfasst Ihre Bereitstellung Maschinenkataloge für Windows-Maschinen und solche für Linux-Maschinen, darf eine Bereitstellungsgruppe nur Maschinen eines Betriebssystems enthalten.
- Citrix empfiehlt, dass Sie alle Maschinen mit der neuesten VDA-Version installieren oder aktualisieren und dann das Upgrade von Maschinenkatalogen und Bereitstellungsgruppen nach Bedarf durchführen. Wenn Sie beim Erstellen einer Bereitstellungsgruppe Maschinen mit verschiedenen VDA-Versionen auswählen, ist die resultierende Bereitstellungsgruppe kompatibel mit der ältesten VDA-Version. (Dies wird als *Funktionsebene* bezeichnet.) Wenn auf einer der ausgewählten Maschinen beispielsweise ein VDA der Version 7.1 und auf den anderen die aktuelle VDA-Version installiert ist, können alle Maschinen der Gruppe nur die Features verwenden, die vom VDA der Version 7.1 unterstützt werden. Das bedeutet, dass einige Features, die neuere VDA-Versionen erfordern, in der Bereitstellungsgruppe möglicherweise nicht zur Verfügung stehen. Zur Verwendung von AppDisks müssen die VDAs (und somit Funktionsebene der Gruppe) beispielsweise mindestens in Version 7.8 vorliegen.
- Alle Maschinen in einem Remote-PC-Zugriff-Maschinenkatalog werden automatisch einer Bereitstellungsgruppe zugewiesen. Wenn Sie eine Remote-PC-Zugriff-Site erstellen, werden automatisch ein Maschinenkatalog unter dem Namen **Remote-PC-Zugriff-Maschinen** und eine Bereitstellungsgruppe unter dem Namen **Remote-PC-Zugriff-Desktops** erstellt.

Schritt 2. Bereitstellungstyp

Diese Seite wird nur angezeigt, wenn Sie einen Maschinenkatalog mit statischen (zugewiesen) Desktopbetriebssystemmaschinen auswählen. Wählen Sie auf der Seite "Bereitstellungstyp" entweder **Anwendungen** oder **Desktops**. Sie können nicht beide Optionen wählen.

Wenn Sie Maschinen aus einem Katalog mit Serverbetriebssystemmaschinen oder einem Katalog mit nach dem Zufallsprinzip zugewiesenen (gepoolten) Desktopbetriebssystemmaschinen ausgewählt

haben, wird als Bereitstellungstyp "Anwendungen und Desktops"angenommen. Sie können Anwendungen, Desktops oder beides bereitstellen.

Schritt 3. AppDisks

Klicken Sie auf **Hinzufügen**, um eine AppDisk hinzuzufügen. Im Dialogfeld "AppDisks auswählen" werden in der linken Spalte die verfügbaren AppDisks angezeigt. In der rechten Spalte werden die Anwendungen auf der jeweiligen AppDisk angezeigt. (Bei Auswahl der Registerkarte **Anwendungen** oberhalb der rechten Spalte werden die Anwendungen in einem dem Startmenü ähnlichen Format angezeigt. Wenn Sie auf die Registerkarte **Installierte Pakete** klicken, werden die Anwendungen ähnlich wie unter "Programme und Features"angezeigt.) Wählen Sie ein oder mehrere Kontrollkästchen.

AppDisks sind veraltet.

Schritt 4. Benutzer

Geben Sie die Benutzer und Benutzergruppen an, die die Anwendungen und/oder Desktops in der Bereitstellungsgruppe verwenden können.

Festlegung von Benutzerlisten

Active Directory-Benutzerlisten werden angegeben, wenn Sie Folgendes erstellen oder bearbeiten:

- Benutzerzugriffsliste für eine Site, die nicht über Studio konfiguriert wird. Standardmäßig umfasst die Anwendungsanspruch-Richtlinienregel alle Benutzer (Einzelheiten siehe BrokerAppEntitlementPolicyRule-Cmdlets des PowerShell-SDKs).
- Anwendungsgruppen (sofern konfiguriert)
- Bereitstellungsgruppen
- Anwendungen:

Die Liste der Benutzer, die Zugriff auf eine Anwendung über StoreFront haben, wird aus der Schnittmenge der oben angegebenen Benutzerlisten erstellt. Beispiel: Konfigurieren der Verwendung von Anwendung A für eine bestimmte Abteilung, ohne den Zugriff auf andere Gruppen übermäßig einzuschränken:

- Verwenden der Standardanwendungsanspruch-Richtlinienregel, die für alle Benutzer gilt
- Konfigurieren Sie die Benutzerliste der Bereitstellungsgruppe so, dass alle Benutzer der Organisation die Anwendungen der Bereitstellungsgruppe verwenden können.

- (Wenn Anwendungsgruppen konfiguriert sind) Konfigurieren Sie die Benutzerliste der Anwendungsgruppe, sodass die Mitglieder der Verwaltung und Buchhaltung auf Anwendung A über L zugreifen können.
- Konfigurieren Sie die Eigenschaften von Anwendung A so, dass sie nur für Mitarbeiter der Debitorenbuchhaltung innerhalb der Finanzabteilung sichtbar ist.

Authentifizierte und nicht authentifizierte Benutzer

Es gibt zwei Benutzertypen: authentifizierte und nicht authentifizierte Benutzer (nicht authentifizierte Benutzer werden auch als "anonyme"Benutzer bezeichnet). Konfigurieren einen oder beide Typen in einer Bereitstellungsgruppe konfigurieren.

Authentifiziert Die Benutzer und Gruppenmitglieder, die Sie namentlich festlegen, müssen für den Zugriff auf Anwendungen und Desktops in StoreFront oder Citrix Receiver Anmeldeinformationen, z. B. Smartcard oder Benutzernamen und Kennwort, angeben. (Bei Bereitstellungsgruppen mit Desktopbetriebssystemmaschinen können Sie eine Liste der Benutzer später unter Bearbeiten der Bereitstellungsgruppe importieren.)

Nicht authentifiziert (anonym) Bei Bereitstellungsgruppen mit Serverbetriebssystemmaschinen können Sie Benutzern Zugriff auf Anwendungen und Desktops gewähren, ohne dass die Benutzer Anmeldeinformationen in StoreFront oder Citrix Receiver eingeben müssen. Beispiel: Beim Zugriff über einen Kiosk werden für die Anwendung Anmeldeinformationen benötigt, nicht aber für das Citrix Zugriffsportal und Citrix Tools. Eine Gruppe anonymer Benutzer wird erstellt, wenn Sie den ersten Delivery Controller installieren.

Damit nicht authentifizierten Benutzern Zugriff erteilt werden kann, muss auf jeder Maschine in der Bereitstellungsgruppe ein VDA für Windows-Serverbetriebssysteme (mindestens Version 7.6) installiert sein. Wenn nicht authentifizierte Benutzer aktiviert sind, müssen Sie einen StoreFront-Store ohne Authentifizierung haben.

Nicht authentifizierte Benutzerkonten werden bei Bedarf beim Start einer Sitzung erstellt und "AnonXYZ"genannt (XYZ ist eineindeutiger dreistelliger Wert).

Für Benutzersitzungen ohne Authentifizierung gilt ein Standardleerlauftimeout von 10 Minuten. Beim Trennen der Verbindung mit dem Client erfolgt automatisch die Abmeldung. Wiederverbindung, Roaming zwischen Clients und Workspace Control werden nicht unterstützt.

In der folgenden Tabelle werden die Optionen der Seite Benutzer erläutert:

Zugriff aktivieren für	Benutzer und Benutzergruppen hinzufügen/zuweisen?	Kontrollkästchen “Nicht authentifizierte Benutzer zulassen”aktivieren?
Nur authentifizierte Benutzer	Ja	Nein
Nur nicht authentifizierte Benutzer	Nein	Ja
Sowohl authentifizierte als auch nicht authentifizierte Benutzer	Ja	Ja

Step 5. Anwendungen

Nützliche Info:

- Sie können Remote-PC-Zugriff-Bereitstellungsgruppen keine Anwendungen hinzufügen.
- Standardmäßig werden neu hinzugefügte Anwendungen in einem Ordner mit dem Namen Applications abgelegt. Sie können einen anderen Ordner angeben. Weitere Informationen finden Sie im Artikel “Verwalten von Anwendungen”.
- Sie können die Eigenschaften von Anwendung beim Hinzufügen zu einer Bereitstellungsgruppe oder später ändern. Weitere Informationen finden Sie im Artikel “Verwalten von Anwendungen” .
- Wenn Sie eine Anwendung hinzufügen und es dort bereits eine Anwendung mit dem gleichen Namen gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie dies ablehnen, wird die Anwendung mit einem Suffix hinzugefügt, sodass ihr Name innerhalb des Ordners eindeutig ist.
- Wenn Sie eine Anwendung mehreren Bereitstellungsgruppen hinzufügen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Bereitstellungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Bereitstellungsgruppen, denen die Anwendung hinzugefügt wurde.
- Wenn Sie zwei Anwendungen mit dem gleichen Namen den gleichen Benutzern bereitstellen, ändern Sie in Studio die Eigenschaft Anwendungsname (Benutzer), sonst wird den Benutzern der Name in Receiver doppelt angezeigt.

Klicken Sie auf die Dropdownliste **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

- **Startmenü:** Anwendungen, die auf Maschinen erkannt werden, die von dem Masterimage im ausgewählten Katalog erstellt wurden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Wählen Sie die Anwendungen, die sie hinzufügen möchten und klicken Sie dann auf **OK**.

- **Manuell definiert:** Anwendungen in der Site oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Wenn Sie diese Informationen eingegeben haben, klicken Sie auf **OK**.
- **Vorhandene:** Anwendungen, die der Site bereits hinzugefügt wurden, ggf. in einer anderen Bereitstellungsgruppe. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Wählen Sie die Anwendungen, die sie hinzufügen möchten und klicken Sie dann auf **OK**.
- **App-V:** Anwendungen in App-V-Paketen. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, in der Sie den App-V-Server oder die Anwendungsbibliothek auswählen. Wählen Sie die Anwendungen, die Sie hinzufügen möchten, und klicken Sie dann auf **OK**. Weitere Informationen finden Sie im Artikel App-V.

Ist eine Anwendungsquelle oder Anwendung nicht verfügbar oder ungültig, wird sie nicht angezeigt oder kann nicht ausgewählt werden. Beispiel: Die Quelle **Vorhandene** ist nicht verfügbar, wenn der Site keine Anwendungen hinzugefügt wurden. Es kann auch sein, dass eine Anwendung nicht mit den auf Maschinen im ausgewählten Maschinenkatalog unterstützten Sitzungstypen kompatibel ist.

Schritt 6. Desktops (oder Desktopzuweisungsregeln)

Der Titel dieser Seite hängt davon ab, welchen Maschinenkatalog Sie zuvor im Assistenten ausgewählt haben:

- Wenn Sie einen Maschinenkatalog mit gepoolten Maschinen gewählt haben, lautet der Titel “Desktops”.
- Wenn Sie einen Maschinenkatalog mit zugewiesenen Maschinen gewählt und auf der Seite “Bereitstellungstyp”die Option “Desktops”gewählt haben, lautet der Titel “Desktopbenutzerzuweisungen”.
- Wenn Sie einen Maschinenkatalog mit zugewiesenen Maschinen gewählt und auf der Seite “Bereitstellungstyp”die Option “Anwendungen”gewählt haben, lautet der Titel “Anwendungsbenutzerzuweisungen”.

Klicken Sie auf **Hinzufügen**. Führen Sie folgende Aktionen im Dialogfeld aus:

- Geben Sie in den Feldern “Anzeigename”und “Beschreibung”die Informationen ein, die in Receiver angezeigt werden sollen.
- Zum Hinzufügen einer Tagbeschränkung zu einem Desktop wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag aus der Dropdownliste aus. (Weitere Informationen finden Sie im Artikel Tags.)

- Geben Sie über die Optionsfelder an, wer einen Desktop starten kann (bei Gruppen mit gepoolten Maschinen) bzw. wem eine Maschine zugewiesen werden soll, wenn er den Desktop startet (bei Gruppen mit zugewiesenen Maschinen). Es können entweder alle Benutzer mit Zugriff auf die Bereitstellungsgruppe oder bestimmte Benutzer und Benutzergruppen ausgewählt werden.
- Wenn die Gruppe zugewiesene Maschinen enthält, geben Sie die maximale Anzahl Desktops pro Benutzer an. Sie müssen eins oder einen höheren Wert eingeben.
- Aktivieren oder deaktivieren Sie den Desktop (bei gepoolten Maschinen) bzw. die Desktopzuordnungsregel (bei zugewiesenen Maschinen). Durch Deaktivieren eines Desktops wird dieser nicht mehr bereitgestellt, durch Deaktivieren einer Desktopzuordnungsregel wird die automatische Desktopzuweisung beendet.
- Wenn Sie fertig sind, klicken Sie auf **OK**.

Schritt 7. Zusammenfassung

Geben Sie einen Namen für die Bereitstellungsgruppe ein. Sie können optional eine Beschreibung eingeben, die in Receiver und Studio angezeigt wird.

Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**. Wenn Sie keine Anwendungen gewählt bzw. keinen Desktop zur Bereitstellung angeben haben, werden Sie gefragt, ob Sie fortfahren möchten.

Verwalten von Bereitstellungsgruppen

August 18, 2021

Einführung

In diesem Artikel werden die Schritte zum Verwalten von Bereitstellungsgruppen beschrieben. Sie können die Einstellungen ändern, die Sie beim Erstellen der Gruppe gewählt haben, und Sie können weitere Einstellungen konfigurieren, die beim Erstellen von Bereitstellungsgruppen nicht zur Verfügung stehen.

Informationen zum Verwalten von Anwendungen in Bereitstellungsgruppen, einschließlich Hinzufügen und Entfernen von Anwendungen in einer Bereitstellungsgruppe und Ändern der Anwendungseigenschaften finden Sie unter Anwendungen.

Das Verwalten von Bereitstellungsgruppen erfordert die Berechtigungen für delegierte Administration der integrierten Bereitstellungsgruppen-Administratorrolle. Weitere Informationen finden Sie unter

Delegierte Administration.

Ändern der Benutzereinstellungen für eine Bereitstellungsgruppe

Der Name dieser Seite lautet **Benutzereinstellungen** oder **Grundeinstellungen**.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Ändern Sie auf der Seite **Benutzereinstellungen** (bzw. **Grundeinstellungen**), die folgenden Optionen nach Bedarf.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Einstellung	Beschreibung
Beschreibung	Text in StoreFront, der Benutzern angezeigt wird
Bereitstellungsgruppe aktivieren	Zeigt an, ob die Bereitstellungsgruppe aktiviert ist.
Zeitzone	Stellt die Zeitzone ein.
Secure ICA aktivieren	Die gesamte Kommunikation zu und von Maschinen in der Bereitstellungsgruppe wird mit SecureICA, das das ICA-Protokoll verschlüsselt, geschützt. Die Standardebene ist 128-Bit. Die Ebene kann über das SDK geändert werden. Citrix empfiehlt die Verwendung zusätzlicher Verschlüsselungsmethoden, z. B. TLS-Verschlüsselung, wenn Datenübertragungen über öffentliche Netzwerke stattfinden. Bei SecureICA wird die Datenintegrität auch nicht geprüft.

Hinzufügen und Entfernen von Benutzern zu bzw. aus Bereitstellungsgruppen

Ausführliche Informationen zu Benutzern finden Sie im Abschnitt “Benutzer”des Artikels “Erstellen von Bereitstellungsgruppen”.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.

2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Zum Hinzufügen von Benutzern klicken Sie auf der Seite **Benutzer** auf **Hinzufügen** und geben Sie die Benutzer an, die Sie hinzufügen möchten. Zum Entfernen von Benutzern wählen Sie mindestens einen Benutzer aus und klicken Sie auf **Entfernen**. Sie können auch den Zugriff nicht authentifizierter Benutzer über das entsprechende Kontrollkästchen aktivieren oder deaktivieren.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Importieren und Exportieren von Benutzerlisten

Bei Bereitstellungsgruppen mit physischen Desktopbetriebssystemmaschinen können Sie Benutzerinformationen nach dem Erstellen der Bereitstellungsgruppe aus einer CSV-Datei importieren. Sie können Benutzerinformationen auch in eine CSV-Datei exportieren. Die CSV-Datei kann Daten aus einer vorherigen Produktversion enthalten.

Die erste Zeile der CSV-Datei muss durch Trennzeichen getrennte Spaltenüberschriften (in beliebiger Reihenfolge) enthalten, z. B. ADComputerAccount, AssignedUser, VirtualMachine und HostId. Die nachfolgenden Zeilen enthalten durch Trennzeichen getrennte Daten. Die Einträge unter ADComputerAccount können allgemeine Namen, IP-Adressen Distinguished Names oder Domänen-/Computernamenpaare sein.

Importieren oder Exportieren von Benutzerinformationen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Klicken Sie auf der Seite **Maschinenzuteilung** auf **Liste importieren** bzw. **Liste exportieren** und navigieren Sie zum Speicherort der Datei.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Ändern des Bereitstellungstyps von Bereitstellungsgruppen

Der Bereitstellungstyp bestimmt, was eine Gruppe bereitstellen kann: Anwendungen, Desktops oder beides.

Bevor Sie eine Bereitstellungsgruppe des Typs **Nur Anwendungen** oder **Desktops und Anwendungen** in eine Bereitstellungsgruppe des Typs **Nur Desktops** ändern, löschen Sie alle Anwendungen aus

der Bereitstellungsgruppe.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Bereitstellungstyp** den gewünschten Bereitstellungstyp.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Ändern der StoreFront-Adressen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **StoreFront** die StoreFront-URLs aus (bzw. fügen Sie sie hinzu), die von der auf jeder Maschine in der Bereitstellungsgruppe installierten Citrix Receiver-Instanz verwendet werden sollen.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Sie können die StoreFront-Serveradresse auch festlegen, indem Sie im Studio-Navigationsbereich **Konfiguration > StoreFront** auswählen.

Hinzufügen, Ändern oder Entfernen von Tagbeschränkungen für einen Desktop

Das Hinzufügen, Bearbeiten und Entfernen von Tagbeschränkungen kann unerwartete Auswirkungen darauf haben, welche Desktops für den Start in Betracht gezogen werden. Lesen Sie die Informationen und Hinweise unter Tags.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Desktops** den Desktop und klicken Sie auf **Bearbeiten**.
4. Zum Hinzufügen einer Tagbeschränkung wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag aus.
5. Zum Ändern oder Entfernen einer Tagbeschränkung wählen Sie ein anderes Tag oder entfernen Sie die Tagbeschränkung vollständig durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.

6. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Durchführen eines Upgrades einer Bereitstellungsgruppe und Rückgängigmachen eines Bereitstellungsgruppenupgrades

Nach dem Upgrade der VDAs auf Maschinen einer Bereitstellungsgruppe sowie auf den Maschinen in den von ihr verwendeten Maschinenkatalogen führen Sie ein Upgrade der Bereitstellungsgruppe durch.

Führen Sie vor dem Upgrade der Bereitstellungsgruppe folgende Schritte durch:

- Wenn Sie Provisioning Services verwenden, aktualisieren Sie die VDA-Version in der Provisioning Services Console.
- Starten Sie die Maschinen mit dem aktualisierten VDA, damit sie sich bei dem Delivery Controller registrieren können. Dadurch wird Studio darüber informiert, welche Elemente in der Bereitstellungsgruppe aktualisiert werden müssen.
- Wenn Sie ältere VDA-Versionen weiterverwenden müssen, sind neuere Produktfeatures ggf. nicht verfügbar. Weitere Informationen finden Sie in den Artikeln zu Upgrades.

Bereitstellungsgruppen aktualisieren:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Upgrade von Bereitstellungsgruppe durchführen**. Die Aktion **Upgrade von Bereitstellungsgruppe durchführen** wird nur angezeigt, wenn Studio aktualisierte VDAs erkennt.

Vor dem Starten des Upgrades wird in Studio gemeldet, welche Maschinen nicht aktualisiert werden können (falls es solche gibt) und warum. Sie können das Upgrade dann abbrechen, die Ursachen beheben und das Upgrade erneut starten.

Wenn das Upgrade abgeschlossen ist, können Sie Maschinen auf ihren vorherigen Zustand zurücksetzen, indem Sie die Bereitstellungsgruppe und dann im Aktionsbereich **Rückgängig machen** wählen.

Verwalten von Remote-PC-Zugriff-Bereitstellungsgruppen

Wenn eine Maschine eines Remote-PC-Zugriff-Maschinenkatalogs keinem Benutzer zugewiesen wurde, weist Studio sie vorübergehend einer Bereitstellungsgruppe zu, die dem Maschinenkatalog zugeordnet ist. Dadurch kann sie später einem Benutzer zugewiesen werden.

Die Zuweisung der Bereitstellungsgruppe zum Maschinenkatalog ist mit einem Prioritätswert verbunden. Die Priorität bestimmt, welcher Bereitstellungsgruppe eine Maschine zugewiesen ist, die bei der Registrierung beim System oder wenn ein Benutzer eine Maschinenzuweisung benötigt: je geringer der Wert, desto höher die Priorität. Wenn ein Remote-PC-Zugriff-Maschinenkatalog mehrere Bereitstellungsgruppenzuweisungen hat, wird die mit der höchsten Priorität vom System ausgewählt. Sie können die Priorität mit dem PowerShell-SDK festlegen.

Beim Erstellen eines Remote-PC-Zugriff-Maschinenkatalogs wird dieser einer Bereitstellungsgruppe zugeordnet. Dies bedeutet, dass dem Maschinenkatalog später hinzugefügte Maschinenkonten oder Organisationseinheiten in der Bereitstellungsgruppe hinzugefügt werden können. Die Zuordnung kann deaktiviert oder aktiviert werden.

Hinzufügen oder Entfernen der Zuordnung eines Remote-PC-Zugriff-Maschinenkatalogs zu einer Bereitstellungsgruppe

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Remote-PC-Zugriff-Gruppe aus.
3. Wählen Sie im Abschnitt "Details"die Registerkarte **Maschinenkataloge** und dann einen Katalog mit Remote-PC-Zugriff.
4. Um eine Zuordnung hinzuzufügen oder wiederherzustellen, wählen Sie **Desktops hinzufügen**. Zum Entfernen einer Zuordnung wählen Sie **Zuordnung entfernen**.

Herunterfahren und Neustarten von Maschinen in einer Bereitstellungsgruppe

Dieser Vorgang wird für Remote-PC-Zugriff-Maschinen nicht unterstützt.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie die Maschine und anschließend im Aktionsbereich eine der folgenden Optionen (einige Optionen sind je nach Maschinenzustand ggf. nicht verfügbar):

    - **Herunterfahren erzwingen**: Das Abschalten der Maschine wird erzwungen und die Liste der Maschinen wird aktualisiert.
    - **Neu starten:** Das Betriebssystem wird heruntergefahren und die Maschine dann neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt die Maschine im aktuellen Zustand.
    - **Neustart erzwingen.** Das Betriebssystem wird heruntergefahren und die Maschine dann neu gestartet.
    - **Anhalten.** Die Maschine wird angehalten, ohne sie herunterzufahren, und die Liste der Maschinen aktualisiert.
    - **Herunterfahren.** Das Betriebssystem wird heruntergefahren.

Wird bei Aktionen ohne Erzwingen eine Maschine nicht innerhalb von 10 Minuten heruntergefahren, wird sie ausgeschaltet. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

Citrix empfiehlt, dass Sie die Auswahl des Befehls **Herunterfahren** durch Benutzer bei Desktopbetriebssystemmaschinen während einer Sitzung nicht zulassen. Einzelheiten finden Sie in der Microsoft-Dokumentation zu Richtlinien.

Sie können auch Maschinen einer Verbindung herunterfahren und neu starten. Informationen dazu finden Sie im Artikel über Verbindungen und Ressourcen.

Energieverwaltung für Maschinen in einer Bereitstellungsgruppe

Die Energieverwaltung ist nur bei virtuellen Desktopbetriebssystemmaschinen, nicht aber bei physischen Maschinen (einschließlich Remote-PC-Zugriff-Maschinen) möglich. Desktopbetriebssystemmaschinen mit GPU-Funktionen können nicht angehalten werden, sodass Energieverwaltungsvorgänge fehlschlagen. Für Serverbetriebssystemmaschinen können Sie einen Neustartzeitplan erstellen. Das Verfahren wird im vorliegenden Abschnitt beschrieben.

In Bereitstellungsgruppen mit gepoolten Maschinen können virtuelle Desktopbetriebssystemmaschinen einen der folgenden Zustände annehmen:

- Zufällig zugewiesen und in Verwendung
- Nicht zugewiesen und nicht verbunden

In Bereitstellungsgruppen mit statischen Maschinen können virtuelle Desktopbetriebssystemmaschinen einen der folgenden Zustände aufweisen:

- Dauerhaft zugeordnet und in Verwendung
- Dauerhaft zugewiesen und nicht verbunden (aber bereit für Verbindungen)
- Nicht zugewiesen und nicht verbunden

Statische Bereitstellungsgruppen enthalten im Normalbetrieb sowohl dauerhaft zugewiesene als auch nicht zugewiesene Maschinen. Anfangs sind alle Maschinen nicht zugewiesen (außer beim Erstellen der Bereitstellungsgruppe manuell zugewiesene Maschinen). Wenn Benutzer eine Verbindung herstellen, werden Maschinen dauerhaft zugewiesen. Die Energieverwaltung ist bei nicht zugewiesenen Maschinen in den Bereitstellungsgruppen vollständig, bei dauerhaft zugewiesenen Maschinen nur teilweise möglich.

Pools und Puffer: Unter einem Pool versteht man bei gepoolten Bereitstellungsgruppen und statischen Bereitstellungsgruppen mit nicht zugewiesenen Maschinen eine Gruppe nicht zugewiesener (oder temporär zugewiesener) Maschinen, die eingeschaltet bleiben und mit denen Benutzer eine

Verbindung herstellen können (eine Maschine ist direkt nach der Anmeldung verfügbar). Die Poolgröße (d. h. die Zahl der Maschinen, die eingeschaltet bleiben) kann abhängig von der Tageszeit konfiguriert werden. Verwenden Sie zum Konfigurieren des Pools bei statischen Bereitstellungsgruppen das SDK.

Ein Puffer ist eine zusätzliche Gruppe nicht zugewiesener Maschinen, die eingeschaltet werden, wenn die Anzahl der Maschinen im Pool unter einen Schwellenwert (Prozentsatz der Größe der Bereitstellungsgruppe) fällt. Für große Bereitstellungsgruppen wird unter Umständen eine große Zahl Maschinen eingeschaltet, wenn der Schwellenwert unterschritten wird. Planen Sie die Größe Ihrer Bereitstellungsgruppen daher sorgfältig oder passen Sie die Standardpuffergröße mit dem SDK an.

Energiestatustimer: Sie können mit den Energiestatustimern Maschinen anhalten, wenn die Verbindung eine bestimmte Zeit lang getrennt war. Maschinen werden zum Beispiel automatisch außerhalb der Bürostunden angehalten, wenn die Verbindung mindestens 10 Minuten lang getrennt war. Zufällige Maschinen oder Maschinen mit persönlichen vDisks werden bei Abmeldung des Benutzers automatisch heruntergefahren, es sei denn, Sie konfigurieren die Bereitstellungsgruppeneigenschaft "ShutdownDesktopsAfterUse"im SDK.

Sie können Timer für Werktage und Wochenenden sowie für Spitzen- und Nebenzeiten konfigurieren.

Teilweise Energieverwaltung bei dauerhaft zugewiesenen Maschinen: Bei dauerhaft zugewiesenen Maschinen können Sie Energiestatustimer, aber keine Pools oder Puffer einrichten. Die Maschinen werden zu Beginn der Spitzenzeit eingeschaltet und zu Beginn der Nebenzeit ausgeschaltet. Es ist keine Feinsteuerung der Zahl der Maschinen möglich, die als Ausgleich für verwendete Maschinen verfügbar werden (im Gegensatz zu nicht zugeordneten Maschinen).

Einstellen der Energieverwaltung für Desktopbetriebssystemmaschinen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Energieverwaltung** im Dropdownmenü "Energieverwaltung für Maschinen"die Option **Werktage** aus. Wochentage umfassen standardmäßig die Tage von Montag bis Freitag.
4. Wählen Sie bei zufälligen Bereitstellungsgruppen unter **Maschinen einschalten** die Option **Bearbeiten** und geben Sie die Poolgröße während der Werktage an. Wählen Sie anschließend die Anzahl der einzuschaltenden Maschinen.
5. Legen Sie unter **Spitzenzeiten** die Zeiträume für Spitzen- und Nebenzeiten für jeden Tag fest.
6. Stellen Sie die Energiestatustimer für Spitzen- und Nebenzeiten an Werktagen ein: Geben Sie für **Während Spitzenzeiten > Wenn getrennt** die Verzögerung in Minuten ein, nach der getrennte Maschinen in der Bereitstellungsgruppe angehalten werden sollen, und klicken Sie auf "Anhalten". Geben Sie für **Während Nicht-Spitzenzeiten > Wenn getrennt** die Verzögerung in

Minuten ein, nach der abgemeldete Maschinen in der Bereitstellungsgruppe heruntergefahren werden, und klicken Sie auf **Herunterfahren**. Dieser Timer ist für Bereitstellungsgruppen mit zufälligen Maschinen nicht verfügbar.

7. Wählen Sie im Dropdownmenü "Energieverwaltung für Maschinen"die Option **Wochenende** aus und konfigurieren Sie die Spitzenzeiten und Energiestatustimer für Wochenenden.
8. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Verwenden Sie das SDK für Folgendes:

- Herunterfahren anstelle von Anhalten von Maschinen basierend auf Energiestatustimern, oder wenn Timer auf Abmeldungen anstatt von Verbindungstrennungen reagieren sollen
- Ändern der Standardeinstellungen für Werktage und Wochenende
- Informationen zum Deaktivieren der Energieverwaltung finden Sie unter CTX217289.

Erstellen eines Neustartzeitplans für Maschinen in einer Bereitstellungsgruppe

In diesem Abschnitt wird beschrieben, wie Sie einen einzelnen Neustartzeitplan in Studio konfigurieren. Sie können mit PowerShell auch mehrere Neustartzeitpläne für verschiedene Teilmengen von Maschinen in einer Bereitstellungsgruppe konfigurieren. Weitere Informationen finden Sie im nächsten Abschnitt.

Über einen Neustartzeitplan wird der regelmäßige Neustart aller Maschinen in einer Bereitstellungsgruppe festgelegt.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wenn Sie nicht möchten, dass die Maschinen in der Bereitstellungsgruppe automatisch neu gestartet werden, wählen Sie auf der Seite **Neustartzeitplan** das Optionsfeld **Nein** und fahren Sie mit dem letzten Schritt dieses Verfahrens fort. Es wird kein Neustartzeitplan bzw. keine Rolloutstrategie konfiguriert. Wenn Sie zuvor einen Zeitplan konfiguriert hatten, wird er durch diese Auswahl aufgehoben.
4. Sollen die Maschinen in der Bereitstellungsgruppe automatisch neu gestartet werden, wählen Sie das Optionsfeld **Ja**.
5. Wählen Sie für **Neustartintervall** die Option **Täglich** oder den Wochentag, an dem der Neustart durchgeführt werden soll.
6. Wählen Sie für **Neustart beginnen um** die Tageszeit, zu der der Neustart beginnen soll.
7. Wählen Sie unter **Neustartdauer** aus, dass alle Maschinen gleichzeitig gestartet werden sollen, oder geben Sie die Gesamtdauer für den Beginn der Neustarts an. Ein interner Algorithmus bestimmt, wann welche Maschine während dieses Zeitraums neu gestartet wird.

8. Wählen Sie in der Dropdownliste **Benachrichtigung** aus, ob auf den betroffenen Maschinen eine Meldung angezeigt werden soll, bevor der Neustart beginnt. In der Standardeinstellung wird keine Meldung angezeigt. Wenn Sie festlegen, dass 15 Minuten vor dem Neustart eine Meldung angezeigt wird, können Sie in der Dropdownliste **Benachrichtigung erneut senden** vorgeben, dass die Meldung alle fünf Minuten nach Erstanzeige wiederholt werden soll. Standardmäßig wird die Meldung nicht wiederholt angezeigt.
9. Geben Sie im Feld **Benachrichtigung** den Text der Meldung ein (es gibt keinen Standardtext). Wenn die Meldung die Zeit in Minuten bis zum Neustart enthalten soll, verwenden Sie die Variable **%m%**. Beispiel: *Warnung: Ihr Computer wird in %m% Minuten automatisch neu gestartet.*Wenn Sie die Benachrichtigung wiederholen lassen und die Variable "%m%"verwenden, wird die Zeitangabe bei jeder Wiederholung um fünf Minuten verringert. Sofern Sie keinen gleichzeitigen Neustart aller Maschinen festgelegt haben, wird die Meldung auf jeder Maschine in der Bereitstellungsgruppe zu der von dem internen Algorithmus berechneten Zeit angezeigt.
10. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Sie können kein automatisiertes Einschalten oder Herunterfahren über Studio durchführen, sondern nur Neustarts.

Erstellen mehrerer Neustartzeitpläne für Maschinen in einer Bereitstellungsgruppe

Sie können mit PowerShell-Cmdlets mehrere Neustartzeitpläne für Maschinen in einer Bereitstellungsgruppe erstellen. Jeder Zeitplan kann für Maschinen mit einem bestimmten Tag konfiguriert werden. Mit der Tagbeschränkung können Sie problemlos unterschiedliche Neustartzeitpläne für verschiedene Maschinenteilmengen in einer Bereitstellungsgruppe erstellen.

Angenommen, Sie verwenden eine Bereitstellungsgruppe für alle Maschinen im Unternehmen. Sie neu starten möchten, auf jedem Computer mindestens einmal wöchentlich (sonntagnachts), aber die Maschinen für die Buchhaltungsteams täglich neu gestartet werden sollen. Sie können einen wöchentlichen Zeitplan für alle Maschinen und einen täglichen Zeitplan für die Maschinen des Buchhaltungsteams festlegen.

Zeitplanüberlagerungen:

Mehrere Zeitpläne können einander überlagern. Im obigen Beispiel gelten für die Maschinen der Buchhaltung beide Zeitpläne, sie werden möglicherweise an Sonntagen zweimal neu gestartet.

Der Zeitplancode ist darauf ausgelegt, unnötige Neustarts zu vermeiden, es besteht jedoch keine Garantie, dass dies immer vermieden wird. Wenn Start- und Dauer beider Zeitpläne genau übereinstimmen, ist es wahrscheinlicher, dass die Maschinen nur einmal neu gestartet werden. Je stärker sich die Zeitpläne unterscheiden, umso wahrscheinlicher wird das Auftreten zweier Neustarts. Auch

die Zahl der von einem Zeitplan betroffenen Maschinen wirkt sich auf die Möglichkeit einer Überlagerung aus. In dem hier aufgeführten Beispiel kann der wöchentliche Zeitplan für den Neustart aller Maschinen Neustarts wesentlich schneller auslösen, als der tägliche Zeitplan (je nach der jeweils konfigurierten Dauer).

Anforderungen:

Das Erstellen mehrerer Neustartzeitpläne in Kombination mit Tagbeschränkungen ist zurzeit nur über die PowerShell-Befehlszeile mit RebootScheduleV2-PowerShell-Cmdlets möglich, die mit XenApp und XenDesktop 7.12 neu eingeführt wurden. Diese werden im vorliegenden Artikel als "V2-Cmdlets" bezeichnet.

Die Verwendung der V2-Cmdlets erfordert Folgendes:

- Delivery Controller-Version 7.12 (Minimum)
  - Wenn Sie das aktuelle SDK-Plug-In mit einem Controller vor Version 7.12 verwenden, funktionieren neue Zeitpläne nicht wie erwartet.
  - In einer gemischten Site (in der einige, aber nicht alle Controller aktualisiert wurden) funktionieren die V2-Cmdlets erst, wenn ein Upgrade der Datenbank und mindestens eines Controllers durchgeführt wurde und dieser Controller (durch Festlegen des Parameters –adminaddress <Controller> über die V2-Cmdlets) verwendet wird.
  - Bewährte Methode: Erstellen Sie keinen neuen Zeitplan, bis alle Controller der Site aktualisiert sind.
- Mit XenApp und XenDesktop 7.12 geliefertes PowerShell-SDK-Snap-In (Minimum). Nach der Installation bzw. dem Upgrade der Komponenten und der Site führen Sie asnp Citrix.* aus, um die neuesten Cmdlets zu laden.

Studio verwendet zurzeit die älteren V1-RebootSchedule-PowerShell-Cmdlets und zeigt keine mit den V2-Cmdlets erstellten Zeitpläne an.

Wenn Sie einen Neustartzeitplan mit einer Tagbeschränkung erstellen und die Tagbeschränkung später mit Studio während eines Neustartzyklus von einer Maschine entfernen oder weiteren Maschinen hinzufügen, treten diese Änderungen erst beim Start des nächsten Neustartzyklus in Kraft. (Die Änderungen haben also keine Auswirkungen auf den aktuellen Neustartzyklus.)

PowerShell-Cmdlets:

Verwenden Sie die folgenden RebootScheduleV2-Cmdlets über die Befehlszeile zum Erstellen mehrerer Zeitpläne unter Verwendung von Tagbeschränkungen.

- New-BrokerRebootScheduleV2 (ersetzt New-BrokerRebootSchedule)
- Get-BrokerRebootScheduleV2 (ersetzt Get-BrokerRebootSchedule)
- Set- BrokerRebootScheduleV2 (ersetzt Set-BrokerRebootSchedule)
- Remove-BrokerRebootScheduleV2 (ersetzt Remove-BrokerRebootSchedule)

- Rename-BrokerRebootScheduleV2 (neu, keine Ersetzung)

Zum Aufrufen der Hilfe zu Syntax und Parametern der Cmdlets geben Sie **Get-Help** –**full** <*cmdlet-name*> ein.

Hinweis zur Terminologie: Im PowerShell-SDK gibt der Parameter "DesktopGroup"die Bereitstellungsgruppe an.

Alle Parameter der Studio-Schnittstelle zum Erstellen eines Neustartzeitplans stehen beim Erstellen und Aktualisieren von Zeitplänen mit den V2-Cmdlets auch zur Verfügung. Darüber hinaus ist Folgendes möglich:

- Einschränken des Zeitplans auf Maschinen mit einem bestimmten Tag
- Angeben eines Intervalls vor dem Senden der ersten Warnung, während dessen keine neuen Sitzungen an die betroffenen Maschinen vermittelt werden

Konfiguration:

Wenn Sie einen Neustartzeitplan mit einer Tagbeschränkung konfigurieren, müssen Sie das Tag den Maschinen hinzufügen, auf die der Zeitplan angewendet werden soll. (Weitere Informationen finden Sie unter Tags.)

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie die Bereitstellungsgruppe mit den Maschinen, für die Sie den Zeitplan erstellen möchten.
3. Klicken Sie auf "Maschinen anzeigen"und wählen Sie die Maschinen, denen Sie das Tag hinzufügen möchten.
4. Wählen Sie im Aktionsbereich **Tags verwalten**.
5. Wenn das Tag bereits vorhanden ist, aktivieren Sie das Kontrollkästchen neben dem Tagnamen. Ist das Tag noch nicht vorhanden, klicken Sie auf **Erstellen** und geben Sie einen Namen für das Tag ein. Aktivieren Sie nach dem Erstellen des Tags das Kontrollkästchen neben dessen Namen.
6. Klicken Sie im Dialogfeld "Tags verwalten"auf **Speichern**.

Nach dem Erstellen und Hinzufügen von Tags verwenden Sie beim Erstellen bzw. Bearbeiten eines Zeitplans mit dem V2-Cmdlet den Parameter –RestrictToTag zum Angeben des Tags.

Zeitpläne aus älteren XenApp- oder XenDesktop-Versionen:

In Studio werden zurzeit die V1-RebootSchedule-Cmdlets verwendet. Wenn Sie einen Neustartzeitplan vor dem Upgrade auf Version 7.12 (Minimum) erstellt haben, können Sie ihn in Studio weiterhin mit V1-Cmdlets verwalten. Allerdings können Sie ihm mit Studio keine Tagbeschränkung hinzufügen und auch keine weiteren Zeitpläne mit Studio erstellen, da Studio die V2-Cmdlets nicht unterstützt. Wenn Sie für Ihren vorhandenen Zeitplan die V1-Cmdlets verwenden, werden in Studio die richtigen Informationen zu diesem angezeigt.

Alternativ können Sie den vorhandenen Zeitplan über die Befehlszeile mit den neuen V2-RebootSchedule-Cmdlets bearbeiten. Mit den neuen V2-Cmdlets können Sie für einen solchen Zeitplan die Tagbeschränkungs-Parameter verwenden und auch weitere Neustartzeitpläne erstellen. Allerdings werden in Studio nach dem Ändern eines Zeitplans mit V2-Cmdlets nicht mehr die vollständigen Informationen angezeigt, da Studio nur V1-Informationen erkennt. Sie können weder Namen und Beschreibung des Zeitplans sehen, noch ob eine Tagbeschränkung verwendet wird.

```
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
New-BrokerRebootScheduleV2 (replaces New-BrokerRebootSchedule)
Get-BrokerRebootScheduleV2 (replaces Get-BrokerRebootSchedule)
Set- BrokerRebootScheduleV2 (replaces Set-BrokerRebootSchedule)
Remove-BrokerRebootScheduleV2 (replaces Remove-BrokerRebootSchedule)
Rename-BrokerRebootScheduleV2 (new; not a replacement)
```

Unterbinden der Benutzerverbindung mit Maschinen (Wartungsmodus) in einer Bereitstellungsgruppe

Wenn Sie vorübergehend verhindern möchten, dass neue Verbindungen mit Maschinen hergestellt werden, können Sie den Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe aktivieren. Das ist beispielsweise vor dem Anwenden von Patches oder der Verwendung von Verwaltungstools nützlich.

- Wenn sich eine Serverbetriebssystemmaschine im Wartungsmodus befindet, können Benutzer eine Verbindung mit vorhandenen Sitzungen herstellen, aber keine neuen Sitzungen starten.
- Bei einer Desktopbetriebssystemmaschine (oder einem Computer mit Remote-PC-Zugriff) im Wartungsmodus können Benutzer keine Verbindung herstellen. Aktuelle Verbindungen bleiben bis zur Trennung oder Abmeldung erhalten.

Wartungsmodus ein- oder ausschalten:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe aus.
3. Zum Aktivieren des Wartungsmodus für alle Maschinen in der Bereitstellungsgruppe wählen Sie im Aktionsbereich **Wartungsmodus einschalten**. Zum Aktivieren des Wartungsmodus für einzelne Maschinen wählen Sie im Aktionsbereich **Maschinen anzeigen**. Wählen Sie eine Maschine aus und wählen Sie dann im Aktionsbereich **Wartungsmodus einschalten**.

4. Zum Deaktivieren des Wartungsmodus für eine oder alle Maschinen in einer Bereitstellungsgruppe folgen Sie den Anweisungen oben unter Auswahl der Option **Wartungsmodus ausschalten** im Aktionsbereich.

Einstellungen für Windows-Remotedesktopverbindungen wirken sich auch darauf aus, ob eine Serverbetriebssystemmaschine im Wartungsmodus ist. Der Wartungsmodus ist in folgenden Fällen aktiviert:

- Der Wartungsmodus wurde wie oben beschrieben aktiviert.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt.
- Die Remotedesktopverbindung wurde auf **Keine Verbindung mit diesem Computer zulassen** festgelegt und für den Anmeldemodus der Remotehostkonfiguration wurde **Neue Verbindungen zulassen, doch neue Anmeldungen verhindern** oder **Neue Verbindungen zulassen, doch Neuanmeldungen bis zum Neustart des Servers verweigern** gewählt.

Sie können auch den Wartungsmodus für eine Verbindung ein- und ausschalten, was sich auf die Maschine auswirkt, die die Verbindung verwendet, oder für einen Maschinenkatalog, was sich auf alle Maschinen in diesem auswirkt.

Ändern der Maschinen-Benutzer-Zuweisung in einer Bereitstellungsgruppe

Sie können die Zuweisungen von Desktopbetriebssystemmaschinen, nicht aber die von Serverbetriebssystemmaschinen oder Maschinen, die mit Provisioning Services erstellt wurden, ändern.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe aus.
3. Wählen Sie dann im Bereich Aktion die Option **Bereitstellungsgruppe bearbeiten** aus. Geben Sie die neuen Benutzer auf der Seite **Desktops** oder **Desktopzuweisungsregeln** an (abhängig vom Typ des Maschinenkatalogs, den die Bereitstellungsgruppe verwendet, ist nur eine dieser Seiten verfügbar).
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Ändern der maximalen Anzahl Maschinen pro Benutzer

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.

3. Legen Sie auf der Seite **Desktopzuweisungsregeln** einen Wert für "Maximale Desktops pro Benutzer"fest.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Lastverwaltung von Maschinen in Bereitstellungsgruppen

Die Lastverwaltung ist nur bei Serverbetriebssystemmaschinen möglich.

Bei der Lastverwaltung wird die Serverlast gemessen und festgelegt, welcher Server unter den aktuellen Umgebungsbedingungen auszuwählen ist. Diese Auswahl basiert auf folgenden Faktoren:

Wartungsmodusstatus des Servers: Eine Serverbetriebssystemmaschine wird nur für den Lastausgleich berücksichtigt, wenn der Wartungsmodus für sie deaktiviert ist.

Serverlastindex: bestimmt, mit welcher Wahrscheinlichkeit ein Server, der Serverbetriebssystemmaschinen bereitstellt, Verbindungen erhält. Der Index basiert auf einer Kombination von Lastauswertungskriterien: Anzahl der Sitzungen sowie Einstellungen für Leistungswerte (z. B. CPU-, Datenträger- und Speichernutzung). Die die Lastauswertungskriterien werden in den Richtlinieneinstellungen für die Lastverwaltung festgelegt.

Sie können den Lastindex in Director, über die Suche in Studio und im SDK überwachen.

In Studio ist die Spalte "Lastindex"standardmäßig ausgeblendet. Zum Anzeigen der Spalte wählen Sie eine Maschine und dann mit der rechten Maustaste eine Spaltenüberschrift und wählen Sie dann Spalte auswählen. Wählen Sie in der Kategorie Maschine die Option Lastindex.

Verwenden Sie im SDK das Cmdlet "Get-BrokerMachine". Weitere Informationen finden Sie unter CTX202150.

Ein Serverlastindex von 10.000 bedeutet, dass der Server voll ausgelastet ist. Wenn keine anderen Server verfügbar sind, erhalten die Benutzer beim Starten einer Sitzung u. U. eine Meldung, dass der Desktop oder die Anwendung zurzeit nicht verfügbar ist.

Richtlinieneinstellung "Toleranzwert für gleichzeitige Anmeldungen": maximale Anzahl gleichzeitiger Serveranmeldeanforderungen. (Diese Einstellung entspricht der Lastdrosselung in XenApp-Versionen vor 7.5.)

Wenn alle Server den Toleranzwert für gleichzeitige Anmeldungen erreichen oder überschreiten, wird die nächste Anmeldeanforderung dem Server mit der niedrigsten Anzahl ausstehender Anmeldungen zugewiesen. Wenn mehrere Server diese Kriterien erfüllen, wird der Server mit dem niedrigsten Lastindex ausgewählt.

Entfernen von Maschinen aus Bereitstellungsgruppen

Beim Entfernen einer Maschine wird diese aus der Bereitstellungsgruppe gelöscht, jedoch nicht aus dem Maschinenkatalog, den die Bereitstellungsgruppe verwendet. Die Maschine steht daher für Zuweisungen zu anderen Bereitstellungsgruppen zur Verfügung.

Maschinen müssen heruntergefahren werden, bevor sie entfernt werden können. Wenn Sie vorübergehend verhindern möchten, dass Benutzer eine Verbindung mit der Maschine herstellen, während Sie sie löschen, setzen Sie die Maschine in den Wartungsmodus, bevor Sie sie herunterfahren.

Wenn Sie eine Maschine einem anderen Benutzer zuweisen, denken Sie daran, dass Maschinen persönliche Daten enthalten können. Es empfiehlt sich ggf. ein Reimaging der Maschine.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und wählen Sie dann im Aktionsbereich **Maschinen anzeigen**.
3. Stellen Sie sicher, dass die Maschine heruntergefahren ist.
4. Wählen Sie im Aktionsbereich **Aus Bereitstellungsgruppe entfernen**.

Sie können eine Maschine auch über die von der Maschine verwendete Verbindung aus einer Bereitstellungsgruppe entfernen. Weitere Informationen finden Sie unter Verbindungen und Ressourcen.

Einschränken des Zugriffs auf Maschinen einer Bereitstellungsgruppe

Alle Änderungen zum Einschränken des Zugriffs auf Maschinen in einer Bereitstellungsgruppe haben Vorrang vor zuvor durchgeführten Einstellungen, unabhängig von der verwendeten Methode. Sie haben folgende Möglichkeiten:

Einschränken des Zugriffs für Administratoren über Geltungsbereiche für die delegierte Administration. Sie können einen Geltungsbereich erstellen und zuweisen, in dem Administratoren auf alle Anwendungen zugreifen können, und einen zweiten Geltungsbereich, der nur den Zugriff auf spezifische Anwendungen zulässt. Weitere Informationen finden Sie im Artikel “Delegierte Administration” .

Einschränken des Zugriffs für Benutzer über SmartAccess-Richtlinienausdrücke, mit denen über NetScaler Gateway hergestellte Benutzerverbindungen gefiltert werden.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Wählen Sie auf der Seite **Zugriffsrichtlinie** die Option **Über NetScaler Gateway hergestellte Verbindungen** aus.

4. Wenn Sie nur einen Teil dieser Verbindungen auswählen möchten, wählen Sie **Verbindungen, auf die mindestens einer der folgenden Filter zutrifft**. Legen Sie dann die NetScaler Gateway-Site fest und fügen Sie SmartAccess-Richtlinienausdrücke für zulässige Benutzerzugriffsszenarios hinzu, bzw. bearbeiten oder löschen Sie diese. Weitere Informationen finden Sie in der Dokumentation zu NetScaler Gateway.
5. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Einschränken des Zugriffs für Benutzer über Ausschlussfilter für mit dem SDK festgelegte Zugriffsrichtlinien. Zugriffsrichtlinien werden auf Bereitstellungsgruppen angewendet, um Verbindungen genauer zu definieren. Sie können beispielsweise den Maschinenzugriff für eine Untergruppe von Benutzern einschränken und zulässige Benutzergeräte festlegen. Mit Ausschlussfiltern können Zugriffsrichtlinien weiter angepasst werden. Aus Sicherheitsgründen können Sie beispielsweise den Zugriff für eine Untergruppe der Benutzer oder Geräte verweigern. Ausschlussfilter sind in der Standardeinstellung deaktiviert.

Wenn Sie beispielsweise den Zugriff von einem Lernlabor im Subnetz des Unternehmensnetzwerks auf eine spezifische Bereitstellungsgruppe verhindern möchten, unabhängig davon, wer die Maschinen im Labor nutzt, verwenden Sie folgenden Befehl: **Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -**.

Sie können das Sternchen (*) als Platzhalter für alle Tags, die mit dem gleichen Richtlinienausdruck beginnen, verwenden. Wenn Sie beispielsweise auf einer Maschine das Tag "VPDesktops_Direct" hinzufügen und auf einer anderen das Tag "VPDesktops_Test", wird der Filter durch Festlegen des Tags auf "VPDesktops_*"im Skript "Set-BrokerAccessPolicy"auf beide Maschinen angewendet.

Wenn Sie über einem Webbrowser verbunden sind oder die einheitlichen Citrix Receiver-Benutzeroberfläche im Store aktiviert ist, können Sie keinen Ausschlussfilter auf Basis des Clientnamens verwenden.

Aktualisieren einer Maschine in einer Bereitstellungsgruppe

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Gruppe und dann im Aktionsbereich **Maschinen anzeigen**.
3. Wählen Sie eine Maschine und dann im Aktionsbereich **Maschinen aktualisieren**.

Zum Auswählen eines anderen Masterimages wählen Sie **Masterimage** und dann einen Snapshot.

Zum Anwenden der Änderungen und Benachrichtigen der Benutzer der Maschine wählen Sie **Rolloutbenachrichtigung für Endbenutzer**. Legen Sie anschließend Folgendes fest: ob die Aktualisierung des Masterimages sofort oder beim nächsten Neustart erfolgen soll, die Neustartverteilung

(Gesamtzeit des Beginns der Aktualisierung aller Maschinen in der Gruppe) und ob Benutzer über den Neustart benachrichtigt werden sollen sowie die entsprechende Meldung.

Abmelden oder Trennen einer Sitzung

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und wählen Sie dann im **Aktionsbereich** die Option **Maschinen** anzeigen.
3. Wählen Sie im mittleren Bereich die Maschine aus und wählen Sie im **Aktionsbereich** die Option **Sitzungen anzeigen** und anschließend eine Sitzung.
    - Alternativ können Sie im mittleren Bereich die Registerkarte **Sitzung** und dann eine Sitzung auswählen.
4. Zum Abmelden eines Benutzers von einer Sitzung wählen Sie im **Aktionsbereich** die Option **Abmelden**. Die Sitzung wird geschlossen und der Benutzer abgemeldet. Die Maschine steht nun anderen Benutzern zur Verfügung, sofern sie nicht einem bestimmten Benutzer zugewiesen ist.
5. Zum Trennen einer Sitzung wählen Sie im **Aktionsbereich** die Option **Trennen**. Anwendungen werden in der Sitzung weiter ausgeführt und die Maschine bleibt dem Benutzer zugewiesen. Der Benutzer kann eine Verbindung mit derselben Maschine wiederherstellen.

Sie können die Energiestatustimer für Desktopbetriebssystemmaschinen so konfigurieren, dass nicht genutzte Sitzungen automatisch verarbeitet werden. Einzelheiten finden Sie unter "Energieverwaltung für Maschinen".

Senden einer Nachricht an eine Bereitstellungsgruppe

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und wählen Sie dann im **Aktionsbereich** die Option **Maschinen** anzeigen.
3. Wählen Sie im mittleren Bereich die Maschine, an die Sie eine Nachricht senden möchten.
4. Wählen Sie im **Aktionsbereich** die Option **Sitzungen anzeigen**.
5. Wählen Sie im mittleren Bereich alle Sitzungen aus und wählen Sie im **Aktionsbereich** die Option **Nachricht senden**.
6. Geben Sie die Nachricht ein und klicken Sie auf **OK**. Sie können bei Bedarf einen Schweregrad angeben. Zur Auswahl stehen **Kritisch**, **Frage**, **Warnung** und **Informationen**.

Alternativ können Sie eine Nachricht über Citrix Director senden. Weitere Informationen finden Sie unter Senden von Nachrichten an Benutzer.

Konfigurieren des Vorabstarts und des Fortbestehens von Sitzungen in einer Bereitstellungsgruppe

Diese Features werden nur auf Serverbetriebssystemmaschinen unterstützt.

Vorabstart und Fortbestehen von Sitzungen ermöglichen einen schnellen Zugriff durch Benutzer auf Anwendungen, indem Sitzungen gestartet werden, bevor sie angefordert werden, und aktiv bleiben, nachdem ein Benutzer alle Anwendungen geschlossen hat.

In der Standardeinstellung werden diese Features nicht verwendet, d. h. eine Sitzung startet, wenn ein Benutzer eine Anwendung startet, und bleibt so lange aktiv, bis die letzte Anwendung der Sitzung geschlossen wird.

Überlegungen:

- Die Bereitstellungsgruppe muss Anwendungen unterstützen und auf den Maschinen muss ein VDA für Windows-Serverbetriebssysteme in mindestens Version 7.6 ausgeführt werden.
- Diese Features werden nur bei Verwendung von Citrix Receiver für Windows unterstützt, sie erfordern außerdem zusätzliche Citrix Receiver-Konfigurationsschritte. Anweisungen hierzu finden Sie in der Produktdokumentation zu Ihrer Citrix Receiver für Windows-Version. Suchen Sie dort nach"Sitzungsvorabstart".
- Citrix Receiver für HTML5 wird nicht unterstützt.
- Wird ein Computer in den Modus "Anhalten"oder in den Ruhezustand versetzt, funktioniert der Sitzungsvorabstart unabhängig von den Vorabstarteinstellungen nicht. Die Benutzer können den Computer bzw. die Sitzung sperren, wenn sie sich jedoch von Citrix Receiver abmelden, wird die Sitzung beendet und ein Vorabstart ist nicht mehr möglich.
- Wird der Sitzungsvorabstart verwendet, können die Energieverwaltungsfunktionen "Anhalten" und "Ruhezustand"auf physischen Clientcomputern nicht verwendet werden. Clientmaschinenbenutzer können ihre Sitzungen sperren, sollten sich aber nicht abmelden.
- Vorab gestartete und fortbestehende Sitzungen verbrauchen eine Lizenz, jedoch nur wenn sie verbunden sind. Nicht genutzte vorab gestartete und fortbestehende Sitzungen werden standardmäßig nach 15 Minuten getrennt. Dieser Wert kann über das PowerShell-Cmdlet "New/Set-BrokerSessionPreLaunch"konfiguriert werden.
- Eine sorgfältige Planung und Überwachung der Aktivitätsmuster von Benutzern ist wichtig, damit diese Features so eingerichtet werden können, dass sie einander ergänzen. In einer optimalen Konfiguration besteht ein Gleichgewicht zwischen dem Vorteil einer schnelleren Anwendungsverfügbarkeit für Benutzer und den durch den Verbrauch von Lizenzen und die fortdauernde Zuteilung von Ressourcen entstehenden Kosten.
- Sie können den Vorabstart von Sitzungen auch für eine spezifische Uhrzeit in Citrix Receiver konfigurieren.

Dauer des Aktivbleibens nicht genutzter vorab gestarteter und fortbestehender Sitzungen

Wie lange eine nicht genutzte Sitzung aktiv bleibt, wenn der Benutzer keine Anwendung startet, kann über ein Timeout oder über Serverlast-Schwellenwerte angegeben werden. Sie können alle Parameter konfigurieren und die Sitzung wird jeweils durch das zuerst auftretende Ereignis beendet.

- **Timeout:** Ein konfiguriertes Timeout gibt die Anzahl der Minuten, Stunden oder Tage an, die eine nicht genutzte, vorab gestartete oder fortbestehende Sitzung aktiv bleibt. Wenn Sie ein zu kurzes Timeout konfigurieren, werden vorab gestartete Sitzungen beendet, bevor der Benutzer in den Genuss des schnelleren Anwendungszugriffs kommt. Ist das Timeout zu lang, werden eingehende Benutzerverbindungen möglicherweise abgewiesen, da der Server nicht genügend Ressourcen hat.

  Sie können dieses Timeout über das SDK (Cmdlet `New`/`Set-BrokerSessionPreLaunch`), nicht aber über Studio deaktivieren. Wenn Sie das Timeout deaktivieren, wird es für die betreffende Bereitstellungsgruppe in Studio und auf den Seiten zum **Bearbeiten von Bereitstellungsgruppen** nicht angezeigt.

- **Schwellenwerte:** Das automatische Beenden vorab gestarteter und fortbestehender Sitzungen auf der Basis der Serverlast gewährleistet, dass Sitzungen so lange wie möglich geöffnet bleiben (vorausgesetzt, es sind Serverressourcen verfügbar). Nicht genutzte vorab gestartete und fortbestehende Sitzungen verursachen keine Abweisung von Verbindungen, da sie automatisch beendet werden, wenn Ressourcen für neue Benutzersitzungen benötigt werden.

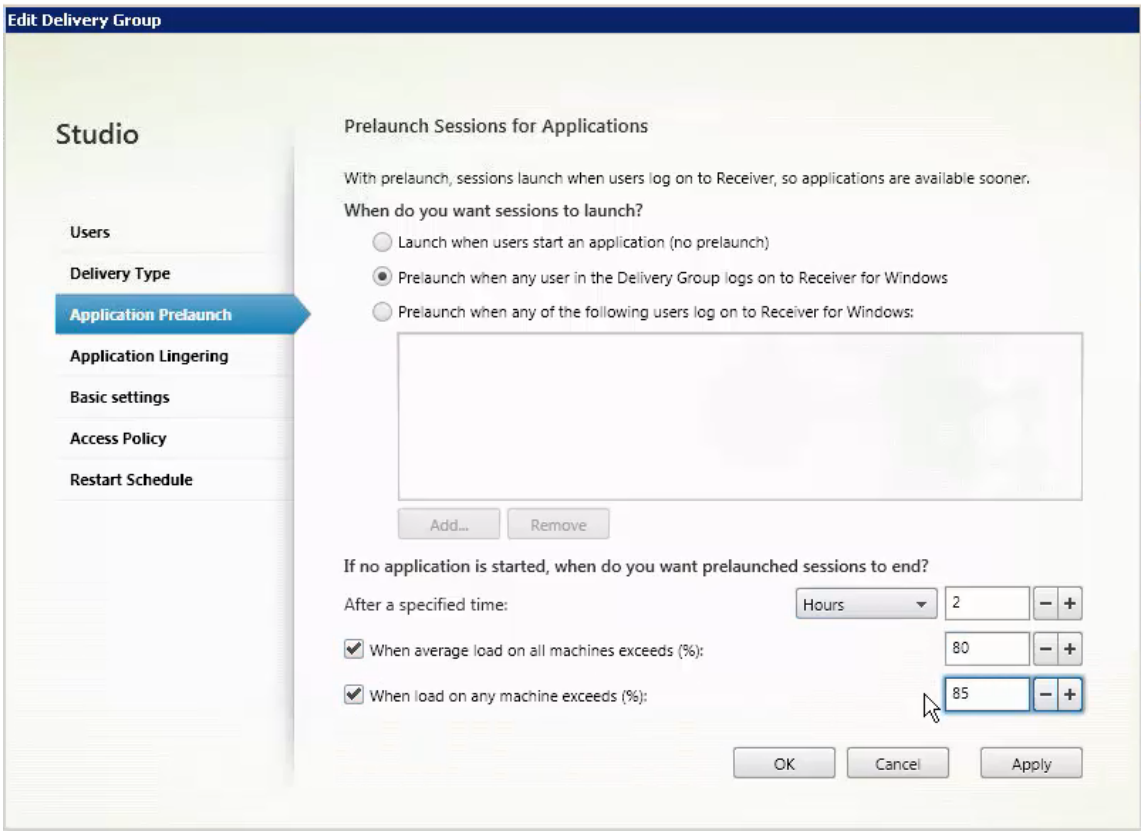
  Sie können zwei Schwellenwerte konfigurieren: die durchschnittliche Last aller Server der Bereitstellungsgruppe und die höchste Last eines Servers in der Bereitstellungsgruppe (beides in Prozent). Wird ein Schwellenwert überschritten, werden jeweils die Sitzungen beendet, die sich am längsten im Zustand “vorab gestartet”bzw. “fortbestehend”befinden. Das Beenden erfolgt einzeln im Minutentakt bis die Last unter den Schwellenwert fällt. (Solange der Schwellenwert überschritten ist, werden keine neuen Sitzungen vorab gestartet.)

Server mit VDAs, die nicht beim Controller registriert sind, und Server im Wartungsmodus gelten als voll ausgelastet. Bei einem ungeplanten Ausfall werden vorab gestartete und fortbestehende Sitzungen automatisch beendet, um Kapazität freizugeben.

Aktivieren des Vorabstarts von Sitzungen

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie den Vorabstart von Sitzungen, indem Sie auf der Seite **Anwendungsvorabstart** auswählen, wann Sitzungen gestartet werden sollen:

- Wenn Benutzer eine Anwendung starten. Dies ist die Standardeinstellung. Der Vorabstart von Sitzungen ist deaktiviert.
- Wenn ein Benutzer der Bereitstellungsgruppe sich bei Citrix Receiver für Windows anmeldet.
- Wenn ein beliebiger Benutzer einer Liste mit Benutzern und Bereitstellungsgruppen sich bei Citrix Receiver für Windows anmeldet. Bei Auswahl dieser Option müssen Sie auch die Benutzer oder Benutzergruppen festlegen.



4. Eine vorab gestartete Sitzung wird durch eine normale Sitzung ersetzt, wenn der Benutzer eine Anwendung startet. Wenn der Benutzer keine Anwendung startet (d. h. die vorab gestartete Sitzung wird nicht verwendet), wird durch die folgenden Einstellungen bestimmt, wie lange die Sitzung aktiv bleibt.

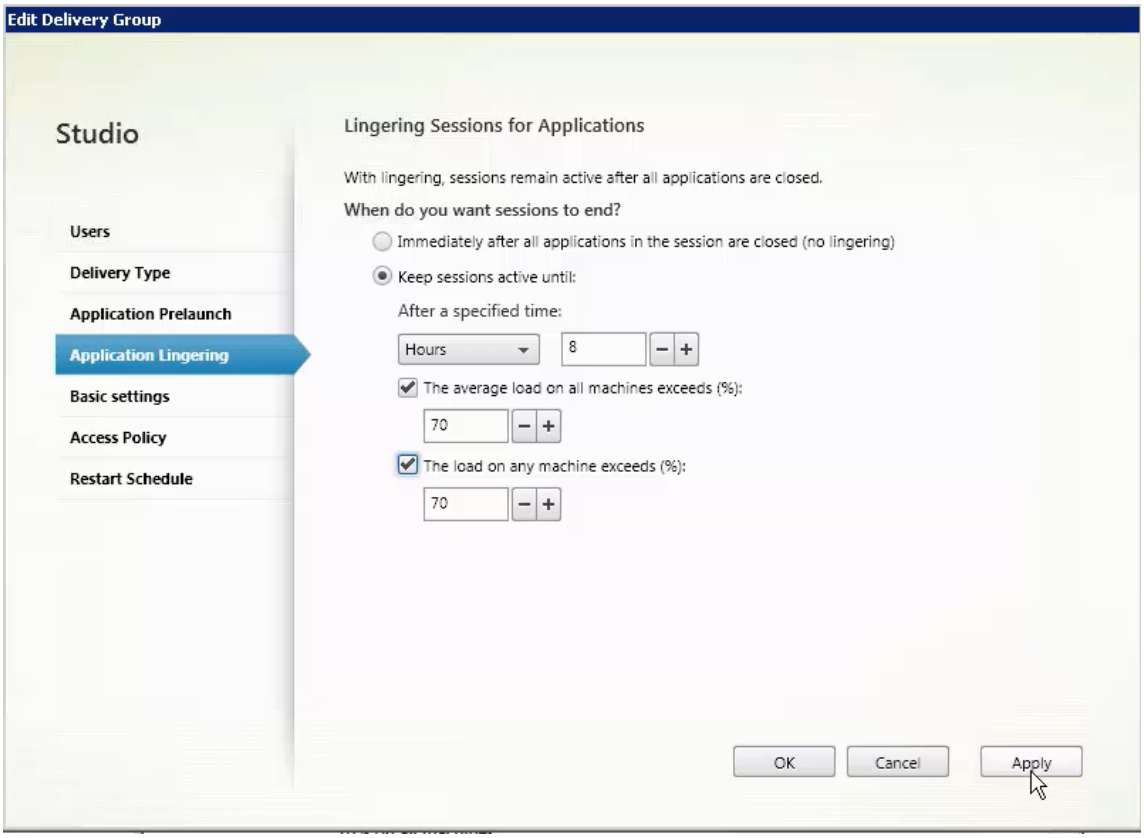
   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern (1-99 Tage, 1-2376 Stunden oder 1-142.560 Minuten).
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.

   Eine vorab gestartete Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der

angegebene Lastschwellenwert wird überschritten.

Aktivieren des Sitzungsfortbestehens

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe bearbeiten**.
3. Aktivieren Sie auf der Seite **Anwendungsfortbestehen** das Sitzungsfortbestehen durch Aktivieren des Optionsfelds **Sitzungen bleiben aktiv bis**.



4. Mehrere Einstellungen wirken sich darauf aus, wie lange eine Sitzung aktiv bleibt, wenn der Benutzer keine weitere Anwendung startet.

   - Ablauf eines vorgegebenen Zeitintervalls. Das Zeitintervall können Sie ändern (1-99 Tage, 1-2376 Stunden oder 1-142.560 Minuten).
   - Wenn die durchschnittliche Last auf allen Maschinen in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.
   - Wenn die Last auf einer Maschine in der Bereitstellungsgruppe einen bestimmten Prozentsatz (1-99 %) übersteigt.

Eine fortbestehende Sitzung bleibt also bis zum Eintreten eines der folgenden Ereignisse aktiv: ein Benutzer startet eine Anwendung, das vorgegebene Zeitintervall läuft ab oder der angegebene Lastschwellenwert wird überschritten.

Problembehandlung

- Nicht bei einem Delivery Controller registrierte VDAs werden beim Starten vermittelter Sitzungen nicht berücksichtigt. Dies führt zu einer Unterauslastung verfügbarer Ressourcen. Es gibt eine Reihe von Gründen, warum ein VDA nicht registriert sein könnte. Viele können vom Administrator behandelt werden. Studio bietet Informationen zur Problembehandlung im Assistenten zum Erstellen von Maschinenkatalogen und nach dem Hinzufügen eines Katalogs zu einer Bereitstellungsgruppe.

  Nach dem Erstellen einer Bereitstellungsgruppe werden in Studio Informationen zu Maschinen angezeigt, die der Gruppe zugeordnet sind. Im Detailbereich für eine Bereitstellungsgruppe wird die Anzahl der Maschinen angezeigt, die registriert sein müssten, es jedoch nicht sind. Es kann also Maschinen geben, die eingeschaltet und nicht im Wartungsmodus sind, jedoch nicht bei einem Controller registriert sind. Beim Anzeigen einer Maschine, die eigentlich registriert sein müsste, enthält die Registerkarte Problembehandlung im Detailbereich Informationen zu möglichen Ursachen und empfohlene Korrekturmaßnahmen.

  Informationen zu Meldungen zur Funktionsebene finden Sie unter VDA-Versionen und Funktionsebenen. Weitere Informationen zur Fehlerbehebung bei der VDA-Registrierung finden Sie unter CTX136668.

- In Studio wird im Detailbereich für Bereitstellungsgruppen unter “Installierte VDA-Version” möglicherweise nicht die tatsächlich auf den Maschinen installierte Version angezeigt. In der Maschine wird in Windows unter “Programme und Features”die tatsächliche VDA-Version angezeigt.
- Empfehlungen für Maschinen mit einem unbekannten Energiezustand finden Sie unter CTX131267.

Erstellen von Anwendungsgruppen

August 18, 2021

Einführung

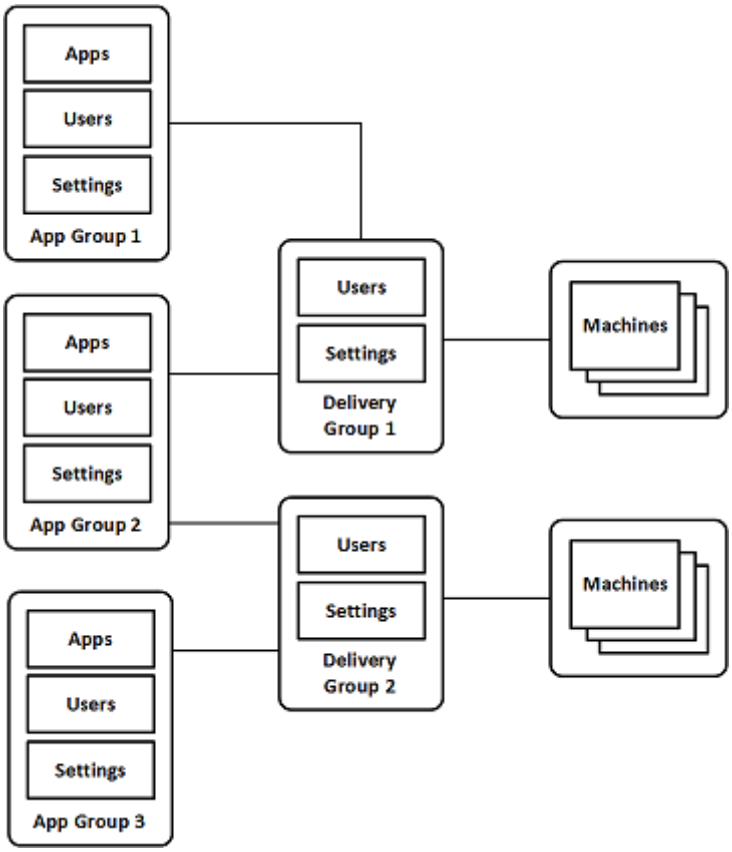
Über Anwendungsgruppen können Sie Anwendungssammlungen verwalten. Sie können Anwendungsgruppen für Anwendungen erstellen, die in verschiedenen Bereitstellungsgruppen oder von einer Benutzerteilgruppe innerhalb einer Bereitstellungsgruppe verwendet werden. Anwendungsgruppen sind optional. Sie bieten eine Alternative zum Hinzufügen derselben Anwendungen zu mehreren Bereitstellungsgruppen. Bereitstellungsgruppen können mehreren Anwendungsgruppen und Anwendungsgruppen können mehreren Bereitstellungsgruppen zugeordnet werden.

Die Verwendung von Anwendungsgruppen kann für die Anwendungsverwaltung und Ressourcensteuerung gegenüber der Verwendung weiterer Bereitstellungsgruppen folgende Vorteile bieten:

- Durch die logische Gruppierung von Anwendungen und deren Einstellungen können Sie diese als Einheit verwalten. Sie müssen beispielsweise dieselbe Anwendung nicht mehreren Bereitstellungsgruppen einzeln hinzufügen (bzw. für diese veröffentlichen).
- Die Sitzungsfreigabe zwischen den Anwendungsgruppen kann Ressourcen sparen. In anderen Fällen ist das Deaktivieren der Sitzungsfreigabe zwischen Anwendungsgruppen möglicherweise nützlich.
- Mit einer *Tagbeschränkung* können Sie Anwendungen aus einer Anwendungsgruppe nur auf einigen Maschinen in den ausgewählten Bereitstellungsgruppen veröffentlichen. Mit Tagbeschränkungen können Sie Ihre vorhandenen Maschinen für mehrere Veröffentlichungstasks verwenden und sparen so die Kosten für die Bereitstellung und Verwaltung zusätzlicher Maschinen. Die Verwendung von Tagbeschränkungen kann man sich als Unterteilung (oder Partitionierung) der Maschinen in einer Bereitstellungsgruppe vorstellen. Anwendungsgruppen und Desktops mit Tagbeschränkungen können auch zur Isolierung von Maschinengruppen in einer Bereitstellungsgruppe zur Problembehandlung nützlich sein.

Beispielkonfigurationen

Beispiel 1 Die folgende Abbildung zeigt eine XenApp- bzw. XenDesktop-Bereitstellung mit Anwendungsgruppen:

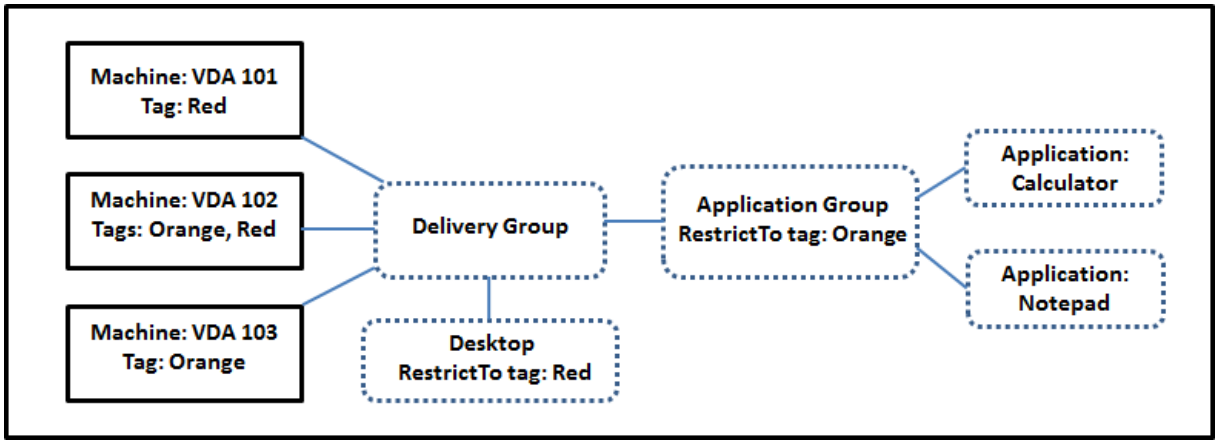


In dieser Konfiguration werden Anwendungen Anwendungsgruppen und nicht Bereitstellungsgruppen hinzugefügt. Über die Bereitstellungsgruppen wird festgelegt, welche Maschinen verwendet werden. (Obwohl dies nicht ausgezeichnet ist, sind die Maschinen in Maschinenkatalogen.)

Anwendungsgruppe 1 ist Bereitstellungsgruppe 1 zugeordnet. Die Anwendungen in Anwendungsgruppe 1 sind für Benutzer der Anwendungsgruppe 1 zugänglich, sofern diese auch auf der Benutzerliste von Bereitstellungsgruppe 1 stehen. Diese Struktur folgt der Leitlinie, dass die Benutzerliste einer Anwendungsgruppe eine Teilgruppe (d. h. Einschränkung) der Benutzerlisten der zugeordneten Bereitstellungsgruppen sein muss. Die Einstellungen von Anwendungsgruppe 1 (Sitzungsfreigabe zwischen den Anwendungsgruppen, zugeordnete Bereitstellungsgruppen usw.) gelten für die Anwendungen und Benutzer in der Gruppe. Die Einstellungen in Bereitstellungsgruppe 1 (z. B. Unterstützung für anonyme Benutzer) gelten für die Benutzer in Anwendungsgruppe 1 und 2, da beide Anwendungsgruppen der Bereitstellungsgruppe zugeordnet sind.

Anwendungsgruppe 2 ist den Bereitstellungsgruppen 1 und 2 zugeordnet. Beiden Bereitstellungsgruppen kann in Anwendungsgruppe 2 eine Priorität zugewiesen werden, welche die Reihenfolge vorgibt, in der die Bereitstellungsgruppen beim Starten einer Anwendung geprüft werden. Für Bereitstellungsgruppen mit der gleichen Priorität findet ein Lastausgleich statt. Die Anwendungen in Anwendungsgruppe 2 sind für Benutzer der Anwendungsgruppe 2 zugänglich, sofern diese auch auf den Benutzerlisten von Bereitstellungsgruppe 1 und 2 stehen.

Beispiel 2 Diese einfache Anordnung besitzt Tagbeschränkungen, die festlegen, welche Maschinen für bestimmte Desktop- und Anwendungsstarts in Betracht gezogen werden. Die Site hat eine freigegebene Bereitstellungsgruppe, einen veröffentlichten Desktop und eine Anwendungsgruppe mit zwei Anwendungen.



Allen drei Maschinen (VDA 101–103) wurden Tags hinzugefügt.

Die Anwendungsgruppe wurde mit der Tagbeschränkung "Orange"erstellt, sodass alle ihre Anwendungen (Rechner und Editor) nur auf Maschinen gestartet werden können, die das Tag "Orange" haben: VDA 102 und 103.

Detailliertere Beispiele und Informationen über die Verwendung von Tagbeschränkungen für Anwendungsgruppen und Desktops finden Sie unter Tags.

Empfehlungen und Tipps

Citrix empfiehlt, Anwendungen entweder Anwendungsgruppen oder Bereitstellungsgruppen zuzuordnen, jedoch nicht beidem. Werden dieselben Anwendungen zwei Gruppentypen zugeordnet, kann dies die Verwaltung erschweren.

Standardmäßig sind Anwendungsgruppen aktiviert. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.

Standardmäßig ist die Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert. Weitere Informationen finden Sie unter Sitzungsfreigabe zwischen Anwendungsgruppen.

Citrix empfiehlt, Bereitstellungsgruppen auf die aktuelle Version zu aktualisieren. Dies erfordert (1) ein Upgrade der VDAs auf den Maschinen der Bereitstellungsgruppe, (2) ein Upgrade der Maschinenkataloge, in denen die Maschinen sind, und (3) das Upgrade der Bereitstellungsgruppe. Weitere Informationen finden Sie unter Verwalten von Bereitstellungsgruppen. Zur Verwendung von Anwendungsgruppen müssen die Kernkomponenten mindestens in Version 7.9 vorliegen.

Zum Erstellen von Anwendungsgruppen ist die Berechtigung zur delegierten Administration der integrierten Rolle des Bereitstellungsgruppenadministrators erforderlich. Siehe Delegierte Administration.

In diesem Abschnitt wird der Begriff der Zuordnung von Anwendungen zu Anwendungsgruppen verwendet, um den Unterschied zum Hinzufügen einer neuen Anwendungsinstanz aus einer verfügbaren Quelle zu unterstreichen. Das Gleiche gilt für Bereitstellungsgruppen und Anwendungsgruppen. Diese werden einander zugeordnet und nicht als Komponenten hinzugefügt.

Sitzungsfreigabe und Anwendungsgruppen

Wenn die Sitzungsfreigabe aktiviert ist, starten alle Anwendungen in der gleichen Anwendungssitzung. Dies spart die Kosten für zusätzliche Sitzungen und ermöglicht die Verwendung von Anwendungsfeatures, wie Kopieren und Einfügen, welche die Zwischenablage erfordern. In manchen Situationen ist es jedoch möglicherweise erforderlich, die Sitzungsfreigabe zu deaktivieren.

Bei Verwendung von Anwendungsgruppen können Sie die Sitzungsfreigabe auf dreierlei Weise konfigurieren (eine Erweiterung gegenüber den Möglichkeiten bei bloßer Verwendung von Bereitstellungsgruppen):

- Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert
- Sitzungsfreigabe nur für Anwendungen innerhalb einer Anwendungsgruppe aktiviert
- Sitzungsfreigabe deaktiviert

Sitzungsfreigabe zwischen Anwendungsgruppen

Sie können die Anwendungssitzungsfreigabe zwischen Anwendungsgruppen aktivieren oder deaktivieren. In letzterem Fall ist sie nur für Anwendungen in derselben Anwendungsgruppe möglich.

Beispielszenario, in dem die Aktivierung der Sitzungsfreigabe zwischen Anwendungsgruppen nützlich ist:

- Anwendungsgruppe 1 enthält Microsoft Office-Anwendungen, z. B. Microsoft Word und Excel. Anwendungsgruppe 2 enthält andere Anwendungen, z. B. Editor und Rechner. Beide Anwendungsgruppen sind derselben Bereitstellungsgruppe zugewiesen. Ein Benutzer mit Zugriff auf beide Anwendungsgruppen startet eine Anwendungssitzung mit Word und startet dann Editor. Wenn der Controller feststellt, dass die Sitzung mit Word zum Ausführen von Editor geeignet ist, wird Editor in der bestehenden Sitzung gestartet. Kann Editor nicht in der vorhandenen Sitzung ausgeführt werden, z. B. weil eine Tagbeschränkung die Maschine ausschließt, auf der die Sitzung ausgeführt wird, wird eine neue Sitzung auf einer geeigneten Maschine erstellt.

Beispielszenario, in dem die Deaktivierung der Sitzungsfreigabe zwischen Anwendungsgruppen nützlich ist:

- Sie haben einige Anwendungen, die mit anderen, auf denselben Maschinen installierten Anwendungen nicht gut zusammenarbeiten, z. B. zwei verschiedene Versionen der gleichen Software oder des gleichen Webbrowsers. Sie möchten nicht, dass ein Benutzer beide Versionen in derselben Sitzung startet.

  Sie erstellen mehrere Anwendungsgruppen und fügen jede Version der Software einer eigenen Anwendungsgruppe hinzu. Wenn die Sitzungsfreigabe zwischen diesen Anwendungsgruppen deaktiviert ist, können die in den Gruppen angegebenen Benutzer Anwendungen der gleichen Version in der gleichen Sitzung ausführen und sie können gleichzeitig andere Anwendungen ausführen, jedoch nicht in der gleichen Sitzung. Wenn ein Benutzer eine der in mehreren Versionen vorliegenden Anwendungen (die in verschiedenen Anwendungsgruppen sind) oder eine nicht in einer Anwendungsgruppe befindliche Anwendung startet, wird diese in einer neuen Sitzung gestartet.

Die Sitzungsfreigabe zwischen Anwendungsgruppen ist keine Sicherheits-Sandbox. Sie ist nicht betriebssicher und kann nicht verhindern, dass Benutzer Anwendungen in ihren Sitzungen über andere Methoden (z. B. über Windows Explorer) starten.

Wenn eine Maschine unter Volllast steht, werden keine neue Sitzungen auf ihr gestartet. Neue Anwendungen werden nach Bedarf in vorhandenen Sitzungen gestartet, vorausgesetzt die hier beschriebenen Bedingungen für die Sitzungsfreigabe sind erfüllt.

Sie können vorab gestartete Sitzungen nur Anwendungsgruppen zur Verfügung stellen, für die die Sitzungsfreigabe zugelassen ist. Sitzungen mit aktiviertem Sitzungsfortbestehen stehen allen Anwendungsgruppen zur Verfügung. Diese Features müssen jedoch in jeder den Anwendungsgruppen zugeordneten Bereitstellungsgruppe aktiviert und konfiguriert werden. Sie können sie nicht in den Anwendungsgruppen konfigurieren.

Die Anwendungssitzungsfreigabe zwischen Anwendungsgruppen wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Dies können Sie bei der Erstellung nicht ändern. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.

Deaktivieren der Sitzungsfreigabe innerhalb von Anwendungsgruppen

Sie können die Sitzungsfreigabe zwischen Anwendungen in derselben Anwendungsgruppe verhindern.

Beispielszenario, in dem die Deaktivierung der Sitzungsfreigabe innerhalb von Anwendungsgruppen nützlich ist:

- Die Benutzer sollen simultan auf mehrere Vollbildsitzungen einer Anwendung auf separaten Monitoren zugreifen.

Sie erstellen eine Anwendungsgruppe und fügen ihr die Anwendungen hinzu. Wenn die Sitzungsfreigabe zwischen den Anwendungen der Anwendungsgruppe nicht zugelassen ist und ein Benutzer Anwendungen nacheinander startet, werden sie in separaten Sitzungen gestartet und der Benutzer kann jede zu einem separaten Monitor verschieben.

Die Anwendungssitzungsfreigabe wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Dies können Sie bei der Erstellung nicht ändern. Nach dem Erstellen einer Anwendungsgruppe können Sie diese Einstellung ändern. Weitere Informationen finden Sie unter Verwalten von Anwendungsgruppen.

Erstellen von Anwendungsgruppen

Gehen Sie zum Erstellen von Anwendungsgruppen folgendermaßen vor:

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und im Aktionsbereich **Anwendungsgruppe erstellen**.
2. Der Assistent zum Erstellen von Anwendungsgruppen wird mit der **Einführungsseite** gestartet, die Sie für zukünftige Starts des Assistenten deaktivieren können.
3. Der Assistent führt Sie durch die nachfolgend beschriebenen Seiten. Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur Seite "Zusammenfassung"gelangen.

Bereitstellungsgruppen

Alle Bereitstellungsgruppen werden zusammen mit der Anzahl enthaltener Maschinen aufgelistet.

- Die Liste **Kompatible Bereitstellungsgruppen** enthält Bereitstellungsgruppen, die Sie auswählen können. Kompatible Bereitstellungsgruppen enthalten zufällige (nicht dauerhaft oder statisch zugewiesene) Server- oder Desktopbetriebssystemmaschinen.
- Die Liste **Nicht kompatible Bereitstellungsgruppen** enthält Bereitstellungsgruppen, die Sie nicht auswählen können. Jeder Eintrag enthält eine Begründung der Inkompatibilität, z. B. "enthält statisch zugewiesene Maschinen".

Eine Anwendungsgruppe kann Bereitstellungsgruppen zugeordnet werden, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten.

Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, wenn (1) die Bereitstellungsgruppe freigegebene Maschinen enthält und mit einer früheren XenDesktop 7.x-Version erstellt wurde und (2) Sie die Berechtigung zum Bearbeiten von Bereitstellungsgruppen haben. Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen"geändert, wenn für den Assistenten zum Erstellen von Anwendungsgruppen ein Commit ausgeführt wird.

Sie können Anwendungsgruppen erstellen, die keiner Bereitstellungsgruppe zugeordnet sind, z. B. zum Organisieren von Anwendungen oder als Speicher für Anwendungen, die gerade nicht verwendet werden. Anwendungsgruppen können jedoch erst dann zum Bereitstellen von Anwendungen verwendet werden, wenn sie mindestens einer Bereitstellungsgruppe zugeordnet sind. Außerdem können Sie einer Anwendungsgruppe keine Anwendungen aus der Quelle Vom Startmenü hinzufügen, wenn keine Bereitstellungsgruppen angegeben sind.

Über die Bereitstellungsgruppen legen Sie fest, welche Maschinen für die Bereitstellung von Anwendungen verwendet werden. Aktivieren Sie die Kontrollkästchen neben den Bereitstellungsgruppen, die Sie der Anwendungsgruppe zuordnen möchten.

Zum Hinzufügen einer Tagbeschränkung wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag aus der Dropdownliste aus. Weitere Informationen finden Sie unter Tags.

Benutzer

Geben Sie an, wer die Anwendungen in der Anwendungsgruppe verwenden kann. Sie können entweder alle Benutzer und Gruppen in den Bereitstellungsgruppen, die Sie auf der vorherigen Seite ausgewählt haben, angeben oder bestimmte Benutzer bzw. Benutzergruppen aus den Bereitstellungsgruppen auswählen. Wenn Sie die Benutzer einschränken, haben nur die in der Bereitstellungsgruppe und der Anwendungsgruppe angegebenen Benutzer Zugriff auf die Anwendungen in der Anwendungsgruppe. Im Prinzip wirkt die Benutzerliste der Anwendungsgruppe als Filter für die Benutzerlisten in den Bereitstellungsgruppen.

Das Aktivieren oder Deaktivieren der Anwendungsverwendung durch nicht authentifizierte Benutzer ist nur über Bereitstellungsgruppen, nicht aber über Anwendungsgruppen möglich.

Festlegung von Benutzerlisten Active Directory-Benutzerlisten werden angegeben, wenn Sie Folgendes erstellen oder bearbeiten:

- Anspruchbenutzerliste für die Bereitstellungsgruppe, die nicht über Studio konfiguriert wird Standardmäßig umfasst die Anwendungsanspruch-Richtlinienregel alle Benutzer (Einzelheiten siehe BrokerAppEntitlementPolicyRule-Cmdlets des PowerShell-SDKs).
- Benutzerliste der Anwendungsgruppe
- Benutzerliste der Bereitstellungsgruppe
- Eigenschaft der Anwendungssichtbarkeit

Die Liste der Benutzer, die Zugriff auf eine Anwendung über StoreFront haben, wird aus der Schnittmenge der oben angegebenen Benutzerlisten erstellt. Wenn Sie beispielsweise die Verwendung von Anwendung A für eine bestimmte Abteilung konfigurieren möchten, ohne Zugriff für andere Gruppen unnötig einzuschränken, gehen Sie folgendermaßen vor:

- Verwenden der Standardanwendungsanspruch-Richtlinienregel, die für alle Benutzer gilt
- Konfigurieren Sie die Benutzerliste der Bereitstellungsgruppe so, dass alle Benutzer der Organisation die Anwendungen der Bereitstellungsgruppe verwenden können.
- Konfigurieren Sie die Benutzerliste der Anwendungsgruppe so, dass die Mitarbeiter der Verwaltungs- und der Finanzabteilung Zugriff auf Anwendungen A bis L erhalten.
- Konfigurieren Sie die Eigenschaften von Anwendung A so, dass sie nur für Mitarbeiter der Debitorenbuchhaltung innerhalb der Finanzabteilung sichtbar ist.

Anwendungen

Nützliche Info:

- Standardmäßig werden neu hinzugefügte Anwendungen in einem Ordner mit dem Namen Applications abgelegt. Sie können einen anderen Ordner angeben. Wenn Sie eine Anwendung hinzufügen und es dort bereits eine Anwendung mit dem gleichen Namen gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Wenn Sie den empfohlenen eindeutigen Namen annehmen, wird die Anwendung unter dem Namen hinzugefügt, ansonsten müssen Sie sie umbenennen, damit sie hinzugefügt werden kann. Weitere Informationen finden Sie unter Verwalten von Anwendungsordnern.
- Sie können Anwendungseigenschaften (Einstellungen) beim Hinzufügen oder später ändern. Weitere Informationen finden Sie unter Ändern der Eigenschaften. Wenn Sie zwei Anwendungen mit dem gleichen Namen den gleichen Benutzern bereitstellen, ändern Sie in Studio die Eigenschaft "Anwendungsname (Benutzer)", sonst wird den Benutzern der Name in Citrix Receiver doppelt angezeigt.
- Wenn Sie eine Anwendung mehreren Anwendungsgruppen hinzufügen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Anwendungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Gruppen, denen die Anwendung hinzugefügt wurde.

Klicken Sie auf die Dropdownliste **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

- **Vom Startmenü:** Anwendungen, die auf einer Maschine in den ausgewählten Bereitstellungsgruppen erkannt werden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**. Diese Quelle kann nicht ausgewählt werden, wenn Sie (1) Anwendungsgruppen gewählt haben, denen keine Bereitstellungsgruppen zugeordnet sind, (2) Anwendungsgruppen gewählt haben, deren zugeordnete Bereitstellungsgruppen keine Maschinen enthalten, oder (3) eine Bereitstellungsgruppe gewählt haben, die keine Maschinen enthält.
- **Manuell definiert:** Anwendungen in der Site oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur

ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Wenn Sie diese Informationen eingegeben haben, klicken Sie auf **OK**.

- **Vorhandene:** Anwendungen, die der Site bereits hinzugefügt wurden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**. Diese Quelle kann nicht ausgewählt werden, wenn es in der Site keine Anwendungen gibt.
- **App-V:** Anwendungen in App-V-Paketen. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, in der Sie den App-V-Server oder die Anwendungsbibliothek auswählen. Aktivieren Sie dort die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf **OK**. Weitere Informationen finden Sie unter App-V. Diese Quelle kann nicht ausgewählt werden (oder wird möglicherweise nicht angezeigt), wenn App-V für die Site nicht konfiguriert ist.

Wie bereits erwähnt, können Einträge in der Dropdownliste **Hinzufügen** nicht ausgewählt werden, wenn es keine gültige Quelle des jeweiligen Typs gibt. Nicht kompatible Quellen werden nicht aufgelistet (z. B. können Sie Anwendungsgruppen keine Anwendungsgruppen hinzufügen, daher wird diese Quelle nicht angezeigt).

Geltungsbereiche

Diese Seite wird nur angezeigt, wenn Sie zuvor einen Geltungsbereich erstellt haben. Standardmäßig ist der Bereich Alles ausgewählt. Weitere Informationen finden Sie unter Delegierte Administration.

Zusammenfassung

Geben Sie einen Namen für die Anwendungsgruppe ein. Sie können optional auch eine Beschreibung eingeben.

Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Verwalten von Anwendungsgruppen

August 18, 2021

Einführung

In diesem Abschnitt wird die Verwaltung von Anwendungsgruppen beschrieben, die Sie erstellt haben.

Unter Anwendungen finden Sie Informationen zur Verwaltung von Anwendungen in Anwendungsgruppen oder Bereitstellungsgruppen. Es werden u. a. folgende Themen behandelt:

- Hinzufügen und Entfernen von Anwendungen zu bzw. aus Anwendungsgruppen:
- Ändern von Anwendungsgruppenzuordnungen

Zum Verwalten von Anwendungsgruppen sind die Berechtigungen zur delegierten Administration der integrierten Rolle des Bereitstellungsgruppenadministrators erforderlich. Weitere Informationen finden Sie unter Delegierte Administration.

Aktivieren und Deaktivieren von Anwendungsgruppen

Wenn eine Anwendungsgruppe aktiviert wurde, kann sie die Anwendungen bereitstellen, die ihr hinzugefügt wurden. Durch Deaktivieren einer Anwendungsgruppe werden alle darin enthaltenen Anwendungen deaktiviert. Anwendungen, die auch anderen aktivierten Anwendungsgruppen zugeordnet sind, können über diese Gruppen bereitgestellt werden. Wenn eine Anwendung nicht nur einer Anwendungsgruppe, sondern explizit auch einer mit der Anwendungsgruppe verknüpften Bereitstellungsgruppe hinzugefügt wurde, hat das Deaktivieren der Anwendungsgruppe keine Auswirkungen auf die Anwendung in der Bereitstellungsgruppe.

Anwendungsgruppen werden beim Erstellen aktiviert. Dies können Sie bei der Erstellung nicht ändern.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Anwendungsgruppe aktivieren**.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Aktivieren und Deaktivieren der Anwendungssitzungsfreigabe zwischen Anwendungsgruppen

Die Sitzungsfreigabe zwischen Anwendungsgruppen wird beim Erstellen von Anwendungsgruppen aktiviert. Dies können Sie bei der Erstellung nicht ändern. Weitere Informationen über die Sitzungsfreigabe finden Sie unter Sitzungsfreigabe zwischen Anwendungsgruppen.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.

3. Aktivieren oder deaktivieren Sie auf der Seite **Einstellungen** das Kontrollkästchen **Sitzungsfreigabe zwischen Anwendungsgruppen aktiviert**.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Deaktivieren der Anwendungssitzungsfreigabe in einer Anwendungsgruppe

Die Sitzungsfreigabe zwischen Anwendungen in einer Gruppe wird beim Erstellen von Anwendungsgruppen standardmäßig aktiviert. Wenn Sie die Sitzungsfreigabe zwischen Anwendungsgruppen deaktivieren, bleibt sie für Anwendungen in derselben Gruppe aktiviert. Mit dem Broker-PowerShell-SDK können Sie Anwendungsgruppen konfigurieren, bei denen die Sitzungsfreigabe zwischen den enthaltenen Anwendungen deaktiviert ist. In manchen Situationen kann dies vorteilhaft sein, etwa wenn Benutzer Nicht-Seamless-Anwendungen in voller Fenstergröße auf separaten Monitoren öffnen sollen. Weitere Informationen über die Sitzungsfreigabe finden Sie unter Sitzungsfreigabe und Anwendungsgruppen.

Wenn Sie die Sitzungsfreigabe in einer Anwendungsgruppe deaktivieren, wird jede Anwendung in der Gruppe in einer eigenen Anwendungssitzung gestartet. Wenn eine geeignete getrennte Sitzung verfügbar ist, in der dieselbe Anwendung ausgeführt wird, wird eine Verbindung zu dieser Sitzung wiederhergestellt. Wenn Sie beispielsweise Editor starten und es gibt eine getrennte Sitzung, in der Editor ausgeführt wird, wird keine neue Sitzung gestartet, sondern die Verbindung mit der getrennten Sitzung wiederhergestellt. Sind mehrere geeignete, getrennte Sitzungen verfügbar, wird eine dieser Sitzungen nach dem Zufallsprinzip gewählt. Die Wahl ist unter einer Bedingung vorhersagbar: Wenn die Situation unter den gleichen Bedingungen erneut auftritt, wird die gleiche Sitzung gewählt.
Mit dem Broker-PowerShell-SDK können Sie die Anwendungssitzungsfreigabe für alle Anwendungen in einer Anwendungsgruppe deaktivieren oder eine Anwendungsgruppe mit deaktivierter Sitzungsfreigabe erstellen.

PowerShell-Cmdlet-Beispiele

Verwenden Sie zum Deaktivieren der Sitzungsfreigabe die Broker-PowerShell-Cmdlets **New-BrokerApplicationGroup** oder **Set-BrokerApplicationGroup** mit der Einstellung “False”für den Parameter **-SessionSharingEnabled** und der Einstellung “True”für den Parameter **-SingleAppPerSession**.

Beispiel zum Erstellen einer Anwendungsgruppe mit deaktivierter Sitzungsfreigabe für alle enthaltenen Anwendungen:

```
New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -
SingleAppPerSession $True
```


Beispiel zum Deaktivieren der Sitzungsfreigabe für alle Anwendungen einer Anwendungsgruppe:

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -
SingleAppPerSession $True
```

> **Hinweise:**
>
> - Um die Eigenschaft "SingleAppPerSession"zu aktivieren, müssen Sie die Eigenschaft "SessionSharingEnabled"auf "False"festlegen. Die beiden Eigenschaften dürfen nicht gleichzeitig aktiviert werden. Der Parameter "SessionSharingEnabled"bezieht sich auf die Sitzungsfreigabe zwischen Anwendungsgruppen.
> - Die Sitzungsfreigabe funktioniert nur bei Anwendungen, die Anwendungsgruppen aber keinen Bereitstellungsgruppen zugeordnet sind. (Für alle direkt einer Bereitstellungsgruppe zugeordneten Anwendungen ist die Sitzungsfreigabe standardmäßig aktiviert.)
> - Wenn eine Anwendung mehreren Anwendungsgruppen zugewiesen ist, stellen Sie sicher, dass die Gruppen keine widersprüchlichen Einstellungen aufweisen (z. B. eine die Einstellung "true"und die andere die Einstellung "false"), da dies zu unvorhersehbarem Verhalten führt.

Umbenennen von Anwendungsgruppen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe umbenennen**.
3. Geben Sie einen neuen eindeutigen Namen ein und klicken Sie auf **OK**.

Hinzufügen und Entfernen von Bereitstellungsgruppenzuordnungen für Anwendungsgruppen und Ändern der Priorität von Gruppenzuordnungen

Eine Anwendungsgruppe kann Bereitstellungsgruppen zugeordnet werden, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten.

Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, wenn (1) die Bereitstellungsgruppe freigegebene Maschinen enthält und mit einer früheren XenDesktop 7.x-Version erstellt wurde und (2) Sie die Berechtigung zum Bearbeiten von Bereitstellungsgruppen haben. Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen"geändert, wenn für das Dialogfeld Anwendungsgruppe bearbeiten ein Commit ausgeführt wird.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.

3. Wählen Sie die Seite **Bereitstellungsgruppen**.
4. Klicken Sie zum Hinzufügen von Bereitstellungsgruppen auf **Hinzufügen**. Aktivieren Sie die Kontrollkästchen verfügbarer Bereitstellungsgruppen. (Nicht kompatible Bereitstellungsgruppen können nicht ausgewählt werden.) Wenn Sie fertig sind, klicken Sie auf **OK**.
5. Zum Entfernen von Bereitstellungsgruppen aktivieren Sie die Kontrollkästchen der gewünschten Gruppen und klicken Sie auf **Entfernen**. Bestätigen Sie die Löschung, wenn Sie dazu aufgefordert werden.
6. Zum Ändern der Priorität von Bereitstellungsgruppen aktivieren Sie das Kontrollkästchen einer Bereitstellungsgruppe und klicken Sie auf **Priorität bearbeiten**. Geben Sie die Priorität an (0=höchste) und klicken Sie auf **OK**.
7. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Hinzufügen und Entfernen von Tagbeschränkungen zu bzw. aus Anwendungsgruppen

Wichtig: Das Hinzufügen, Bearbeiten und Entfernen von Tagbeschränkungen kann unerwartete Auswirkungen darauf haben, welche Maschinen für den Anwendungsstart in Betracht gezogen werden. Lesen Sie unbedingt die Informationen und Hinweise im Artikel Tags.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Bereitstellungsgruppen**.
4. Zum Hinzufügen einer Tagbeschränkung wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag aus der Dropdownliste aus.
5. Zum Ändern oder Entfernen einer Tagbeschränkung wählen Sie ein anderes Tag aus der Dropdownliste oder entfernen Sie die Tagbeschränkung vollständig durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.
6. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Hinzufügen und Entfernen von Benutzern zu bzw. aus Anwendungsgruppen

Ausführliche Informationen zu Benutzern finden Sie unter Erstellen von Anwendungsgruppen im Abschnitt *Benutzer*.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.

2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Benutzer**. Geben Sie an, ob alle Benutzer oder nur bestimmte Benutzer und Gruppen in den zugeordneten Bereitstellungsgruppen Anwendungen in der Anwendungsgruppe verwenden können sollen. Zum Hinzufügen von Benutzern klicken Sie auf **Hinzufügen** und geben Sie die Benutzer an, die Sie hinzufügen möchten. Zum Entfernen von Benutzern wählen Sie mindestens einen Benutzer aus und klicken Sie auf **Entfernen**.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Ändern der Geltungsbereiche in Anwendungsgruppen

Sie können Geltungsbereiche nur dann ändern, wenn Sie einen Geltungsbereich erstellt haben. Den Geltungsbereich "Alle"können Sie nicht bearbeiten. Weitere Informationen finden Sie im Artikel Delegierte Administration.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie dann im Aktionsbereich auf **Anwendungsgruppe bearbeiten**.
3. Wählen Sie die Seite **Geltungsbereiche**. Aktivieren oder deaktivieren Sie das Kontrollkästchen neben einem Geltungsbereich.
4. Klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Löschen von Anwendungsgruppen

Eine Anwendung muss mindestens einer Bereitstellungsgruppe oder Anwendungsgruppe zugeordnet sein. Wenn durch das Löschen einer Anwendungsgruppe eine oder mehrere Anwendungen nicht mehr zu einer Gruppe gehören würden, wird eine Warnung angezeigt, dass mit dem Löschen der Gruppe auch diese Anwendungen gelöscht würden. Sie können den Löschvorgang dann bestätigen oder abbrechen.

Durch das Löschen einer Anwendung wird diese nicht aus der ursprünglichen Quelle gelöscht, doch wenn Sie sie wieder zur Verfügung stellen möchten, müssen Sie sie erneut hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich eine Anwendungsgruppe aus, und klicken Sie im Aktionsbereich auf **Gruppe löschen**.
3. Bestätigen Sie die Löschung, wenn Sie dazu aufgefordert werden.

Remote-PC-Zugriff

October 21, 2021

Remote-PC-Zugriff ist eine Funktion von Citrix Virtual Apps and Desktops, mit der Organisationen ihren Mitarbeitern einfach und sicher Zugriff auf Unternehmensressourcen geben können. Die Citrix-Plattform ermöglicht diesen sicheren Zugriff, indem Benutzer Zugriff auf ihre physischen Büro-PCs erhalten. Wenn Benutzer auf ihre Büro-PCs zugreifen können, können sie auf alle Anwendungen, Daten und Ressourcen zugreifen, die sie für ihre Arbeit benötigen. Mit Remote-PC-Zugriff ist das Einführen und Bereitstellen anderer Tools für die Telearbeit überflüssig. Zum Beispiel virtuelle Desktops oder Anwendungen und die zugehörige Infrastruktur.

Remote-PC-Zugriff verwendet dieselben Citrix Virtual Apps and Desktops-Komponenten zum Bereitstellen von virtuellen Desktops und Anwendungen. Daher sind die Anforderungen und der Prozess für die Bereitstellung und Konfiguration des Remote-PC-Zugriffs die gleichen wie für die Bereitstellung von virtuellen Ressourcen mit Citrix Virtual Apps and Desktops. Diese Einheitlichkeit bietet eine konsistente und gemeinsame administrative Erfahrung. Benutzer erhalten die beste Benutzererfahrung, wenn sie Citrix HDX für die Bereitstellung ihrer Büro-PC-Sitzungen verwenden.

Das Feature besteht aus einem Maschinenkatalog vom Typ **Remote-PC-Zugriff**, der diese Funktionalität bietet:

- Möglichkeit, Maschinen durch Angeben von Organisationseinheiten hinzuzufügen. Diese Fähigkeit erleichtert das Hinzufügen von PCs in großen Mengen.
- Automatische Benutzerzuweisung basierend auf dem Benutzer, der sich am Windows-PC im Büro anmeldet. Wir unterstützen Einzel- und Mehrbenutzerzuweisungen.

Citrix Virtual Apps and Desktops weitere Anwendungsfälle für physische PCs über andere Arten von Maschinenkatalogen abdecken. Anwendungsfälle sind unter anderen:

- Physische Linux-PCs
- Gepoolte physische PCs (d. h. zufällig zugewiesen, nicht dediziert)

> **Hinweise:**
>
> Einzelheiten zu den unterstützten Betriebssystemversionen finden Sie in den Systemanforderungen für Virtual Delivery Agent (VDA) für Desktopbetriebssysteme und für Linux VDA.
>
> Bei On-Premises-Bereitstellungen gilt Remote-PC-Zugriff nur für Advanced- und Premium-Lizenzen für Citrix Virtual Apps and Desktops. Sitzungen verbrauchen Lizenzen genau wie andere Citrix Virtual Desktops-Sitzungen. Bei Citrix Cloud ist Remote-PC-Zugriff für Citrix Virtual Apps and Desktops Service und Workspace Premium Plus gültig.

Überlegungen

Während alle technischen Anforderungen und Überlegungen, die für Citrix Virtual Apps and Desktops im Allgemeinen gelten, auch für Remote-PC-Zugriff zutreffen, sind einige möglicherweise relevanter oder gelten exklusiv für den Anwendungsfall physischer PCs.

Überlegungen zur Bereitstellung

Beim Planen der Bereitstellung des Remote-PC-Zugriffs treffen Sie einige allgemeine Entscheidungen.

- Sie können den Remote-PC-Zugriff zu einer vorhandenen Citrix Virtual Apps and Desktops-Bereitstellung hinzufügen. Bevor Sie diese Option wählen, sollten Sie Folgendes bedenken:
  - Sind die aktuellen Delivery Controller oder Cloud Connectors entsprechend groß, um die zusätzliche Last zu unterstützen, die durch die Remote-PC-Zugriff-VDAs verursacht wird?
  - Sind die On-Premises-Sitekonfigurationsdatenbanken und Datenbankserver entsprechend groß, um die zusätzliche Last zu unterstützen, die durch die Remote-PC-Zugriff-VDAs verursacht wird?
  - Übersteigen die vorhandenen VDAs und die neuen VDAs für Remote-PC-Zugriff die Anzahl der maximal unterstützten VDAs pro Site?
- Sie müssen den VDA über einen automatisierten Prozess auf Büro-PCs bereitstellen. Die folgenden Optionen sind verfügbar:
  - ESD-Tools (Electronic Software Distribution) wie z. B. SCCM: Installieren von VDAs mit SCCM.
  - Bereitstellungsskripts: Installieren von VDAs mit Skripts.
- Lesen Sie die Sicherheitsüberlegungen für Remote-PC-Zugriff.

Überlegungen zum Maschinenkatalog

Die Art des erforderlichen Maschinenkatalogs hängt vom Anwendungsfall ab:

- Remote-PC-Zugriff
  - Dedizierte Windows-PCs
  - Dedizierte Windows-Mehrbenutzer-PCs
- Einzelsitzungs-OS
  - Statisch - Dedizierte Linux-PCs
  - Zufällig - Gepoolte Windows- und Linux-PCs

Wenn Sie den Typ des Maschinenkatalogs identifiziert haben, sollten Sie Folgendes beachten:

- Eine Maschine kann nur jeweils einem Maschinenkatalog zugewiesen sein.
- Um die delegierte Administration zu erleichtern, sollten Sie Maschinenkataloge auf der Grundlage des geografischen Standorts, der Abteilung oder einer anderen Gruppierung erstellen, die die Delegierung der Verwaltung jedes Katalogs an die entsprechenden Administratoren erleichtert.
- Wählen Sie bei der Auswahl der Organisationseinheit, in der die Maschinenkonten sind, Organisationseinheiten auf einer niedrigeren Ebene aus, um eine größere Granularität zu erzielen. Wenn eine solche Granularität nicht erforderlich ist, können Sie übergeordnete Organisationseinheiten auswählen. Wählen Sie beispielsweise im Fall von Bank/Bankbeamte/Kassierer die Option **Kassierer** aus, um eine größere Granularität zu erzielen. Sonst können Sie **Bankbeamte** oder **Bank** wählen, je nach Anforderung.
- Das Verschieben oder Löschen von Organisationseinheiten nachdem sie einem Remote-PC-Zugriffs-Maschinenkatalog zugewiesen wurden, wirkt sich auf VDA-Zuordnungen aus und verursacht Probleme mit zukünftigen Zuweisungen. Daher sollten Sie Zuweisungsupdates von Organisationseinheiten für Maschinenkataloge bei der Active Directory-Änderungsplanung berücksichtigen.
- Wenn die OU-Struktur keine einfache Auswahl der Organisationseinheiten zulässt, um Maschinen einem Maschinenkatalog hinzuzufügen, müssen Sie keine Organisationseinheiten auswählen. Sie können PowerShell verwenden, um anschließend Maschinen dem Katalog hinzuzufügen. Automatische Benutzerzuweisungen funktionieren weiterhin, wenn die Desktopzuweisung in der Bereitstellungsgruppe korrekt konfiguriert ist. Ein Beispielskript zum Hinzufügen von Maschinen zum Maschinenkatalog zusammen mit Benutzerzuweisungen ist verfügbar unter GitHub.
- Integriertes Wake-On-LAN ist nur mit einem Maschinenkatalog des Typs **Remote-PC-Zugriff** verfügbar.

Linux-VDA-Überlegungen

Diese Überlegungen gelten speziell für den Linux-VDA:

- Verwenden Sie den Linux-VDA auf physischen Maschinen nur im Nicht-3D-Modus. Aufgrund von Einschränkungen des NVIDIA-Treibers kann der lokale Bildschirm des PCs nicht ausgeblendet werden und zeigt die Aktivitäten der Sitzung an, wenn der HDX 3D-Modus aktiviert ist. Das Anzeigen dieses Bildschirms ist ein Sicherheitsrisiko.
- Verwenden Sie Maschinenkataloge des Typs “Einzelsitzungs-OS”für physische Linux-Maschinen.
- Die integrierte Wake-On-LAN-Funktionalität ist für Linux-Maschinen nicht verfügbar.

Technische Anforderungen und Überlegungen

Dieser Abschnitt enthält die technischen Anforderungen und Überlegungen für physische PCs.

- Folgendes wird nicht unterstützt:
  - KVM-Switches oder andere Komponenten, die eine Sitzung trennen.
  - Hybrid-PCs, einschließlich All-in-One- und NVIDIA Optimus-Laptops und -PCs.
- Schließen Sie Tastatur und Maus direkt an den PC an. Beim Anschließen an den Monitor oder an andere Komponenten, die ausgeschaltet oder getrennt werden können, sind diese Peripheriegeräte dann möglicherweise nicht mehr verfügbar. Wenn Sie Eingabegeräte an Komponenten wie beispielsweise Bildschirme anschließen müssen, schalten Sie diese Komponenten nicht aus.
- Die PCs müssen zu einer Active Directory-Domänendienste-Domäne gehören.
- Secure Boot wird nur unter Windows 10 unterstützt.
- Der PC muss eine aktive Netzwerkverbindung haben. Eine Kabelverbindung wird für eine höhere Zuverlässigkeit und Bandbreite bevorzugt.
- Bei WLAN-Verbindungen gehen Sie wie folgt vor:
  1. Legen Sie die Energieeinstellungen so fest, dass der WLAN-Adapter eingeschaltet bleibt.
  2. Konfigurieren Sie den WLAN-Adapter und das Netzwerkprofil so, dass die automatische Verbindung mit dem WLAN-Netzwerk vor der Benutzeranmeldung zulässig ist. Sonst wird der VDA erst registriert, wenn sich der Benutzer anmeldet. Der PC ist erst für den Remotezugriff verfügbar, wenn ein Benutzer sich angemeldet hat.
  3. Stellen Sie sicher, dass die Delivery Controller oder Cloud Connectors im Wi-Fi-Netzwerk erreichbar sind.
- Remote-PC-Zugriff kann auf Laptops verwendet werden. Stellen Sie sicher, dass der Laptop an eine Stromquelle angeschlossen ist, anstatt mit dem Akku zu arbeiten. Konfigurieren Sie die Energieoptionen von Laptops wie bei Desktop-PCs. Beispiel:
  1. Deaktivieren Sie den Ruhezustand.
  2. Deaktivieren Sie den Energiesparmodus.
  3. Legen Sie die Aktion beim Schließen des Deckels auf **Nichts tun** fest.
  4. Legen Sie die Aktion bei Betätigen der Ein-/Ausschalttaste auf **Herunterfahren** fest.
  5. Deaktivieren Sie die Energiesparfunktionen der Netzwerk- und der Grafikkarte.
- Remote-PC-Zugriff wird auf Surface Pro-Geräten mit Windows 10 unterstützt. Folgen Sie den gleichen Richtlinien für Laptops, die zuvor erwähnt wurden.
- Wenn Sie eine Dockingstation verwenden, können Sie Laptops abdocken und neu andocken. Wenn Sie einen Laptop abdocken, registriert sich der VDA bei Delivery Controllern bzw. Cloud

Connectors neu über das Wi-Fi-Netzwerk. Wenn Sie den Laptop neu andocken, wechselt der VDA allerdings nicht zur Kabelverbindung, es sei denn, Sie trennen den WLAN-Adapter vom Netzwerk. Bei einigen Geräten sorgt eine integrierte Funktion für die Trennung des WLAN-Adapters beim Herstellen einer Kabelverbindung. Bei anderen ist eine benutzerdefinierte Lösung oder ein Hilfsprogramm eines Drittanbieters erforderlich. Konsultieren Sie in diesem Zusammenhang die zuvor erwähnten Wi-Fi-Überlegungen.

Zum Aktivieren des An- und Abdockens von Remote-PC-Zugriff-Geräten führen Sie folgende Schritte aus:

1. Wählen Sie im Menü **Start** die Option **Einstellungen > System > Netzbetrieb und Standbymodus** und legen Sie für **Standbymodus** die Einstellung **Nie** fest.
2. Rufen Sie unter **Geräte-Manager > Netzwerkadapter > Ethernet-Adapter** den Bereich **Energieverwaltung** auf und deaktivieren Sie **Computer kann das Gerät ausschalten, um Energie zu sparen**. Stellen Sie sicher, dass **Gerät kann den Computer aus dem Ruhezustand aktivieren** aktiviert ist.

- Mehrere Benutzer mit Zugriff auf denselben Büro-PC sehen in Citrix Workspace dasselbe Symbol. Wenn sich ein Benutzer bei Citrix Workspace anmeldet, wird diese Ressource als nicht verfügbar angezeigt, wenn sie bereits von einem anderen Benutzer verwendet wird.
- Installieren Sie die Citrix Workspace-App auf jedem Clientgerät (z. B. einem Heim-PC), das auf den Büro-PC zugreift.

Konfigurationssequenz

Dieser Abschnitt enthält eine Übersicht über das Konfigurieren des Remote-PC-Zugriffs, wenn Sie einen Maschinenkatalog des Typs **Remote-PC-Zugriff** verwenden. Weitere Informationen zum Erstellen anderer Arten von Maschinenkatalogen finden Sie unter Erstellen von Maschinenkatalogen.

1. Nur On-Premises-Site - Um die integrierte Wake-On-LAN-Funktion zu verwenden, konfigurieren Sie die unter Wake-On-LAN beschriebenen Voraussetzungen.
2. Wenn eine neue Citrix Virtual Apps and Desktops-Site für Remote-PC-Zugriff erstellt wurde:
   a) Wählen Sie als Sitetyp **Remote-PC-Zugriff**.
   b) Auf der Seite **Energieverwaltung** aktivieren oder deaktivieren Sie die Energieverwaltung für den Standardmaschinenkatalog für Remote-PC-Zugriff. Sie können diese Einstellung später ändern, indem Sie die Eigenschaften des Maschinenkatalogs bearbeiten. Weitere Informationen zur Konfiguration von Wake-On-LAN finden Sie unter Wake-On-LAN.
   c) Füllen Sie die Seiten **Benutzer** und **Maschinenkonten** aus.

   Mit diesen Schritten werden automatisch ein Maschinenkatalog **Remote-PC-Zugriff-Maschinen** und eine Bereitstellungsgruppe **Remote-PC-Zugriff-Desktops** erstellt.

3. Wenn eine vorhandene Citrix Virtual Apps and Desktops-Site erweitert wird:

    a) Erstellen Sie einen Maschinenkatalog vom Typ **Remote-PC-Zugriff** (im Assistenten auf der Seite "Betriebssystem"). Weitere Informationen zum Erstellen eines Maschinenkatalogs finden Sie unter Erstellen von Maschinenkatalogen. Stellen Sie sicher, dass Sie die richtige Organisationseinheit zuweisen, damit die Ziel-PCs für die Verwendung mit Remote-PC-Zugriff verfügbar sind.

    b) Erstellen Sie eine Bereitstellungsgruppe, um Benutzern Zugriff auf die PCs im Maschinenkatalog zu gewähren. Weitere Informationen zum Erstellen einer Bereitstellungsgruppe finden Sie unter Erstellen von Bereitstellungsgruppen. Stellen Sie sicher, dass Sie die Bereitstellungsgruppe einer Active Directory-Gruppe zuweisen, in der die Benutzer, die Zugriff auf ihre PCs benötigen, enthalten sind.

4. Stellen Sie den VDA auf den Büro-PCs bereit.

    - Wir empfehlen, das VDA-Kerninstallationsprogramm für Einzelsitzungs-OS (VDAWorkstationCoreSetup.exe) zu verwenden.
    - Sie können auch das vollständige VDA-Installationsprogramm für Einzelsitzungs-OS (VDAWorkstationSetup.exe) mit der Option `/remotepc` verwenden. Dadurch wird das gleiche Ergebnis erzielt, wie mit dem VDA-Kerninstallationsprogramm.
    - Erwägen Sie, die Windows-Remoteunterstützung zu aktivieren, damit Helpdeskteams Remotesupport über Citrix Director bereitstellen können. Verwenden Sie dazu die Option `/enable_remote_assistance`. Weitere Informationen finden Sie unter Installieren über die Befehlszeile.
    - Um Informationen zur Anmeldedauer in Director anzuzeigen, müssen Sie das vollständige VDA-Installationsprogramm für Einzelsitzungs-OS verwenden und die Komponente **Citrix User Profile Manager WMI Plug-In** installieren. Schließen Sie diese Komponente mit der Option `/includeadditional` ein. Weitere Informationen finden Sie unter Installieren über die Befehlszeile.
    - Informationen zum Bereitstellen des VDA mit SCCM finden Sie unter Installieren von VDAs mit SCCM.
    - Informationen zum Bereitstellen des VDA über Bereitstellungsskripts finden Sie unter Installieren von VDAs mit Skripts.

    Nachdem Sie die Schritte 2 bis 4 erfolgreich abgeschlossen haben, werden Benutzer automatisch ihren eigenen Computern zugewiesen, wenn sie sich lokal an den PCs anmelden.

5. Weisen Sie die Benutzer an, auf jedem Clientgerät, das sie für den Remotezugriff auf den Büro-PC verwenden, die Citrix Workspace-App herunterzuladen und zu installieren. Citrix Workspace-App ist unter `https://www.citrix.com/downloads/` und in den Anwendungsstores für unterstützte Mobilgeräte verfügbar.

Über die Registrierung verwaltete Features

> **Achtung:**
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Deaktivieren von automatischen Zuweisungen mehrerer Benutzer

Fügen Sie auf jedem Delivery Controller folgende Registrierungseinstellung hinzu:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Name: AllowMultipleRemotePCAssignments
- Typ: DWORD
- Wert: 0

Energiesparmodus (mindestens Version 7.16)

Damit eine Maschine mit Remote-PC-Zugriff in den Energiesparmodus wechseln kann, fügen Sie dem VDA folgende Registrierungseinstellung hinzu und starten die Maschine dann neu. Nach dem Neustart gelten die Energiespareinstellungen des Betriebssystems. Nach Ablauf der konfigurierten Leerlaufzeit wechselt die Maschine dann in den Energiesparmodus. Wenn die Maschine wieder reaktiviert wird, registriert sie sich erneut beim Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Name: DisableRemotePCSleepPreventer
- Typ: DWORD
- Wert: 1

Sitzungsverwaltung

Standardmäßig wird eine Remotesitzung des Benutzers automatisch getrennt, wenn ein lokaler Benutzer eine Sitzung auf dieser Maschine (durch Drücken von Strg + Alt + Entf) initiiert. Fügen Sie den folgenden Registrierungseintrag auf dem Büro-PC hinzu und starten Sie dann die Maschine neu, um diese automatische Aktion zu verhindern.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: SasNotification
- Typ: DWORD
- Wert: 1

Standardmäßig erhält der Remotebenutzer Vorzug vor dem lokalen Benutzer, wenn die Verbindungsmeldung nicht innerhalb des Timeouts quittiert wird. Verwenden Sie die folgende Einstellung, um das Verhalten zu konfigurieren:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaMode
- Typ: DWORD
- Wert:
  - 1 = Remotebenutzer wird stets bevorzugt, wenn er nicht innerhalb des Timeouts auf die Meldung reagiert. Dies ist das Standardverhalten bei nicht konfigurierter Einstellung.
  - 2 - Lokaler Benutzer wird bevorzugt.

Das Standardtimeout zum Erzwingen des Remote-PC-Zugriffsmodus liegt bei 30 Sekunden. Sie können dieses Zeitlimit konfigurieren, aber keinen Wert unter 30 Sekunden wählen. Verwenden Sie diese Registrierungseinstellung, um das Zeitlimit zu konfigurieren.

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Name: RpcaTimeout
- Typ: DWORD
- Wert: Anzahl der Sekunden für Timeout als Dezimalwert

Wenn ein Benutzer den Zugriff auf die Konsole erzwingen möchte, kann der lokale Benutzer innerhalb von 10 Sekunden zwei Mal Strg + Alt + Entf drücken, um lokal auf die Remotesitzung zuzugreifen und eine Verbindungstrennung zu erzwingen.

Wenn ein lokaler Benutzer nach der Registrierungsänderung und dem Maschinenneustart für die Anmeldung am PC Strg + Alt + Entf drückt und die Maschine von einem Remotebenutzer verwendet wird, wird dem Remotebenutzer eine Bestätigungsaufforderung angezeigt. Die Aufforderung fragt, ob die Verbindung des lokalen Benutzers zugelassen oder verweigert werden soll. Bei der Zulassung der Verbindung wird die Sitzung des Remotebenutzers getrennt.

Wake-On-LAN

Integriertes Wake-On-LAN ist nur für On-Premises-Versionen von Citrix Virtual Apps and Desktops verfügbar und erfordert Microsoft System Center Configuration Manager (SCCM).

Remote-PC-Zugriff unterstützt Wake-On-LAN, sodass physische PCs remote eingeschaltet werden können. Dieses Feature ermöglicht es Benutzern, ihre Büro-PCs ausgeschaltet zu lassen, wenn diese

nicht verwendet werden, um Energiekosten zu sparen. Außerdem ist ein Remotezugriff möglich, wenn Maschinen unabsichtlich ausgeschaltet wurden. Zum Beispiel wegen eines Stromausfalls.

Wake-On-LAN für Remote-PC-Zugriff wird von
PCs unterstützt, auf denen die Option "Wake-On-LAN"im BIOS/UEFI aktiviert ist.

SCCM und Wake-On-LAN für Remote-PC-Zugriff

Um Wake-On-LAN für Remote-PC-Zugriff zu konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den VDA bereitstellen.

- Konfigurieren Sie SCCM 2012 R2, 2016 oder 2019 innerhalb der Organisation. Stellen Sie dann den SCCM-Client auf allen Remote-PC-Zugriff-Maschinen bereit. Warten Sie, bis der geplante SCCM-Bestandszyklus ausgeführt wurde (oder erzwingen Sie das Ausführen manuell bei Bedarf).
- Für die Unterstützung von SCCM Wake Proxy bzw. Magic Packet gilt Folgendes:
  - Konfigurieren Sie Wake-On-LAN in den BIOS/UEFI-Einstellungen aller PCs.
  - Zur Unterstützung von Wake Proxy aktivieren Sie die entsprechende Option in SCCM. Für jedes Subnetz des Unternehmens mit PCs, auf denen das Wake-On-LAN-Feature für Remote-PC-Zugriff verwendet wird, müssen mindestens drei Maschinen als Sentinelmaschinen fungieren können.
  - Zur Unterstützung von Magic Packet konfigurieren Sie Netzwerkrouter und Firewalls so, dass Magic Packets entweder per subnetzgesteuertem Broadcast oder Unicast gesendet werden können.

Nach der Installation des VDAs auf Büro-PCs aktivieren oder deaktivieren Sie die Energieverwaltung beim Erstellen der Verbindung und des Maschinenkatalogs.

- Wenn Sie die Energieverwaltung für den Maschinenkatalog aktivieren, geben Sie Verbindungsdetails an, d. h. SCCM-Adresse, Anmeldeinformationen und einen Verbindungsnamen. Die Zugriffsanmeldeinformationen müssen Zugriff auf Sammlungen im Bereich und für die Rolle **Remotetoolsverantwortlicher** haben.
- Wenn Sie die Energieverwaltung nicht aktivieren, können Sie später eine Energieverwaltungsverbindung (Configuration Manager) hinzufügen und dann den Remote-PC-Zugriff-Maschinenkatalog bearbeiten, um die Energieverwaltung zu aktivieren.

Sie können eine Energieverwaltungsverbindung zum Konfigurieren der erweiterten Einstellungen bearbeiten. Sie können Folgendes aktivieren:

- Aktivierungsproxy, der von SCCM bereitgestellt wird.
- Wake-On-LAN-Pakete (Magic Packets). Wenn Sie Wake-On-LAN-Pakete aktivieren, können Sie eine Wake-On-LAN-Übertragungsmethode auswählen: subnetzgesteuertes Broadcast oder Unicast.

Der PC verwendet AMT-Energiebefehle (sofern unterstützt) und alle aktivierten erweiterten Einstellungen. Wenn der PC keine AMT-Befehle verwendet, werden die erweiterten Einstellungen verwendet.

Problembehandlung

Diagnoseinformationen

Diagnoseinformationen zu Remote-PC-Zugriff werden in das Windows-Anwendungsereignisprotokoll geschrieben. Informationsmeldungen werden nicht eingeschränkt. Fehlermeldungen werden durch Löschen doppelter Nachrichten eingeschränkt.

- 3300 (Informationsmeldung): Maschine zum Katalog hinzugefügt
- 3301 (Informationsmeldung): Maschine der Bereitstellungsgruppe hinzugefügt
- 3302 (Informationsmeldung): Maschine dem Benutzer zugewiesen
- 3303 (Fehler): Ausnahme

Energieverwaltung

Wenn die Energieverwaltung für Remote-PC-Zugriff aktiviert ist, können Maschinen, die sich in einem anderen Subnetz als der Controller befinden, ggf. nicht per subnetzgesteuertes Broadcast gestartet werden. Wenn Sie eine subnetzübergreifende Energieverwaltung mit subnetzgesteuertem Broadcast benötigen und AMT nicht unterstützt wird, versuchen Sie es mit dem Aktivierungsproxy oder Unicast. Stellen Sie sicher, dass diese Einstellungen in den erweiterten Eigenschaften der Energieverwaltungsverbindung aktiviert sind.

Weitere Ressourcen

Im Folgenden finden Sie weitere Ressourcen für Remote-PC-Zugriff:

- Solution design guidance: Remote PC Access Design Decisions.
- Remote-PC-Zugriff-Musterarchitekturen: Referenzarchitektur für Citrix Remote-PC-Zugriff-Lösung.

App-V

August 18, 2021

Verwenden von App-V in XenApp und XenDesktop

Mit Microsoft Application Virtualization (App-V) können Sie Anwendungen als Dienste bereitstellen, aktualisieren und unterstützen. Benutzer können auf Anwendungen zugreifen, ohne sie auf ihren Geräten installieren zu müssen. App-V und Microsoft User State Virtualization (USV) ermöglichen den Zugriff auf Anwendungen und Daten unabhängig vom Standort oder von der Internetverbindung.

Die folgende Tabelle enthält eine Liste der unterstützen Versionen.

App-V	XenDesktop-/XenApp-Version	
	Delivery Controller	**VDA**
5.0 und 5.0 SP1	XenDesktop 7 bis aktuelle Version, XenApp 7.5 bis aktuelle Version	7.0 bis aktuelle Version
5.0 SP2	XenDesktop 7 bis aktuelle Version, XenApp 7.5 bis aktuelle Version	7.1 bis aktuelle Version
5.0 SP3 und 5.1	XenDesktop 7.6 bis aktuelle Version, XenApp 7.6 bis aktuelle Version	7.6.300 bis aktuelle Version
App-V unter Windows Server 2016	XenDesktop 7.12 bis aktuelle Version, XenApp 7.12 bis aktuelle Version	7.12 bis aktuelle Version

Der Offlinezugriff auf Anwendungen wird von App-V-Client nicht unterstützt. Die Unterstützung der App-V-Integration umfasst die Verwendung von SMB-Freigaben für Anwendungen. Das HTTP-Protokoll wird nicht unterstützt.

Wenn Sie mit App-V nicht vertraut sind, konsultieren Sie die Dokumentation von Microsoft. In diesem Artikel werden folgende App-V-Komponenten behandelt:

- **Verwaltungsserver**: Bietet eine zentrale Konsole zum Verwalten der App-V-Infrastruktur und stellt virtuelle Anwendungen für den App-V-Desktopclient und den Remotedesktopdienste-Client bereit. Der App-V-Verwaltungsserver führt das vom Administrator benötigte Authentifizieren, Anfordern und Bereitstellen von Sicherheit, Messungen, Überwachung und Sammeln von Daten durch. Der Server verwendet Active Directory und unterstützende Tools zum Verwalten von Benutzern und Anwendungen.
- **Veröffentlichungsserver**: Stellt App-V-Clients mit Anwendungen für bestimmte Benutzer bereit und hostet das virtuelle Anwendungspaket für das Streaming. Die Pakete werden vom Verwaltungsserver abgerufen.

- **Client**: Ruft virtuelle Anwendungen ab, veröffentlicht die Anwendungen auf dem Client und erstellt und verwaltet automatisch virtuelle Umgebungen zur Laufzeit auf Windows-Geräten. Der App-V-Client wird auf dem VDA installiert und speichert dort in jedem Benutzerprofil benutzerspezifische Einstellungen für virtuelle Anwendungen, z. B. Registrierungs- und Dateiänderungen.

Anwendungen sind nahtlos verfügbar, ohne dass Vorkonfigurationen oder Änderungen an den Einstellungen des Betriebssystems vorgenommen werden müssen. Sie können App-V-Anwendungen von Serverbetriebssystem- und Desktopbetriebssystem-Bereitstellungsgruppen starten:

- Über Citrix Receiver
- Vom Startmenü
- Über den App-V-Client und Citrix Receiver
- Gleichzeitig von mehreren Benutzern auf mehreren Geräten
- Über Citrix StoreFront

Geänderte App-V-Anwendungseigenschaften werden implementiert, wenn die Anwendung gestartet wird. Beispiel: Bei Anwendungen mit einem geänderten Anzeigenamen oder einem angepassten Symbol wird die Modifikation angezeigt, wenn Benutzer die Anwendung starten.

Verwaltungsmethoden

Sie können mit dem App-V Sequencer erstellte und auf einem App-V-Server oder einer Netzwerkfreigabe gehostete App-V-Pakete verwenden.

- **App-V-Server:** Die Verwendung von Anwendungen aus Paketen auf App-V-Servern erfordert eine ständige Verbindung zwischen Studio und App-V-Server für Ermittlung, Konfiguration und Download auf die VDAs. Dies ist mit Hardware-, Infrastruktur- und Verwaltungsaufwand verbunden. Studio und App-V-Server müssen insbesondere für die Benutzerberechtigungen immer synchronisiert bleiben.

  Diese Methode wird als *duale Verwaltung* bezeichnet, da der Zugriff auf App-V-Pakete und -Anwendungen sowohl die Studio- als auch die App-V-Serverkonsole erfordert. Die Methode funktioniert besten in gekoppelten App-V-/Citrix Bereitstellungen.

- **Netzwerkfreigabe:** Werden Pakete in Netzwerkfreigaben gespeichert, ist Studio nicht von der App-V-Server- und Datenbankinfrastruktur abhängig, wodurch sich der entsprechende Aufwand verringert. (Sie müssen den Microsoft App-V-Client auf jedem VDA installieren.)

  Diese Methode wird als *Einzelverwaltung* bezeichnet, da die Verwendung von App-V-Paketen und -Anwendungen nur die Studiokonsole erfordert. Sie navigieren zu der Netzwerkfreigabe und fügen App-V-Pakete von dort der Anwendungsbibliothek auf Siteebene hinzu.

"Anwendungsbibliothek"bezeichnet bei Citrix ein Cachingrepository für Informationen zu App-V-Paketen. In der Anwendungsbibliothek werden auch Informationen für andere Citrix Technologien zur Anwendungsbereitstellung gespeichert.

Sie können eine Verwaltungsmethode verwenden oder beide parallel. Das heißt, wenn Sie Bereitstellungsgruppen Anwendungen hinzufügen, dürfen diese aus App-V-Paketen auf App-V-Servern und/oder in einer Netzwerkfreigabe stammen.

Wenn Sie **Konfiguration > App-V-Veröffentlichung** im Navigationsbereich von Studio wählen, werden App-V-Paketnamen und -quellen angezeigt. In der Spalte "Quelle"wird angegeben, ob die Pakete auf dem App-V-Server oder in der Anwendungsbibliothek gespeichert sind. Wenn Sie ein Paket auswählen, werden im Detailbereich die Anwendungen im Paket angezeigt.

Lastausgleich für App-V-Server

Der Lastausgleich für Verwaltungs- und Veröffentlichungsserver per DNS-Roundrobin wird unterstützt, sofern Sie die duale Verwaltung verwenden. Ein Lastausgleich für den Verwaltungsserver hinter einer virtuellen Netscaler-, F5- (oder ähnlich) IP wird aufgrund der Art und Weise der Kommunikation zwischen Studio und dem Verwaltungsserver über die Remote-PowerShell nicht unterstützt. Weitere Informationen finden Sie in diesem Citrix Blogbeitrag.

Isolationsgruppen

Wenn Sie die App-V-Einzelverwaltung einsetzen, können Sie über Isolationsgruppen Gruppen untereinander abhängiger Anwendungen festlegen, die in der Sandbox ausgeführt werden müssen. Diese ähneln den App-V-Verbindungsgruppen, sind jedoch nicht mit diesen identisch. Anstelle der in App-V-Verwaltungsserver für Pakete verwendeten Begriffe "verbindlich"und "optional"verwendet Citrix zur Beschreibung der Paketbereitstellungsoptionen "automatisch"und "explizit".

- Wenn ein Benutzer eine App-V-Anwendung (primäre Anwendung) startet, werden die Isolationsgruppen nach anderen Anwendungspaketen durchsucht, die zum automatischen Einschließen gekennzeichnet sind. Diese Pakete werden automatisch heruntergeladen und in der Isolierungsgruppe eingeschlossen. Sie müssen sie nicht der Bereitstellungsgruppe hinzufügen, die die primäre Anwendung enthält.
- Ein als "explizit"gekennzeichnetes Anwendungspaket in der Isolationsgruppe wird nur heruntergeladen, wenn Sie es derselben Bereitstellungsgruppe hinzugefügt haben, die die primäre Anwendung enthält.

Auf diese Weise können Sie Isolationsgruppen mit automatisch enthaltenen Anwendungen zur globalen Bereitstellung für alle Benutzer erstellen. Eine solche Gruppe kann zudem Plug-Ins und andere Anwendungen enthalten (etwa mit bestimmten Lizenzeinschränkungen), die Sie auf eine bestimmte,

über Bereitstellungsgruppen festgelegte Benutzergruppe beschränken möchten, ohne dass Sie zusätzliche Isolationsgruppen erstellen müssen.

Beispiel: Anwendung A erfordert zur Ausführung JRE 1.7. Sie können eine Isolationsgruppe mit Anwendung A mit expliziter Bereitstellung und JRE 1.7 mit automatischer Bereitstellung erstellen. Die App-V-Pakete fügen Sie anschließend einer oder mehreren Bereitstellungsgruppen hinzu. Wenn ein Benutzer Anwendung A startet, wird auch JRE 1.7 automatisch bereitgestellt.

Sie können eine Anwendung mehreren App-V-Isolationsgruppen hinzufügen. Wenn ein Benutzer die Anwendung startet, wird allerdings immer die erste Isolationsgruppe, der die Anwendung hinzugefügt wurde, verwendet. Sie können die Reihenfolge anderer Isolationsgruppen mit dieser Anwendung nicht ändern oder diese priorisieren.

Einrichtung

Die folgende Tabelle enthält die Reihenfolge der Setupaufgaben zur Verwendung von App-V in XenApp und XenDesktop.

Einzelverwaltung	Duale Verwaltung	Aufgabe
X	X	Bereitstellen von App-V
X	X	Bereitstellen von Paketen
	X	Konfigurieren von App-V-Serveradressen in Studio
X	X	Installieren von Software auf VDA-Maschinen
X		Hinzufügen von App-V-Paketen zur Anwendungsbibliothek
X		Hinzufügen von App-V-Isolationsgruppen (optional)
X	X	Hinzufügen von App-V-Anwendungen zu Bereitstellungsgruppen

Bereitstellen von Microsoft App-V

Anweisungen zur App-V-Bereitstellung finden Sie unter https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/?redirectedfrom=MSDN.

Optional können Sie die Einstellungen des App-V-Veröffentlichungsservers ändern. Citrix empfiehlt die Verwendung der SDK-Cmdlets auf dem Controller. Weitere Informationen finden Sie in der SDK-Dokumentation.

- Zum Anzeigen der Einstellungen des Veröffentlichungsservers geben Sie **Get-CtxAppvServerSetting -AppVPublishingServer <*pubServer*>** ein.
- Um sicherzustellen, dass App-V-Anwendungen richtig gestartet werden, geben Sie **Set-CtxAppvServerSetting –UserRefreshonLogon 0** ein.

Wenn Sie zuvor GPO-Richtlinieneinstellungen für die Verwaltung der Veröffentlichungsservereinstellungen verwendet haben, werden die App-V-Integrationseinstellungen einschließlich Cmdlet-Einstellungen von den GPO-Einstellungen außer Kraft gesetzt. Dies kann dazu führen, dass der Start von App-V-Anwendungen fehlschlägt. Citrix empfiehlt, dass Sie alle GPO-Richtlinieneinstellungen entfernen und diese Einstellungen dann mit dem SDK konfigurieren.

Bereitstellen von Paketen

Erstellen Sie bei beiden Verwaltungsmethoden Anwendungspakete mit dem App-V Sequencer. Weitere Informationen hierzu finden Sie in der Microsoft Dokumentation.

- Für die Einzelverwaltung stellen Sie die Pakete an einem freigegebenen UNC- oder SMB-Speicherort im Netzwerk zur Verfügung. Stellen Sie sicher, dass der Studio-Administrator, der den Bereitstellungsgruppen Anwendungen hinzufügt, zumindest Lesezugriff auf diesen Speicherort hat.
- Für die duale Verwaltung veröffentlichen Sie die Pakete auf dem App-V-Verwaltungsserver an einem UNC-Pfad. (Die Veröffentlichung über HTTP-URLs wird nicht unterstützt.)

Unabhängig davon, ob die Pakete auf dem App-V-Server oder in einer Netzwerkfreigabe sind, stellen Sie sicher, dass ihre Sicherheitsberechtigungen den Zugriff durch den Studio-Administrator gestatten. Netzwerkfreigaben müssen für "Authentifizierte Benutzer"freigegeben sein, damit der VDA und Studio standardmäßig Lesezugriff haben.

Konfigurieren von App-V-Serveradressen in Studio

> **Wichtig:**
>
> Citrix empfiehlt die Verwendung von PowerShell auf dem Controller zum Festlegen von App-V-Serveradressen für Server, die keine Standardwerte verwenden. Weitere Informationen finden Sie in der SDK-Dokumentation. Wenn Sie App-V-Serveradressen in Studio ändern, werden möglicherweise einige der von Ihnen angegebenen Serververbindungseigenschaften auf die Standardwerte zurückgesetzt. Diese Eigenschaften werden auf den VDAs für die Verbindung mit App-V-Veröffentlichungsservern verwendet. Konfigurieren Sie in diesem Fall

> die fälschlicherweise zurückgesetzten Eigenschaften auf den Servern erneut.

Diese Vorgehensweise gilt nur für die duale Verwaltung.

Geben Sie für die duale Verwaltung die Adressen von App-V-Verwaltungsserver und -Veröffentlichungsserver während oder nach der Erstellung der Site an. Sie können dies während oder nach dem Erstellen der Site tun.

Während der Siteerstellung:

- Geben Sie auf der Seite **App-V** des Assistenten die URL für den Microsoft App-V-Verwaltungsserver und die URL und Portnummer des App-V-Veröffentlichungsservers ein. Testen Sie die Verbindung, bevor Sie mit dem Assistenten fortfahren. Wenn der Test fehlschlägt, konsultieren Sie den Abschnitt "Problembehandlung"weiter unten.

Nach der Siteerstellung:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > App-V-Veröffentlichung**.
2. Wenn Sie noch keine App-V-Serveradressen angegeben haben, wählen Sie im Aktionsbereich **Microsoft Server hinzufügen**.
3. Zum Ändern der App-V-Serveradressen wählen Sie **Microsoft Server bearbeiten** im Aktionsbereich.
4. Geben Sie die URL für den Microsoft App-V-Verwaltungsserver und die URL und Portnummer des App-V-Veröffentlichungsservers ein.
5. Testen Sie die Verbindung mit diesen Servern, bevor Sie das Dialogfeld schließen. Wenn der Test fehlschlägt, konsultieren Sie den Abschnitt "Problembehandlung"weiter unten.

Wenn Sie später alle Verbindungen mit App-V-Verwaltungsserver und -Veröffentlichungsserver entfernen möchten, damit Studio keine App-V-Pakete auf diesen Servern mehr ermittelt, wählen Sie im Aktionsbereich die Option **Microsoft Server entfernen**. Diese Aktion ist nur zulässig, wenn gerade keine Anwendungen in Paketen auf diesen Servern in einer Bereitstellungsgruppe veröffentlicht sind. Ist dies der Fall, müssen Sie die Anwendungen zuerst von den Bereitstellungsgruppen entfernen, bevor Sie die App-V-Server entfernen können.

Installieren von Software auf VDA-Maschinen

Auf Maschinen mit VDAs müssen zur Unterstützung von App-V zwei Softwareanwendungen installiert sein: eine von Microsoft und eine von Citrix.

Microsoft App-V-Client Diese Anwendung ruft virtuelle Anwendungen ab, veröffentlicht die Anwendungen auf dem Client und erstellt und verwaltet automatisch virtuelle Umgebungen zur Laufzeit auf Windows-Geräten. Der App-V-Client speichert benutzerspezifische virtuelle Anwendungseinstellungen, wie Registrierungs- und Dateiänderungen, in den Benutzerprofilen.

Der App-V-Client ist bei Microsoft erhältlich. Installieren Sie den Client auf jeder Maschine mit einem VDA oder auf dem Masterimage, das in einem Maschinenkatalog zum Erstellen von VMs verwendet wird. **Hinweis**: Windows Server 2016 und Windows 10 (1607 oder höher) enthalten bereits den App-V-Client. Bei diesen Betriebssystemen können Sie den App-V-Client aktivieren, indem Sie das PowerShell-Cmdlet **Enable-AppV** (ohne Parameter) ausführen. Das Cmdlet **Get-AppVStatus** ruft den aktuellen Aktivierungsstatus ab.

Tipp: Nach der Installation des App-V-Clients mit Administratorberechtigungen führen Sie das PowerShell-Cmdlet **Get-AppvClientConfiguration** aus und vergewissern Sie sich, dass "EnablePackageScripts"auf 1 gesetzt ist. Wenn es nicht auf "1"gesetzt ist, führen Sie **Set-AppvClientConfiguration -EnablePackageScripts $true** aus.

Citrix App-V-Komponenten Die Citrix Software für App-V wird mit der Installation eines VDAs standardmäßig installiert und aktiviert.

Sie können diese Standardaktion während der Installation steuern. Deaktivieren Sie auf der grafischen Oberfläche das Kontrollkästchen **Citrix Personalisierung für App-V - VDA** auf der Seite **Zusätzliche Komponenten**. Verwenden Sie in der Befehlszeilenschnittstelle die Option **/exclude "Citrix Personalization for App-V - VDA"**.

Wenn Sie die Installation der Citrix App-V-Komponenten bei der VDA-Installation deaktiviert haben und später App-V-Anwendungen verwenden möchten, klicken Sie in der Liste "Programme und Funktionen"der Windows-Maschine mit der rechten Maustaste auf den Eintrag **Citrix Virtual Delivery Agent** und dann auf **Ändern**. Ein Assistent wird gestartet. Aktivieren Sie in dem Assistenten die Option zum Installieren und Aktivieren der App-V-Veröffentlichungskomponenten.

Hinzufügen oder Entfernen von App-V-Paketen zur bzw. aus der Anwendungsbibliothek

Diese Vorgehensweisen gelten nur für die Einzelverwaltung.

Sie müssen mindestens Lesezugriff auf die Netzwerkfreigabe mit den App-V-Paketen haben.

Hinzufügen von App-V-Paketen zur Anwendungsbibliothek

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > App-V-Veröffentlichung**.
2. Wählen Sie im Aktionsbereich **Pakete hinzufügen**.
3. Navigieren Sie zu der Freigabe mit den App-V-Paketen und wählen Sie ein oder mehrere Pakete aus.
4. Klicken Sie auf **Hinzufügen**.

Entfernen von App-V-Paketen aus der Anwendungsbibliothek Durch das Entfernen eines App-V-Pakets aus der Anwendungsbibliothek wird es aus dem Knoten "App-V-Veröffentlichung"von Studio entfernt. Die zugehörigen Anwendungen werden jedoch nicht aus den Bereitstellungsgruppen entfernt und können weiterhin gestartet werden. Das Paket verbleibt an dem Speicherort im Netzwerk. (Dies unterscheidet sich vom Entfernen einer App-V-Anwendung aus einer Bereitstellungsgruppe.)

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > App-V-Veröffentlichung**.
2. Wählen Sie ein oder mehrere Pakete zum Entfernen aus.
3. Wählen Sie im Aktionsbereich **Paket entfernen**.

Hinzufügen, Bearbeiten und Entfernen von App-V-Isolationsgruppen

Hinzufügen von App-V-Isolationsgruppen

1. Wählen Sie im Studio-Navigationsbereich **App-V-Veröffentlichung**.
2. Wählen Sie im Aktionsbereich **Isolationsgruppe hinzufügen**.
3. Geben Sie im Dialogfeld **Isolationsgruppeneinstellungen hinzufügen** einen Namen und eine Beschreibung für die Isolationsgruppe ein.
4. Wählen Sie in der Liste "Verfügbare Pakete"die Anwendungen aus, die Sie der Isolationsgruppe hinzufügen möchten, und klicken Sie dann auf den nach rechts weisenden Pfeil. Die ausgewählten Anwendungen werden jetzt in der Liste der Pakete in der Isolationsgruppe angezeigt. Wählen Sie in der Dropdownliste **Bereitstellung** neben jeder Anwendung **Explizit** oder **Automatisch**. Sie können auch mit den Pfeilschaltflächen die Reihenfolge der Anwendungen in der Liste ändern.
5. Wenn Sie fertig sind, klicken Sie auf **OK**.

Hinzufügen von App-V-Isolationsgruppen

1. Wählen Sie im Studio-Navigationsbereich **App-V-Veröffentlichung**.
2. Wählen Sie die Registerkarte **Isolationsgruppen** im mittleren Bereich und dann die gewünschte Isolationsgruppe.
3. Wählen Sie im Aktionsbereich **Isolationsgruppe bearbeiten**.
4. Ändern Sie im Dialogfeld **Isolationsgruppe bearbeiten** den Namen oder die Beschreibung der Isolationsgruppe, fügen Sie Anwendungen hinzu oder entfernen Sie sie oder ändern Sie den Bereitstellungstyp oder die Reihenfolge der Anwendungen.
5. Wenn Sie fertig sind, klicken Sie auf **OK**.

Entfernen von App-V-Isolationsgruppen Durch Entfernen einer Isolationsgruppe werden keine Anwendungspakete entfernt. Es wird nur die Gruppierung entfernt.

1. Wählen Sie im Studio-Navigationsbereich **App-V-Veröffentlichung**.

2. Wählen Sie die Registerkarte **Isolationsgruppen** im mittleren Bereich und dann die gewünschte Isolationsgruppe.
3. Wählen Sie im Aktionsbereich **Isolationsgruppe entfernen**.
4. Bestätigen Sie das Entfernen.

Hinzufügen von App-V-Anwendungen zu Bereitstellungsgruppen

Nachfolgend wird das Hinzufügen von App-V-Anwendungen zu Bereitstellungsgruppen behandelt. Detaillierte Informationen zum Erstellen von Bereitstellungsgruppen finden Sie unter Erstellen von Bereitstellungsgruppen.

Schritt 1: Geben Sie an, ob Sie eine neue Bereitstellungsgruppe erstellen oder App-V-Anwendungen einer vorhandenen Bereitstellungsgruppe hinzufügen möchten:

Bereitstellungsgruppe für App-V-Anwendungen erstellen:

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie im Aktionsbereich **Bereitstellungsgruppe erstellen**.
3. Geben Sie auf den Seiten des Assistenten einen Maschinenkatalog und Benutzer an.

App-V-Anwendungen einer vorhandenen Bereitstellungsgruppe hinzufügen:

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im Aktionsbereich **Anwendungen hinzufügen**.
3. Wählen Sie eine oder mehrere Bereitstellungsgruppen für die App-V-Anwendungen.

Schritt 2: Klicken Sie auf der Seite **Anwendungen** des Assistenten auf die Dropdownliste **Hinzufügen**, um Anwendungsquellen anzuzeigen. Wählen Sie **App-V**.

Schritt 3: Klicken Sie auf den Seite **App-V-Anwendungen hinzufügen** die App-V-Quelle: App-V-Server oder die Anwendungsbibliothek. Es werden nun die Anwendungsnamen mit den Paketnamen und -versionen angezeigt. Aktivieren Sie die Kontrollkästchen der Programme, die Sie hinzufügen möchten. Klicken Sie dann auf **OK**.

Schritt 4: Schließen Sie den Assistenten ab.

Nützliche Info:

- Wenn Sie beim Hinzufügen einer App-V-Anwendung zu einer Bereitstellungsgruppe die Eigenschaften der Anwendung ändern, treten die Änderungen beim Starten der Anwendung in Kraft. Wenn Sie beispielsweise den Anzeigenamen oder das Symbol einer Anwendung ändern, erscheinen die geänderten Elemente, wenn ein Benutzer die Anwendung startet.
- Wenn Sie später den Bereitstellungstyp einer Bereitstellungsgruppe mit App-V-Anwendungen von Desktops und Anwendungen auf Anwendungen ändern, ändert sich die Leistung der App-V-Anwendungen nicht.

- Wenn Sie ein zuvor veröffentlichtes (einzeln verwaltetes) App-V-Paket aus einer Bereitstellungsgruppe entfernen, versuchen die Citrix App-V-Clientkomponenten, Pakete, die nicht weiter von der Einzelverwaltung verwendet werden, zu bereinigen, die Veröffentlichung aufzuheben und die Pakete zu entfernen.
- In einer Hybridbereitstellung mit Einzelverwaltung und einem App-V-Veröffentlichungsserver, der per Dualverwaltung oder einen anderen Mechanismus (z. B. durch Gruppenrichtlinien) verwaltet wird, ist es nicht möglich festzustellen, welche (jetzt potenziell redundanten) Pakete aus welcher Quelle stammen. In diesem Fall wird keine Bereinigung durchgeführt.
- Wenn Sie keinen Veröffentlichungsserver verwenden, es aber auf dem VDA Pakete gibt, die durch einen anderen Mechanismus verwaltet werden (z. B. SCCM, benutzerdefinierte Skripts oder die App-V-Verwaltungslösung eines Drittanbieters), werden durch die Bereinigungsroutinen eventuell Pakete entfernt, die noch gebraucht werden. Fügen Sie in einem solchen Szenario eine Pseudoregistrierung eines App-V-Verwaltungsservers zum VDA hinzu, um die Bereinigung zu verhindern.

Problembehandlung

Probleme, die nur bei Verwendung der dualen Verwaltung auftreten können, sind mit "(DUAL)" gekennzeichnet.

(DUAL) Wenn Sie **Konfiguration > App-V-Veröffentlichung** im Studio-Navigationsbereich wählen, tritt ein PowerShell-Verbindungsfehler auf.

- Ist der Studio-Administrator gleichzeitig App-V-Serveradministrator? Der Studio-Administrator muss auf dem App-V-Verwaltungsserver zu der Administratorengruppe gehören, um mit diesem kommunizieren können.

(DUAL) Wenn Sie App-V-Serveradressen in Studio angeben tritt beim Testen der Verbindung ein Fehler auf.

- Wurde der App-V-Server hochgefahren? Senden Sie entweder einen Ping-Befehl oder prüfen Sie die IIS-Verwaltung. Jeder App-V-Server muss den Zustand "Gestartet"und "Ausgeführt"haben.
- Ist auf dem App-V-Server PowerShell-Remoting aktiviert? Falls nicht, konsultieren Sie https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)?redirectedfrom=MSDN.
- Ist der Studio-Administrator gleichzeitig App-V-Serveradministrator? Der Studio-Administrator muss auf dem App-V-Verwaltungsserver zu der Administratorengruppe gehören, um mit diesem kommunizieren können.
- Ist auf dem App-V-Server die Dateifreigabe aktiviert? Geben Sie in Windows Explorer oder über den Befehl "Ausführen"***<App-V-Server-FQDN>*** ein.

- Hat der App-V-Server dieselben Dateifreigabeberechtigungen wie der App-V-Administrator? Fügen Sie auf dem App-V-Server für \\<*App-V-Server-FQDN*> unter "Gespeicherte Benutzernamen und Kennwörter"einen Eintrag mit den Anmeldeinformationen des Benutzers ein, der Administratorberechtigungen auf dem App-V-Server hat. Erläuterungen finden Sie unter https://support.microsoft.com/kb/306541.
- Ist der App-V-Server in Active Directory?

  Sind Studio-Maschine und App-V-Server in verschiedenen Active Directory-Domänen, zwischen denen keine Vertrauensbeziehung besteht, führen Sie über die PowerShell-Konsole auf der Studio-Maschine **winrm s winrm/Config/client '@(TrustedHosts="*<App-V-Server FQDN>*")'** aus.

  Wird "TrustedHosts"über das Gruppenrichtlinienobjekt verwaltet, wird eine Fehlermeldung angezeigt, die besagt, dass die Konfigurationseinstellung "TrustedHosts"nicht geändert werden kann, da sie von Richtlinien gesteuert wird, The policy would need to be set to Not Configured to change the config setting."In diesem Fall fügen Sie einen Eintrag für den App-V-Servernamen in der TrustedHosts-Richtlinie im Gruppenrichtlinienobjekt hinzu (**Administrative Vorlagen > Windows-Komponenten > Windows-Remoteverwaltung (WinRM) > WinRM-Client**).

(DUAL) Discovery schlägt beim Hinzufügen einer App-V-Anwendung zu einer Bereitstellungsgruppe fehl.

- Ist der Studio-Administrator gleichzeitig Administrator des App-V-Verwaltungsservers? Der Studio-Administrator muss auf dem App-V-Verwaltungsserver zu der Administratorengruppe gehören, um mit diesem kommunizieren können.
- Wird der App-V-Verwaltungsserver ausgeführt? Senden Sie entweder einen Ping-Befehl oder prüfen Sie die IIS-Verwaltung. Jeder App-V-Server muss den Zustand "Gestartet"und "Ausgeführt"haben.
- Ist PowerShell-Remoting auf beiden App-V-Servern aktiviert? Falls nicht, konsultieren Sie https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)?redirectedfrom=MSDN.
- Haben die Pakete die richtigen Sicherheitsberechtigungen, sodass der Studio-Administrator Zugriff hat?

App-V-Anwendungen werden nicht gestartet.

- (DUAL) Wird der Veröffentlichungsserver ausgeführt?
- (DUAL) Haben die App-V-Pakete die richtigen Sicherheitsberechtigungen, sodass Benutzer Zugriff haben?
- (DUAL) Stellen Sie auf dem VDA sicher, dass "Temp"auf den richtigen Speicherort verweist und dass genügend Speicherplatz im Verzeichnis "Temp"ist.

- (DUAL) Führen Sie auf dem App-V-Veröffentlichungsserver `Get-AppvPublishingServer \*` aus, damit die Liste der Veröffentlichungsserver angezeigt wird.
- (DUAL) Stellen Sie sicher, dass auf dem App-V-Veröffentlichungsserver "UserRefreshonLogon" auf "False"festgelegt ist.
- (DUAL) Führen Sie auf dem App-V-Veröffentlichungsserver als Administrator **Set-AppvPublishingServer** aus und stellen Sie "UserRefreshonLogon"auf "False"ein.
- Ist auf dem VDA eine unterstützte Version des App-V-Clients installiert? Ist auf dem VDA die Einstellung "enable package scripts"aktiviert?
- Rufen Sie auf der Maschine mit dem App-V-Client und dem VDA im Registrierungseditor (regedit) den Eintrag "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV"auf. Stellen Sie sicher, dass der Schlüssel "AppVServers"den folgenden Wert hat: AppVManagementServer+metadata;PublishingServer (zum Beispiel: `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082`).
- Prüfen Sie auf der Maschine bzw. dem Masterimage mit dem App-V Client und dem VDA, ob "PowerShell ExecutionPolicy"auf "RemoteSigned"festgelegt ist. Das von Microsoft zur Verfügung gestellte App-V-Clientmodul ist nicht signiert. Mit dieser ExecutionPolicy-Einstellung kann PowerShell unsignierte lokale Skripts und Cmdlets ausführen. Stellen Sie "ExecutionPolicy"mit einer der folgenden Methoden ein: (1) Führen Sie als Administrator das Cmdlet **Set-ExecutionPolicy RemoteSigned** aus oder (2) navigieren Sie in den Gruppenrichtlinieneinstellungen zu **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Windows PowerShell > Skriptausführung aktivieren**.

Wenn Sie mit diesen Schritten die Probleme nicht beheben können, aktivieren und prüfen Sie die Protokolle.

Protokolle

Mit App-V zusammenhängende Protokolle sind im Ordner "C:\CtxAppvLogs". Die Anwendungsstartprotokolle sind im Ordner "%LOCALAPPDATA%\Citrix\CtxAppvLogs". LOCALAPPDATA wird in den lokalen Ordner des angemeldeten Benutzers aufgelöst. Prüfen Sie den lokalen Ordner des Benutzers, bei dem der Anwendungsstart fehlgeschlagen ist.

Zum Aktivieren der für App-V verwendeten Studio- und VDA-Protokolle müssen Sie Administratorberechtigung haben. Sie benötigen außerdem einen Texteditor (z. B. Editor).

Aktivieren von Studio-Protokollen

1. Erstellen Sie den Ordner C:\CtxAppvLogs.
2. Gehen Sie zu C:\Programme\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Öffnen Sie CtxAppvCommon.dll.config in einem Texteditor und heben Sie die Auskommentierung der Zeile "<add key ="LogFileName"value="C:\CtxAppvLogs\log.txt"/>"auf.

3. Starten Sie den Brokerdienst neu, um die Protokollierung zu starten.

Aktivieren von VDA-Protokollen

1. Erstellen Sie den Ordner C:\CtxAppvLogs.
2. Gehen Sie zu C:\Programme\Citrix\Virtual Desktop Agent. Öffnen Sie CtxAppvCommon.dll.config in einem Texteditor und heben Sie die Auskommentierung der Zeile ‘‘<add key =’’LogFileName’’value=’’C:\CtxAppvLogs\log.txt’’/>’’auf.
3. Heben Sie die Auskommentierung der folgenden Zeile auf und stellen Sie den Wert auf 1 ein: <add key =’’EnableLauncherLogs’’value=’’1’’/>
4. Starten Sie die Maschine neu, um die Protokollierung zu starten.

AppDisks

August 18, 2021

Übersicht

Die Verwaltung von Anwendungen und der Images, auf denen sie installiert sind, ist nicht unbedingt einfach. Das Citrix Feature AppDisks ist hier eine gute Lösung. AppDisks trennen Anwendungen und Anwendungsgruppen vom Betriebssystem, sodass Sie beides separat verwalten können.

Sie können verschiedene AppDisks mit den Anwendungen für einzelne Benutzergruppen erstellen und dann auf einem Masterimage Ihrer Wahl zusammenstellen. Durch eine solche Gruppierung und Verwaltung von Anwendungen haben Sie mehr Kontrolle über diese und benötigen weniger Masterimages. Dank der so vereinfachten IT-Verwaltung können Sie schneller auf die Anforderungen der Benutzer reagieren. Anwendungen in AppDisks werden über Bereitstellungsgruppen bereitgestellt.

Wenn Ihre Bereitstellung auch Citrix AppDNA enthält, kann es zusammen mit dem AppDisks-Feature verwendet werden. Mit AppDNA können in XenApp und XenDesktop Anwendungen automatisch auf AppDisk-Basis analysiert werden. Mit AppDNA können Sie die Vorzüge des AppDisks-Features optimal nutzen. Die Kompatibilität ohne AppDNA wurde weder getestet noch dokumentiert.

AppDisks unterscheiden sich von anderen Technologien zur Anwendungsbereitstellung in zweierlei Hinsicht: Isolation und Änderungsmanagement.

- Microsoft App-V ermöglicht die Koexistenz nicht kompatibler Anwendungen, indem es diese isoliert. Von AppDisks werden keine Anwendungen isoliert. Stattdessen trennt es die Anwendungen mit den zugehörigen Dateien und Registrierungsschlüsseln vom Betriebssystem. Für Betriebssystem und Benutzer verhalten sich AppDisks so, als wären sie direkt auf einem Masterimage installiert.

- Änderungsmanagement (Masterimageupdate und Testen der Kompatibilität von Updates mit installierten Anwendungen) kann erhebliche Kosten verursachen. AppDNA-Berichte helfen bei der Identifizierung von Problemen und enthalten Lösungsvorschläge. Mit AppDNA können Sie beispielsweise Anwendungen mit gemeinsamen Abhängigkeiten (.NET o. Ä.) finden und auf einem einzelnen gemeinsamen Basisimage installieren. AppDNA ermöglicht auch die Identifizierung von Anwendungen, die beim Betriebssystemstart früh geladen werden, damit Sie sicherstellen können, dass diese ordnungsgemäß funktionieren.

Nützliche Info:

- Nach einem Imageupdate können einige Anwendungen möglicherweise nicht ordnungsgemäß ausgeführt werden, da zuvor installierte Lizenzen nicht überprüft werden können. Beispielsweise kann nach einem Imageupdate beim Starten von Microsoft Office folgende Fehlermeldung angezeigt werden:

  Microsoft Office Professional Plus 2010 kann die Lizenz für diese Anwendung nicht überprüfen. Fehler bei einem Reparaturversuch oder Abbruch durch den Benutzer. Die Anwendung wird jetzt heruntergefahren.”

Um dieses Problem zu lösen, deinstallieren Sie Microsoft Office und installieren Sie die neue Version auf dem Basisimage.

- Das Herunterladen von Metro-Apps aus dem Windows Store auf eine veröffentlichte virtuelle Maschine kann lange dauern und dann fehlschlagen.
- Citrix empfiehlt, dass Sie immer alle Microsoft Office-Komponenten auf derselben AppDisk zusammenfassen. Beispiel: eine AppDisk mit Microsoft Office mit Project und eine zweite mit Microsoft Office mit Visio und Project.
- Auf einigen Systemen stürzt SCCM beim Update eines Images ab. Dies tritt ein, wenn Updates am Basisimage ausgeführt und dann angewendet werden, wodurch ein Fehler auf dem SCCM-Client verursacht wird. Installieren zur Problembehebung die SCCM-Clientinstanz zunächst auf dem Basisimage.
- In manchen Fällen wird eine auf der AppDisk installierte Anwendungen nicht im Windows-Startmenü angezeigt, nachdem sie einer Bereitstellungsgruppe und der virtuellen Maschine eines Benutzers zugewiesen wurde. Weitere Informationen finden Sie unter Anzeige von Anwendungen im Startmenü.
- Für die Benutzer bleiben die Trennung von Anwendungen vom Betriebssystem und andere Aspekte des AppDisks-Features verborgen. Die Anwendungen verhalten sich so, als wären sie auf dem Image installiert. AppDisks mit komplexen Anwendungen können beim Desktopstart eine geringe Verzögerung verursachen.
- Sie können nur AppDisks mit gehosteten, freigegebenen und gepoolten Desktops verwenden.
- Sie können AppDisks mit gehosteten, freigegebenen Desktops verwenden.
- AppDisks können theoretisch auf Anwendungsbasis masterimage- und betriebssystemüber-

greifend verwendet werden, dies ist jedoch nicht bei allen Anwendungen möglich. Bei Anwendungen mit einem Skript zur Installation auf einem Desktopbetriebssystem, welches deren Funktion auf einem Serverbetriebssystem nicht zulässt, empfiehlt Citrix die separate Verpackung der Anwendungen für jedes der beiden Betriebssysteme.

- In vielen Fällen funktionieren AppDisks auf unterschiedlichen Betriebssystemen. Sie können beispielsweise eine auf einer Windows 7-VM erstellte AppDisk einer Bereitstellungsgruppe mit Windows 2008 R2-Maschinen hinzufügen, sofern beide Betriebssysteme die gleiche Bitanzahl haben (32 oder 64) und die Anwendung unterstützen. Citrix rät allerdings davon ab, eine auf einer neueren Betriebssystemversion (z. B. Windows 10) erstellte AppDisk Bereitstellungsgruppen mit Maschinen hinzuzufügen, auf denen eine ältere Betriebssystemversion (z. B. Windows 7) ausgeführt wird, da es dadurch zu Betriebsstörungen kommen kann.
- Wenn Sie bestimmte Anwendungen auf einer AppDisk nur einer Teilgruppe von Benutzern in einer Bereitstellungsgruppe zugänglich machen möchten, empfiehlt Citrix die Verwendung der Gruppenrichtlinie, um diese Anwendungen vor den anderen Benutzern zu verbergen. Die ausführbare Datei der Anwendung steht weiterhin zur Verfügung, kann für die anderen Benutzer jedoch nicht ausgeführt werden.
- Unter Windows 7 in russischer oder chinesischer Sprache wird das Neustartdialogfeld nicht automatisch geschlossen. In diesem Fall sollte es nach der Anmeldung bei dem bereitgestellten Desktop angezeigt und schnell wieder geschlossen werden.
- Bei Verwendung des Skripttools **Upload-PvDDiags** fehlen Protokollinformationen bezüglich der PVD-Benutzerschicht, wenn die Laufwerksbezeichnung eines Benutzers nicht auf “P”festgelegt ist.
- In Umgebungen mit Sprachwahl Baskisch wird unter Windows 7 auf dem Bildschirm mit der Neustartaufforderung möglicherweise nicht die richtige Sprache angezeigt. Wenn Sie Baskisch festlegen möchten, installieren Sie zunächst Französisch oder Spanisch als übergeordnete Sprache, installieren Sie anschließend Baskisch und legen Sie es als aktuelle Sprache fest.
- Beim Herunterfahren eines Computers wird die Erinnerung zur PVD-Aktualisierung angezeigt, selbst wenn die PVD auf schreibgeschützt festgelegt ist.
- Bei direkten Upgrades kann eine Registrierungsdatei (DaFsFilter) gelöscht werden, wodurch das Upgrade fehlschlägt.

> **Tipp:**
>
> Verwenden Sie beim Erstellen einer AppDisk eine VM, auf der nur das Betriebssystem installiert ist, d. h. es sind keine anderen Apps vorhanden. Das Betriebssystem muss alle Updates enthalten, bevor Sie die AppDisk erstellen.

Übersicht über die Bereitstellung

Die folgende Liste bietet eine Übersicht über die Schritte zum Bereitstellen von AppDisks. Einzelheiten finden Sie weiter unten in diesem Artikel.

1. Installieren Sie über die Hypervisor-Verwaltungskonsole einen Virtual Delivery Agent (VDA) auf einer VM.
2. Erstellen Sie über die Hypervisor-Verwaltungskonsole und Studio eine AppDisk.
3. Installieren Sie über die Hypervisor-Verwaltungskonsole Anwendungen auf der AppDisk.
4. Versiegeln Sie die AppDisk über die Hypervisor-Verwaltungskonsole oder über Studio. Durch das Versiegeln können XenApp und XenDesktop die AppDisk-Anwendungen und die zugehörigen Dateien in einer Anwendungsbibliothek (AppLibrary) eintragen.
5. Erstellen oder bearbeiten Sie in Studio eine Bereitstellungsgruppe und wählen Sie die AppDisks für diese aus. Dieser Schritt wird als *Zuweisung von AppDisks* bezeichnet, die verwendete Aktion in Studio heißt dagegen **AppDisks verwalten**. Wenn VMs in der Bereitstellungsgruppe starten, erfolgt eine Koordinierung zwischen XenApp/XenDesktop und der AppLibrary. XenApp und XenDesktop interagieren dann mit Maschinenerstellungsdienste (MCS) oder Provisioning Services (PVS) und dem Delivery Controller zum Streamen der Startgeräte, nachdem die AppDisks auf diesen konfiguriert wurden.

Anforderungen

Neben den unter Systemanforderungen aufgeführten Anforderungen gelten zusätzliche Anforderungen für AppDisks.

AppDisks werden nur in Bereitstellungen unterstützt, in denen die Version der Delivery Controller und von Studio mindestens der im XenApp- und XenDesktop 7.8-Download entspricht, einschließlich der automatisch installierten Voraussetzungen (.NET 4.5.2 usw.).

AppDisks können auf denselben Windows-Betriebssystemversionen erstellt werden, die auch für VDAs unterstützt werden. Auf den Maschinen in Bereitstellungsgruppen, für die AppDisks verwendet werden sollen, muss mindestens Version 7.8 des VDAs installiert sein.

Citrix empfiehlt, dass Sie alle Maschinen mit der neuesten VDA-Version installieren oder aktualisieren und dann das Upgrade von Maschinenkatalogen und Bereitstellungsgruppen nach Bedarf durchführen. Wenn Sie beim Erstellen einer Bereitstellungsgruppe Maschinen mit verschiedenen VDA-Versionen auswählen, ist die resultierende Bereitstellungsgruppe kompatibel mit der ältesten VDA-Version. Dies wird als *Funktionsebene* bezeichnet. Weitere Informationen zur Funktionsebene finden Sie im Artikel Erstellen von Bereitstellungsgruppen.

Zum Bereitstellen von VMs, die zum Erstellen von AppDisks verwendet werden sollen, können Sie Folgendes verwenden:

- Mit Controllerversion 7.8 (Minimum) gelieferte Maschinenerstellungsdienste
- Auf der Downloadseite zusammen mit der verwendeten XenApp-/XenDesktop-Version verfügbare PVS-Version
- Unterstützte Hypervisors:
  - XenServer
  - VMware (mindestens Version 5.1)
  - Microsoft System Center Virtual Machine Manager

AppDisks können nicht mit anderen, für XenApp und XenDesktop unterstützten Hypervisors oder Clouddiensten verwendet werden.

Das Erstellen von AppDisks wird nicht für Maschinen in MCS-Maschinenkatalogen unterstützt, die temporäre Daten zwischenspeichern.

> **Hinweis:**
>
> Sie können AppDisks mit dem Schreibcache an Maschinen anfügen, die mit MCS bereitgestellt wurden. Diese Maschinen können jedoch nicht zum Erstellen von AppDisks verwendet werden.

Remote-PC-Zugriff-Kataloge unterstützen keine AppDisks.

Auf der zum Erstellen einer AppDisk verwendeten VM muss der Windows-Volumeschattenkopie-Dienst aktiviert sein. Der Dienst ist standardmäßig aktiviert.

Mit AppDisks verwendete Bereitstellungsgruppen dürfen Maschinen aus gepoolten zufälligen Maschinenkatalogen mit Serverbetriebssystem- oder Desktopbetriebssystemmaschinen enthalten. Sie können AppDisks nicht mit Maschinen aus anderen Katalogtypen, z. B. solchen mit gepoolten statischen oder dedizierten (zugewiesenen) Maschinen, verwenden.

Auf Maschinen, auf denen Studio installiert ist, muss zusätzlich zu anderen ggf. installierten .NET-Versionen .NET Framework 3.5 installiert sein.

AppDisks können Auswirkungen auf den Speicher haben. Weitere Informationen finden Sie unter Überlegungen zu Speicher und Leistung.

Wenn Sie AppDNA verwenden:

- Lesen Sie die AppDNA-Dokumentation und die AppDisk-FAQ.
- Die AppDNA-Software muss auf einem anderen Server als solchen mit Controller installiert werden. Verwenden Sie die mit diesem Release von XenApp und XenDesktop gelieferte AppDNA-Version. Weitere Anforderungen für AppDNA sind in der zugehörigen Dokumentation aufgeführt.
- Stellen Sie sicher, dass auf dem AppDNA-Server eine Firewallausnahme für den Standardport 8199 festgelegt ist.
- Deaktivieren Sie eine bestehende AppDNA-Verbindung beim Erstellen einer AppDisk nicht.

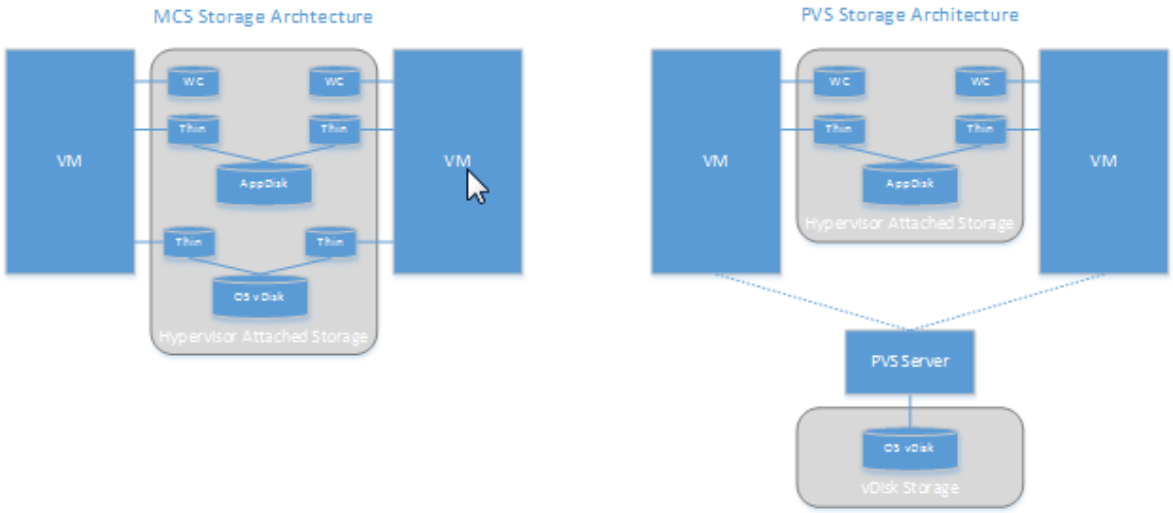
- Beim Erstellen der XenApp- bzw. XenDesktop-Site können Sie die Kompatibilitätsanalyse mit AppDNA auf der Seite **Weitere Features** des Assistenten aktivieren. Sie können diese später über **Konfiguration > AppDNA** im Navigationsbereich von Studio aktivieren oder deaktivieren.
- Durch Klicken auf den Link "Problembericht anzeigen"in Studio wird der AppDNA-Bericht aufgerufen, allerdings sind die in der Standardeinstellung von AppDNA verwendeten Betriebssystemkombinationen Windows 7 64-Bit für Desktopbereitstellungsgruppen und Windows Server 2012 R2 für Serverbereitstellungsgruppen. Wenn Ihre Bereitstellungsgruppen andere Windows-Versionen enthalten, sind die Standard-Imagekombinationen in den Studio-Berichten falsch. Bearbeiten Sie als Workaround die Lösung in AppDNA nach der Erstellung durch Studio manuell.
- Es besteht ein Abhängigkeitsverhältnis zwischen der Studio- und der AppDNA-Serverversion.
  - Ab Version 7.12 muss Studio in der gleichen (oder einer höheren) Version vorliegen wie der AppDNA-Server.
  - Bei Version 7.9 und 7.11 müssen Studio- und AppDNA-Serverversion übereinstimmen.
  - Der folgenden Tabelle ist zu entnehmen, welche Versionen zusammen funktionieren ("Ja" = funktionieren zusammen, –= funktionieren nicht zusammen):

Produktversion	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	Ja	–	–	–	–	–
AppDNA 7.11	–	Ja	–	–	–	–
AppDNA 7.12	–	–	Ja	Ja	Ja	Ja
AppDNA 7.13	–	–	Ja	Ja	Ja	Ja
AppDNA 7.14	–	–	–	–	Ja	Ja
AppDNA 7.15	–	–	–	–	–	Ja

Überlegungen zu Speicher und Leistung

Das Trennen von Anwendungen und Betriebssystem durch Verwendung zweier Datenträger und Speichern dieser Datenträger in verschiedenen Bereichen hat Auswirkungen auf die Speicherstrategie. Die folgende Abbildung zeigt die Speicherarchitektur von MCS und PVS. "WC"steht für den Schreib-

cache und “Thin”für Thin-Datenträger, die zur Speicherung der Unterschiede zwischen den AppDisks und den virtuellen Betriebssystemdatenträgern einer VM verwendet werden.



MCS-Umgebungen

- Sie die Größe der AppDisks und Betriebssystem-vDisks gemäß den im Unternehmen geltenden Größenrichtlinien wählen. Werden AppDisks von mehreren Bereitstellungsgruppen verwendet, kann die allgemeine Speicherkapazität reduziert werden.
- Da Betriebssystem-vDisks und AppDisks im gleichen Speicherbereich sind, planen Sie den Speicherbedarf sorgfältig, um negative Auswirkungen auf die Kapazität durch die Bereitstellung von AppDisks zu vermeiden. AppDisks erzeugen Mehraufwand. Stellen Sie sicher, dass der Speicher diesen und die Anwendungen abdeckt.
- Es gibt keinen Nettoeffekt auf IOPS, da Betriebssystem-vDisks und AppDisks im gleichen Speicherbereich sind. Bei Verwendung von MCS müssen keine Überlegungen in puncto Schreibcache angestellt werden.

PVS-Umgebungen

- Sie müssen eine Steigerung von Kapazität und IOPS berücksichtigen, da Anwendungen vom AppDisk-Speicher in den an den Hypervisor angeschlossenen Speicher umsiedeln.
- In PVS-Umgebungen verwenden Betriebssystem-vDisks und AppDisks verschiedene Speicherbereiche. Die Speicherkapazität von Betriebssystem-vDisks ist geringer, dafür ist der an den Hypervisor angeschlossene Speicher größer. Sie müssen die Größe Ihrer PVS-Umgebung entsprechend wählen.
- AppDisks im am Hypervisor angeschlossenen Speicher erzeugen mehr IOPS, die Betriebssystem-vDisks hingegeben weniger.

- Schreibcache: PVS verwendet eine dynamische VHDX-Datei auf einem NTFS-formatierten Laufwerk. Beim Schreiben von Blöcken in den Schreibcache wird die VHDX-Datei dynamisch erweitert. Werden AppDisks einer virtuellen Maschine angefügt, dann werden sie mit den Betriebssystem-vDisks zusammengeführt, um eine einheitliche Ansicht des Dateisystems zu ermöglichen. Beim Zusammenführen werden in der Regel zusätzliche Daten in den Schreibcache geschrieben und die Schreibcachedatei entsprechend größer. Berücksichtigen Sie dies bei der Kapazitätsplanung.

MCS- und PVS-Umgebungen: Verringern Sie die Größe der Betriebssystem-vDisks, um einen Nutzen aus der Verwendung von AppDisks zu ziehen. Wenn Sie dies nicht tun, planen Sie die Verwendung von mehr Speicher ein.

Schalten viele Benutzer in einer Site ihren Computern gleichzeitig ein (beispielsweise zum Beginn des Arbeitstags), kann die Belastung des Hypervisors durch die zahlreichen Startanforderungen sich auf die Leistung auswirken. In PVS-Umgebungen sind die Anwendungen nicht auf der Betriebssystem-vDisk, sodass weniger Anforderungen beim PVS-Server eingehen. Aufgrund der geringeren Last auf den einzelnen Zielgeräten kann der PVS-Server an mehr Ziele streamen. Eine höhere Ziel-Server-Dichte kann allerdings die Leistung bei einem Boot Storm beeinträchtigen.

Erstellen von AppDisks

Es gibt zwei Methoden zu Erstellen von AppDisks, Installieren von Anwendungen darauf und Versiegeln der AppDisks. Bei beiden Methoden wird sowohl die Hypervisor-Verwaltungskonsole als auch Studio verwendet. Die Methoden unterscheiden sich darin, wo Sie die meisten der Schritte ausführen.

Bei beiden Methoden gilt Folgendes:

- Setzen Sie für die AppDisk-Erstellung selbst 30 Minuten an.
- Wenn Sie AppDNA verwenden, befolgen Sie die Anweisungen unter Anforderungen weiter oben. Deaktivieren Sie eine bestehende AppDNA-Verbindung beim Erstellen einer AppDisk nicht.
- Beim Hinzufügen von Anwendungen zu einer AppDisk stellen Sie sicher, dass Sie die Anwendungen für alle Benutzer installieren. Führen Sie für alle Anwendungen, die die Key Management Server-Aktivierung verwenden, eine Rearm-Operation durch. Weitere Informationen finden Sie in der Anwendungsdokumentation.
- Bei der AppDisk-Erstellung an benutzerspezifischen Orten erstellte Dateien, Ordner und Registrierungseinträge werden nicht beibehalten. Bei einigen Anwendungen wird ein Ersteinsatz-Assistent zum Erstellen von Benutzerdaten während der Installation ausgeführt. Verwenden Sie eine Profilverwaltungslösung, um diese Daten zu speichern und die Anzeige des Assistenten bei jedem AppDisk-Start zu verhindern.
- Bei Verwendung von AppDNA erfolgt direkt nach der Erstellung eine automatische Analyse. Während der Analyse wird als AppDisk-Status in Studio “Analysieren”angezeigt.

Überlegungen zu PVS

AppDisks auf Maschinen aus Maschinenkatalogen, die von Provisioning Services erstellt wurden, erfordern zusätzliche Konfigurationsschritte. Führen Sie in der Provisioning Services Console die folgenden Schritte aus:

1. Erstellen Sie eine neue Version der mit der Gerätesammlung, die die VM enthält, verknüpften vDisk.
2. Setzen Sie die VM in den Wartungsmodus.
3. Wählen Sie bei der AppDisk-Erstellung bei jedem VM-Neustart auf dem Startbildschirm die Wartungsversion.
4. Nach dem Versiegeln der AppDisk versetzen Sie die VM wieder in die Produktion und löschen Sie die vDisk-Version, die Sie erstellt haben.

Erstellen einer AppDisk unter hauptsächlicher Verwendung von Studio

Dieser Vorgang umfasst drei Aufgaben: Erstellen der AppDisk, Erstellen von Anwendungen auf der AppDisk und Versiegeln der AppDisk.

Erstellen von AppDisks

1. Wählen Sie im Studio-Navigationsbereich **AppDisks** und im Aktionsbereich **AppDisk erstellen**.
2. Überprüfen Sie die Informationen auf der Seite **Einführung** des Assistenten und klicken Sie dann auf **Weiter**.
3. Aktivieren Sie auf der Seite **AppDisk erstellen** das Optionsfeld **Neue AppDisk erstellen**. Wählen Sie eine vordefinierte Datenträgergröße für die AppDisk (klein, mittel, groß) oder geben Sie die Größe in GB ein (Mindestgröße = 3 GB). Die Datenträgergröße muss für die Anwendungen ausreichen, die Sie hinzufügen möchten. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Vorbereitungsmaschine** einen Poolkatalog mit Zufallszuweisung aus, der als Masterimage für die AppDisk-Erstellung verwendet werden soll. Hinweis: Es werden alle Maschinenkataloge der Site nach Typ angezeigt, ausgewählt werden können nur solche, die mindestens eine verfügbare Maschine enthalten. Wenn Sie einen Katalog wählen, der keine zufälligen gepoolten virtuellen Maschinen enthält, schlägt die AppDisk-Erstellung fehl. Nach Auswahl einer VM aus dem Katalog klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Zusammenfassung** einen Namen und eine Beschreibung für die AppDisk ein. Überprüfen Sie die auf den vorherigen Seiten des Assistenten angegebenen Informationen. Klicken Sie auf **Fertig stellen**.

Nicht vergessen: Wenn Sie PVS verwenden, folgen Sie den Anweisungen unter "Überlegungen zu PVS"
.

Nach dem Schließen des Assistenten wird in Studio für die neue AppDisk “Wird erstellt”angezeigt. Nach der Erstellung der AppDisk ändert sich die Anzeige in “Bereit zur Installation von Anwendungen” .

Installieren von Anwendungen auf der AppDisk Installieren Sie über die Hypervisor-Verwaltungskonsole Anwendungen auf der AppDisk. (**Tipp:** Wenn Sie den Namen der VM vergessen haben, wählen Sie im Studio-Navigationsbereich **AppDisks** und dann im Aktionsbereich **Anwendungen installieren**, um den Namen anzuzeigen. Informationen zur Installation von Anwendungen finden Sie in der Dokumentation zum Hypervisor. (**Nicht vergessen:** Zum Installieren von Anwendungen auf der AppDisk verwenden Sie die Hypervisor-Verwaltungskonsole. Verwenden Sie nicht die Aufgabe Anwendungen installieren im Aktionsbereich von Studio.)

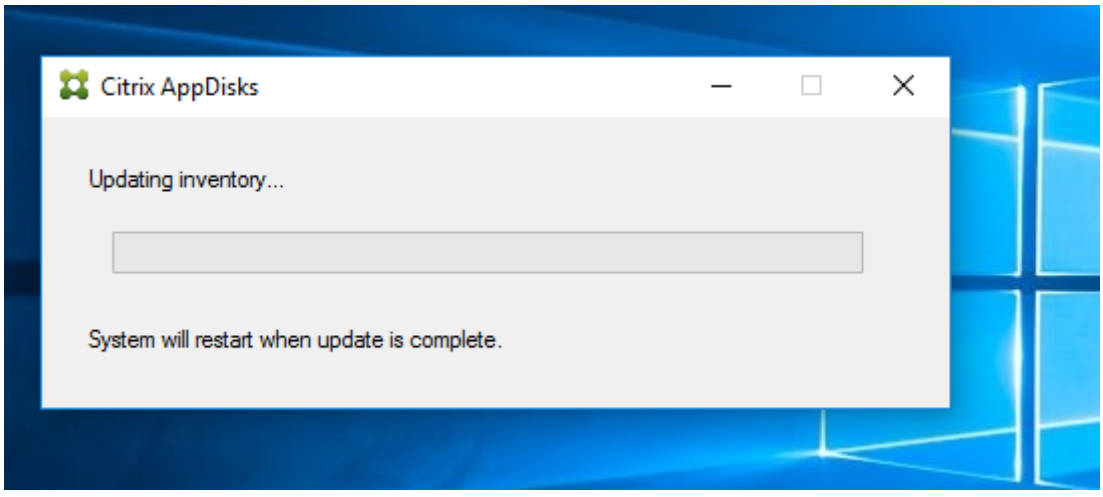
Versiegeln der AppDisk

1. Wählen Sie im Studio-Navigationsbereich **AppDisks**.
2. Wählen Sie die zuvor erstellte AppDisk und dann im Studio-Aktionsbereich **AppDisk versiegeln**.

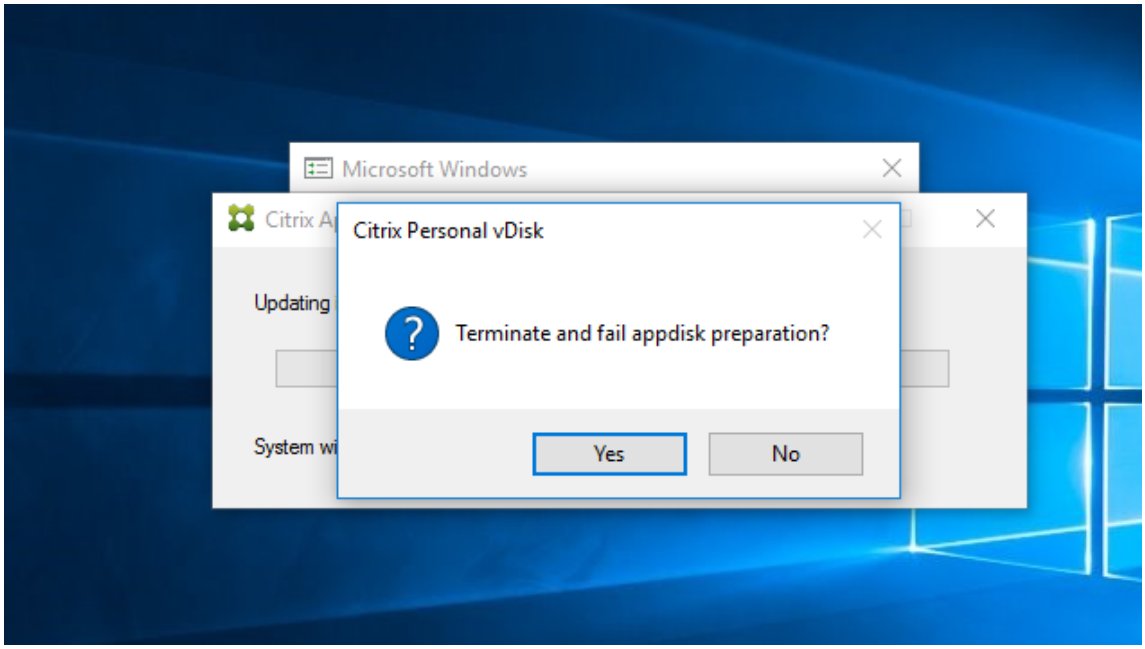
Nachdem Sie eine AppDisk erstellt, Anwendungen darauf installiert und die AppDisk versiegelt haben, weisen Sie sie einer Bereitstellungsgruppe zu.

Abbrechen der AppDisk-Vorbereitung und -Versiegelung In einigen Fällen muss der Administrator die AppDisk-Erstellung oder Versiegelung möglicherweise abbrechen:

1. Greifen Sie auf die VM zu.
2. Schließen Sie das Dialogfeld:



3. Nachdem Sie das Dialogfeld geschlossen haben, wird eine Meldung angezeigt, die Sie zur Bestätigung des Abbruchs auffordert. Klicken Sie auf **Ja**.



> **Hinweis:**
>
> Wenn Sie die AppDisk-Vorbereitung abbrechen, wird die Maschine durch einen Neustart in den ursprünglichen Zustand zurückversetzt. Andernfalls müssen Sie eine saubere VM erstellen.

Erstellen einer AppDisk auf dem Hypervisor und importieren der AppDisk in Studio

Bei diesem Verfahren erstellen Sie die AppDisk über die Hypervisor-Verwaltungskonsole und importieren sie anschließend in Studio.

Erstellen einer AppDisk, Installieren von Anwendungen und Versiegeln der AppDisk auf dem Hypervisor

1. Erstellen Sie über die Hypervisor-Verwaltungskonsole eine VM und installieren Sie einen VDA.
2. Fahren Sie die Maschine herunter und erstellen Sie einen Snapshot von ihr.
3. Erstellen Sie mit dem Snapshot eine neue Maschine und fügen Sie dieser einen neuen Datenträger hinzu. Der Datenträger (der später zur AppDisk wird) muss groß genug für alle Anwendungen sein, die Sie darauf installieren möchten.
4. Starten Sie die Maschine und wählen Sie **Starten > AppDisk vorbereiten**. Wenn diese Startmenüverknüpfung auf dem Hypervisor nicht verfügbar ist, öffnen Sie eine Eingabeaufforderung unter C:\Programme\Citrix\personal vDisk\bin und geben Sie **CtxPvD.Exe -s LayerCreationBegin** ein. Die Maschine wird neu gestartet und der Datenträger wird vorbereitet. Ein zweiter Neustart erfolgt, wenn einige Minuten später die Vorbereitung abgeschlossen ist.
5. Installieren Sie die Anwendungen, die Sie den Benutzern zur Verfügung stellen möchten.

6. Doppelklicken Sie auf die Verknüpfung **AppDisk verpacken** auf dem Maschinendesktop. Die Maschine wird wieder neu gestartet und die Versiegelung beginnt. Wenn das Dialogfeld "In Bearbeitung"geschlossen wird, fahren Sie die VM herunter.

Importieren der auf dem Hypervisor erstellten AppDisk mit Studio

1. Wählen Sie im Studio-Navigationsbereich **AppDisks** und im Aktionsbereich **AppDisk erstellen**.
2. Überprüfen Sie die Informationen auf der Seite **Einführung** des Assistenten und klicken Sie dann auf **Weiter**.
3. Aktivieren Sie auf der Seite **AppDisk erstellen** das Optionsfeld **Vorhandene AppDisk importieren**. Wählen Sie die Ressource (Netzwerk und Speicher), in der die auf dem Hypervisor erstellte AppDisk residiert. Klicken Sie auf **Weiter**.
4. Navigieren Sie auf der Seite **Vorbereitungsmaschine** zu der Maschine, wählen Sie den Datenträger aus und klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Zusammenfassung** einen Namen und eine Beschreibung für die AppDisk ein. Überprüfen Sie die auf den vorherigen Seiten des Assistenten angegebenen Informationen. Klicken Sie auf **Fertig stellen**. Die AppDisk wird von Studio importiert.

Wenn Sie die AppDisk in Studio importiert haben, weisen Sie sie einer Bereitstellungsgruppe hinzu.

Zuweisen einer AppDisk zu einer Bereitstellungsgruppe

Sie können einer Bereitstellungsgruppe beim Erstellen oder später eine oder mehrere AppDisks zuweisen. Dabei verwenden Sie im Prinzip die gleichen AppDisk-Informationen.

Wenn Sie AppDisks einer Bereitstellungsgruppe bei deren Erstellung hinzufügen, gehen Sie auf der Seite **AppDisks** des Assistenten zum Erstellen von Bereitstellungsgruppen gemäß den nachfolgenden Erläuterungen vor. (Informationen zu anderen Seiten des Assistenten finden Sie im Artikel Erstellen von Bereitstellungsgruppen.)

Hinzufügen (oder Entfernen) von AppDisks zu einer vorhandenen Bereitstellungsgruppe

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe und dann im Aktionsbereich **Bereitstellungsgruppe verwalten**. Informationen zur Seite **AppDisks** finden Sie weiter unten.
3. Wenn Sie die AppDisk-Konfiguration einer Bereitstellungsgruppe ändern, ist ein Neustart der Maschinen in der Gruppe erforderlich. Folgen Sie auf der Seite **Rolloutstrategie** den Anweisungen unter Erstellen eines Neustartzeitplans.

Seite "AppDisks"

Auf der Seite **AppDisks** (im Assistenten zum Erstellen von Bereitstellungsgruppen bzw. im Workflow "AppDisks verwalten") werden die der Bereitstellungsgruppe bereitgestellten AppDisks mitsamt ihrer Priorität aufgelistet. (Beim Erstellen der Bereitstellungsgruppe ist die Liste leer.) Weitere Informationen finden Sie im Abschnitt AppDisk-Priorität.

1. Klicken Sie auf **Hinzufügen**. Im Dialogfeld "AppDisks auswählen"werden in der linken Spalte alle AppDisks angezeigt. AppDisks, die der Bereitstellungsgruppe bereits zugewiesen wurden, haben ein aktiviertes Kontrollkästchen und können nicht ausgewählt werden.
2. Wählen Sie mindestens ein Kontrollkästchen einer verfügbaren AppDisk in der linken Spalte aus. In der rechten Spalte werden die Anwendungen auf der jeweiligen AppDisk angezeigt. (Bei Auswahl der Registerkarte **Anwendungen** oberhalb der rechten Spalte werden die Anwendungen in einem dem Startmenü ähnlichen Format angezeigt. Wenn Sie auf die Registerkarte **Installierte Pakete** klicken, werden die Anwendungen ähnlich wie unter "Programme und Features"angezeigt.)
3. Wenn Sie eine oder mehrere AppDisks ausgewählt haben, klicken Sie auf **OK**.
4. Klicken Sie auf der Seite "AppDisks"auf **Weiter**.

AppDisk-Priorität in einer Bereitstellungsgruppe

Sind einer Bereitstellungsgruppe mehrere AppDisks zugewiesen, werden diese auf der Seite **AppDisks** (in den Anzeigen "Bereitstellungsgruppe erstellen", "Bereitstellungsgruppe bearbeiten"und "AppDisks verwalten") in absteigender Priorität aufgeführt. Einträge am Anfang der Liste haben höhere Priorität. Die Priorität gibt an, in welcher Reihenfolge die AppDisks verarbeitet werden.

Sie können die AppDisk-Priorität mit den Pfeilschaltflächen neben der Liste ändern. Ist AppDNA in die AppDisk-Bereitstellung integriert, analysiert es die Anwendungen automatisch und weist die Priorität zu, wenn die AppDisks der Bereitstellungsgruppe zugewiesen werden. Wenn Sie später AppDisks hinzufügen oder aus der Gruppe entfernen, können Sie mit der **Option zum automatischen Sortieren** eine erneute AppDNA-Analyse der aktuellen AppDisk-Liste zur Bestimmung der Priorität starten. Analyse und Priorisieren (falls erforderlich) können mehrere Minuten dauern.

Verwalten von AppDisks

Nach dem Erstellen von AppDisks und dem Zuweisen zu Bereitstellungsgruppen können Sie die AppDisk-Eigenschaften über den Knoten "AppDisks"im Navigationsbereich von Studio ändern. Änderungen an den Anwendungen auf einer AppDisk müssen über die Hypervisor-Verwaltungskonsole vorgenommen werden.

> **Wichtig:**
>
> Sie können den Windows Update-Dienst zum Aktualisieren von Anwendungen einer AppDisk (Office o. Ä.) verwenden. Verwenden Sie Windows Update jedoch nicht zum Anwenden von Betriebssystemupdates auf AppDisks. Wenden Sie Betriebssystemupdates auf Masterimages und nicht auf AppDisks an, sonst werden die AppDisks nicht richtig initialisiert.
>
> - Wenden Sie nur Patches und andere Updates auf Anwendungen einer AppDisk an, die wirklich für die Anwendungen benötigt werden. Wenden Sie keine für andere Anwendungen vorgesehenen Updates an.
> - Bei der Installation von Windows-Updates deaktivieren Sie zunächst alle Einträge und wählen Sie dann nur die Einträge aus, die für die Anwendungen auf der AppDisk erforderlich sind, die Sie aktualisieren.

AppDisk-Erstellung und Antivirenprogramme

Beim Erstellen einer AppDisk kann es zu Problemen kommen, wenn auf der Basis-VM ein Antivirenagent (A/V) installiert ist. In solchen Fällen kann die AppDisk-Erstellung fehlschlagen, wenn bestimmte Prozesse vom A/V-Agent verdächtigt werden. Die Prozesse **CtxPvD.exe** und **CtxPvDSrv.exe** müssen der Ausnahmeliste für den A/V-Agent hinzugefügt werden, der von der Basis-VM verwendet wird.

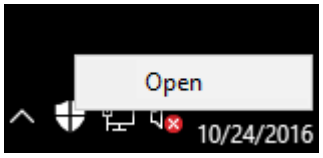
Dieser Abschnitt enthält Informationen zum Hinzufügen von Ausnahmen für folgende Antivirus-Anwendungen:

- Windows Defender (für Windows 10)
- OfficeScan (Version 11.0)
- Symantec (Version 12.1.16)
- McAfee (Version 4.8)

Windows Defender

Gehen Sie wie folgt vor, wenn auf der Basis-VM Windows Defender (Version 10) ausgeführt wird:

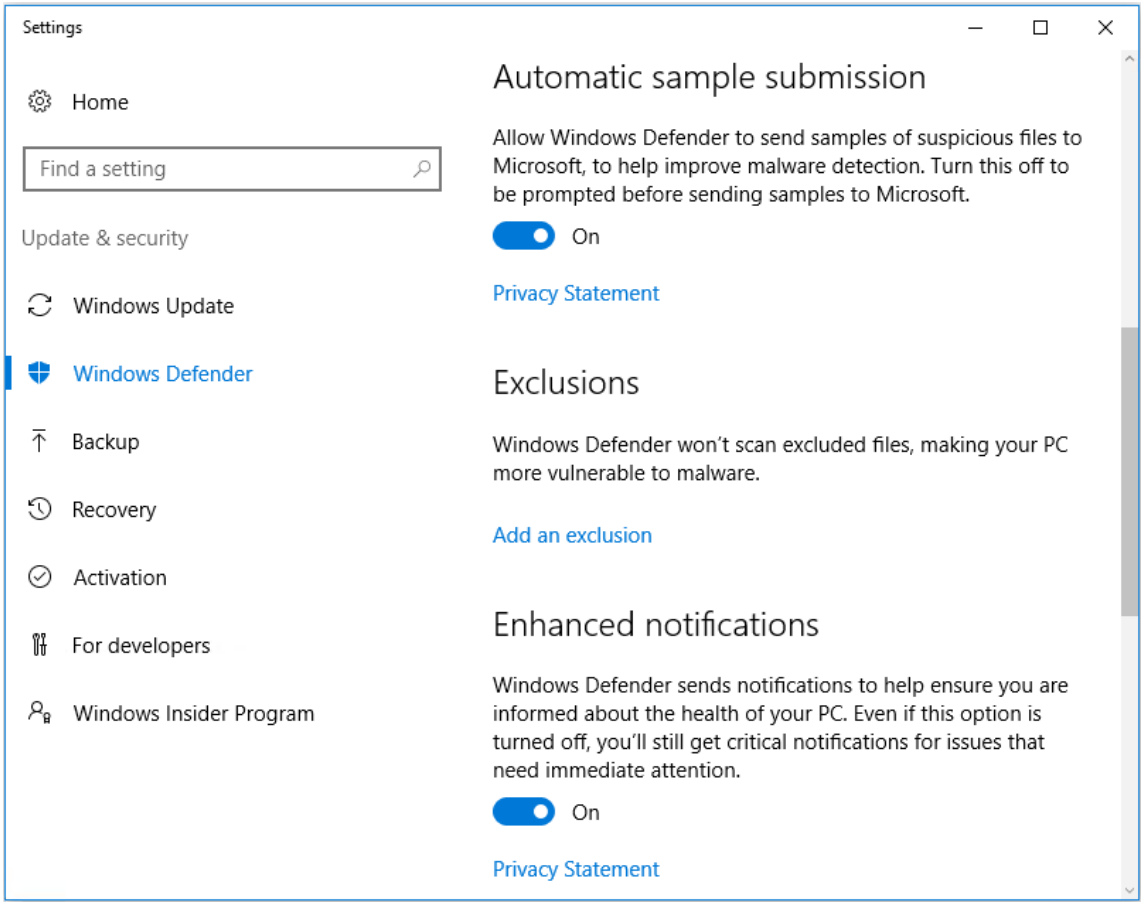
1. Melden Sie sich bei dem Computer als lokaler Administrator an.
2. Klicken Sie mit der rechten Maustaste auf das Windows Defender-Symbol, um die Schaltfläche **Öffnen** anzuzeigen:



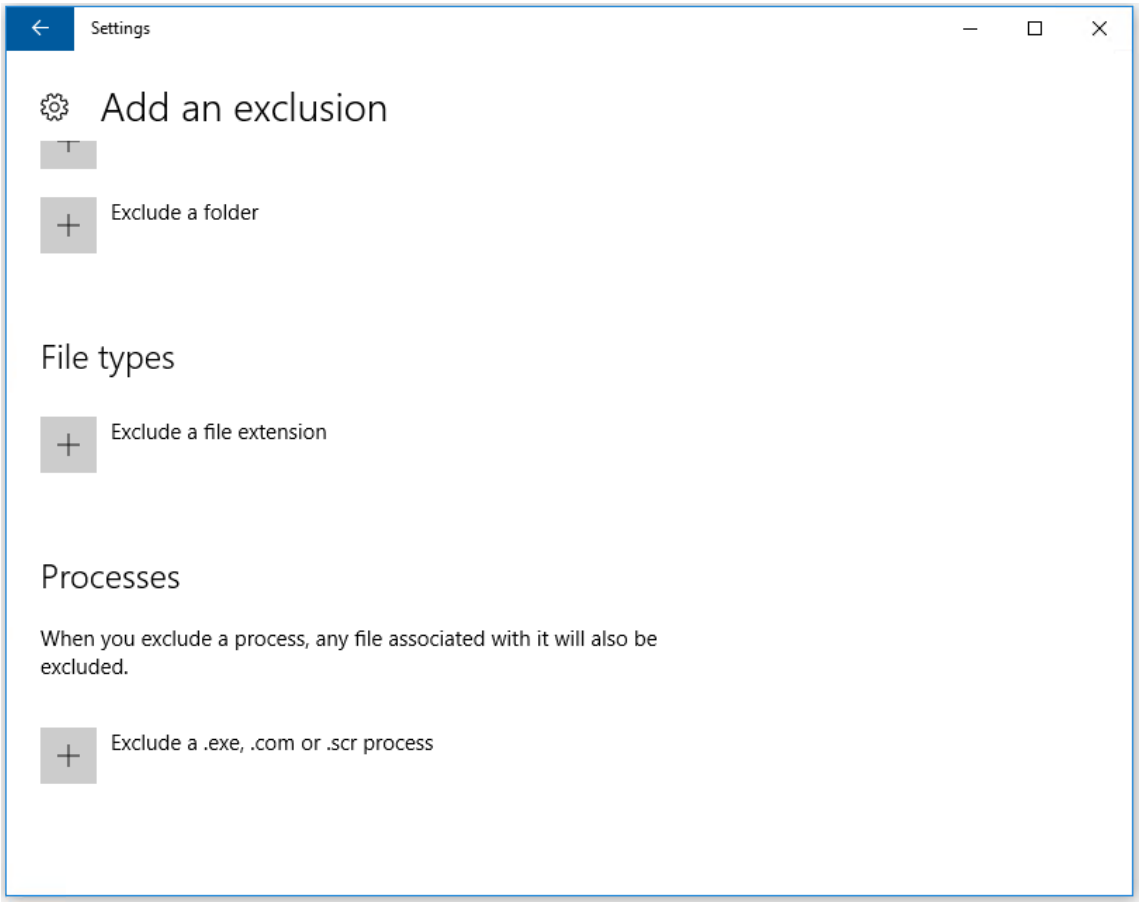
3. Wählen Sie in der Windows Defender-Konsole rechts oben **Einstellungen**:

   lokalisierte Abbildung](/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-main-page.png)

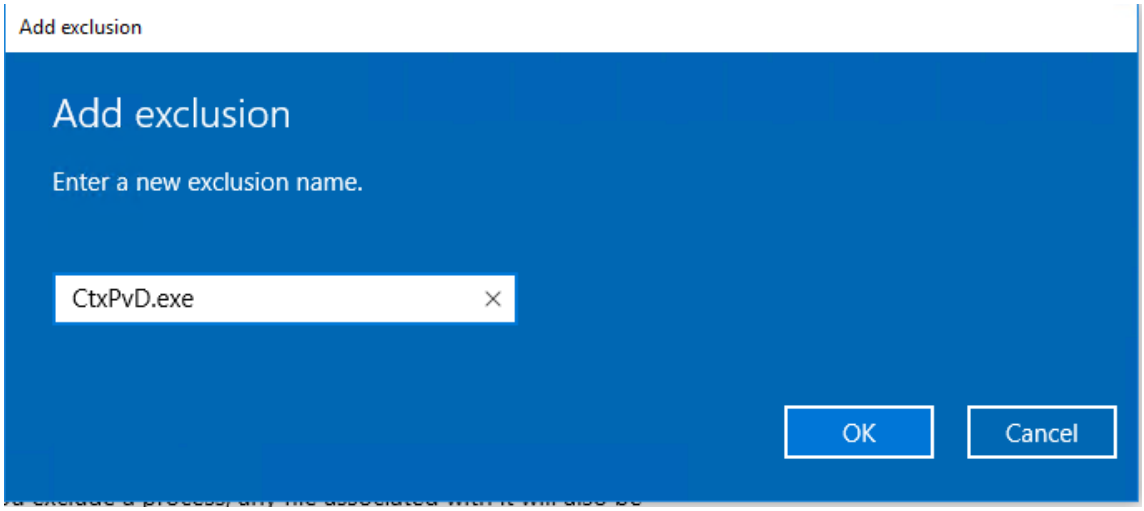
4. Klicken Sie im Bereich **Ausschlüsse** auf **Ausschluss hinzufügen**:



5. Wählen Sie im Bildschirm **Ausschluss hinzufügen** die Option **EXE-, COM- oder SCR-Prozess ausschließen**:



6. Geben Sie im Bildschirm **Ausschluss hinzufügen** den Namen des Ausschlusses ein: Sie müssen sowohl **CtxPvD.exe** als auch **CtxPvDSvc.exe** hinzufügen, um Konflikte beim Erstellen einer AppDisk zu verhindern. Wenn Sie den Ausschlussnamen eingegeben haben, klicken Sie auf **OK**:



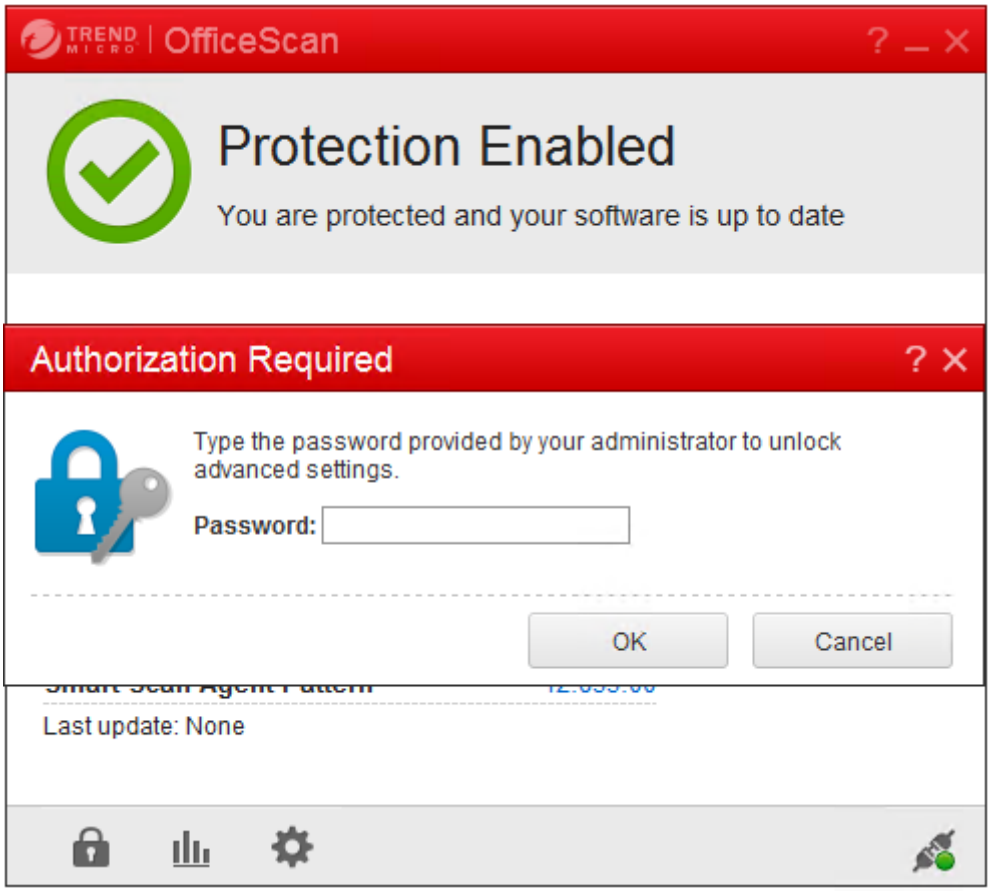
Nach dem Hinzufügen der Ausschlüsse erscheinen sie in der Liste der ausgeschlossenen Prozesse auf dem Bildschirm **Einstellungen**:


```
1 ![localized image](/en-us/xenapp-and-xendesktop/7-15-ltsr/media/wd-
    process-added.png)
```

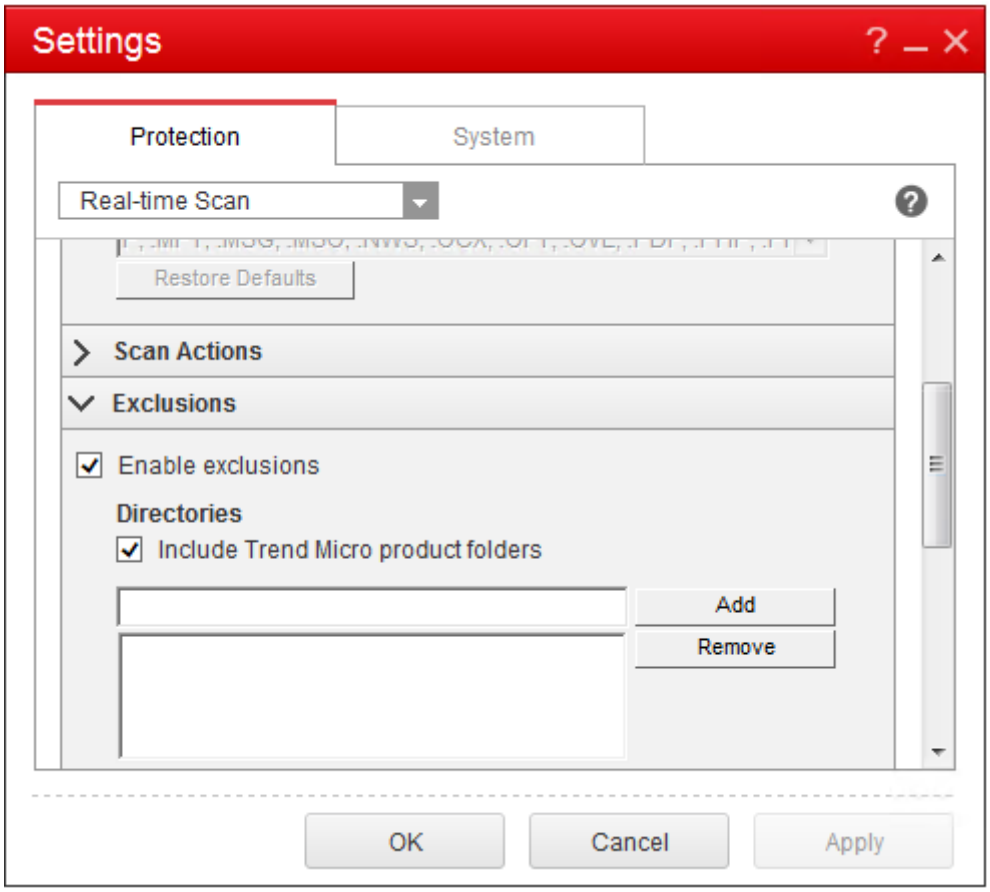
OfficeScan

Gehen Sie wie folgt vor, wenn auf der Basis-VM OfficeScan (Version 11) ausgeführt wird:

1. Starten Sie die OfficeScan-Konsole.
2. Klicken Sie auf das Schlosssymbol unten links und geben Sie Ihr Kennwort ein:

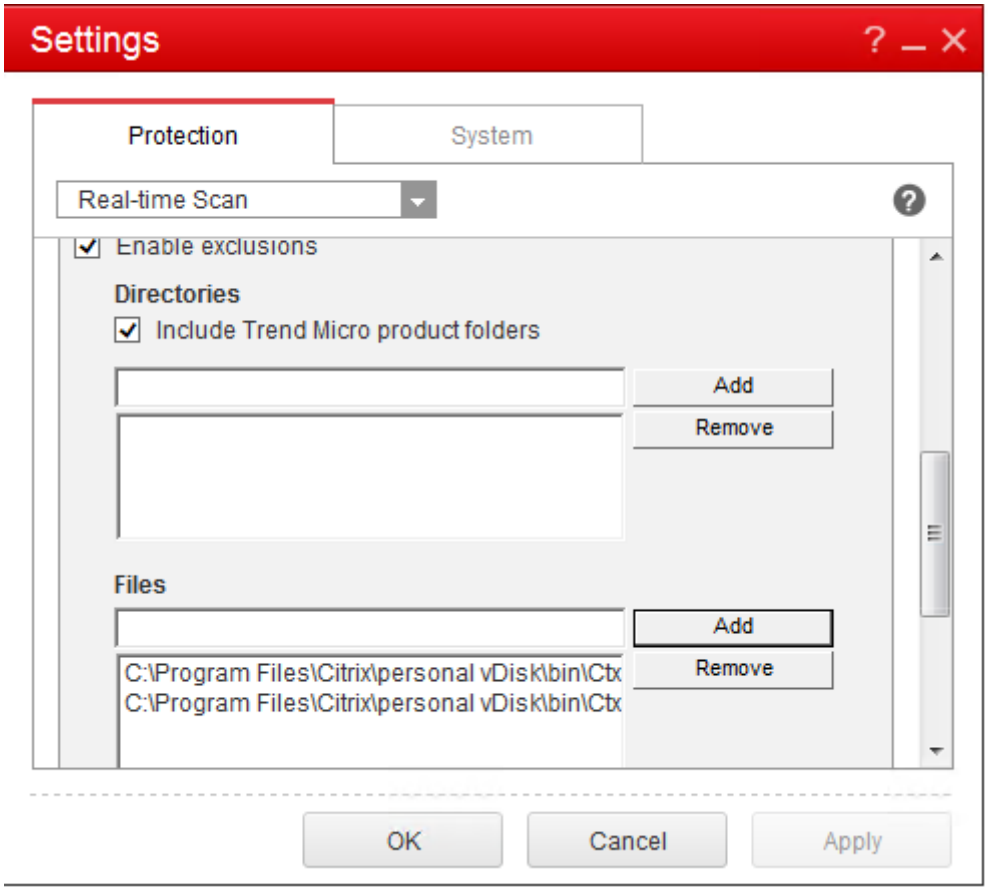


3. Klicken Sie auf das Symbol **Settings**, um die Konfigurationsoptionen anzuzeigen.
4. Wählen Sie im Bildschirm mit den Einstellungen die Registerkarte **Protection**.
5. Scrollen Sie auf der Registerkarte nach unten zum Abschnitt **Exclusions**.



6. Klicken Sie im Abschnitt **Files** auf **Add** und geben Sie die folgenden AppDisk-Prozesse zur Aufnahme in die Ausnahmenliste an:

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```

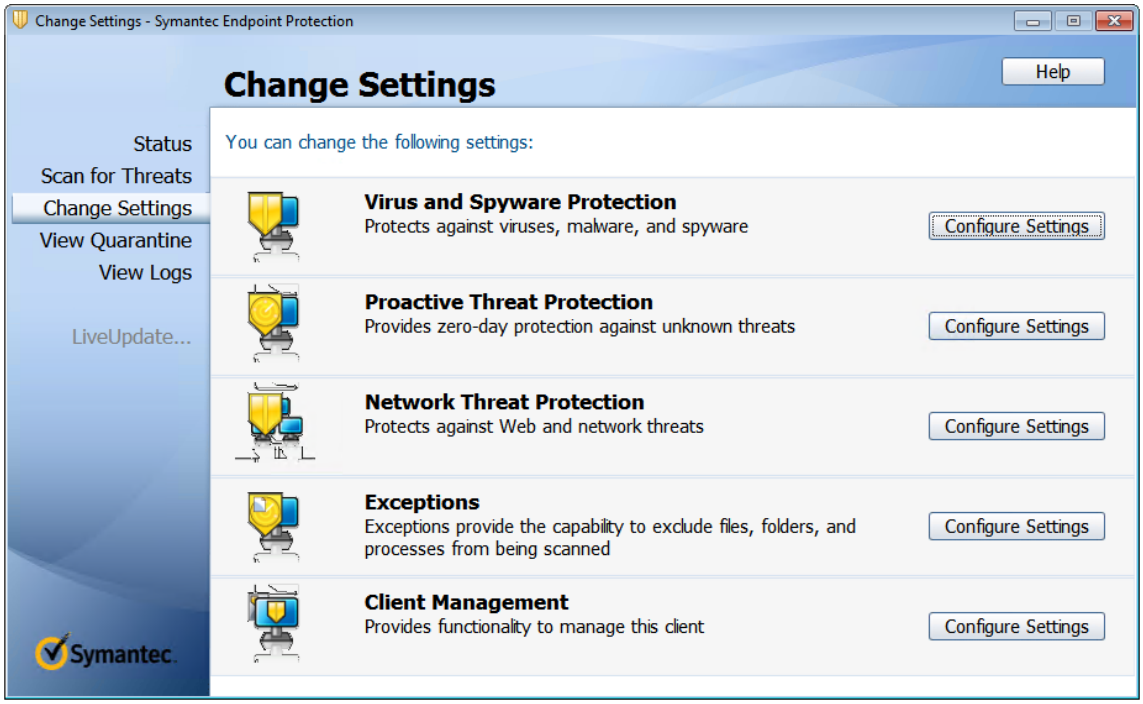



Klicken Sie auf **Apply** und dann auf **OK**, um die Ausschlüsse hinzuzufügen.

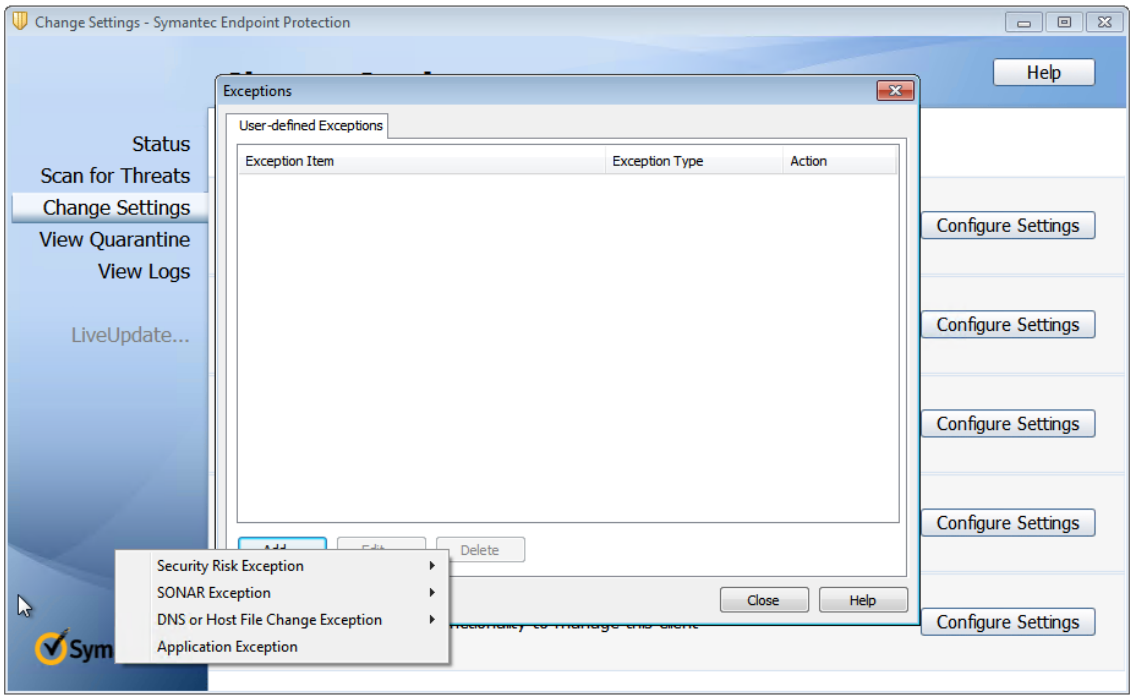
Symantec

Gehen Sie wie folgt vor, wenn auf der Basis-VM Symantec (Version 12.1.16) ausgeführt wird:

1. Starten Sie die Symantec-Konsole.
2. Klicken Sie auf **Change Settings**.
3. Klicken Sie im Bereich **Exceptions** auf **Configure Settings**:

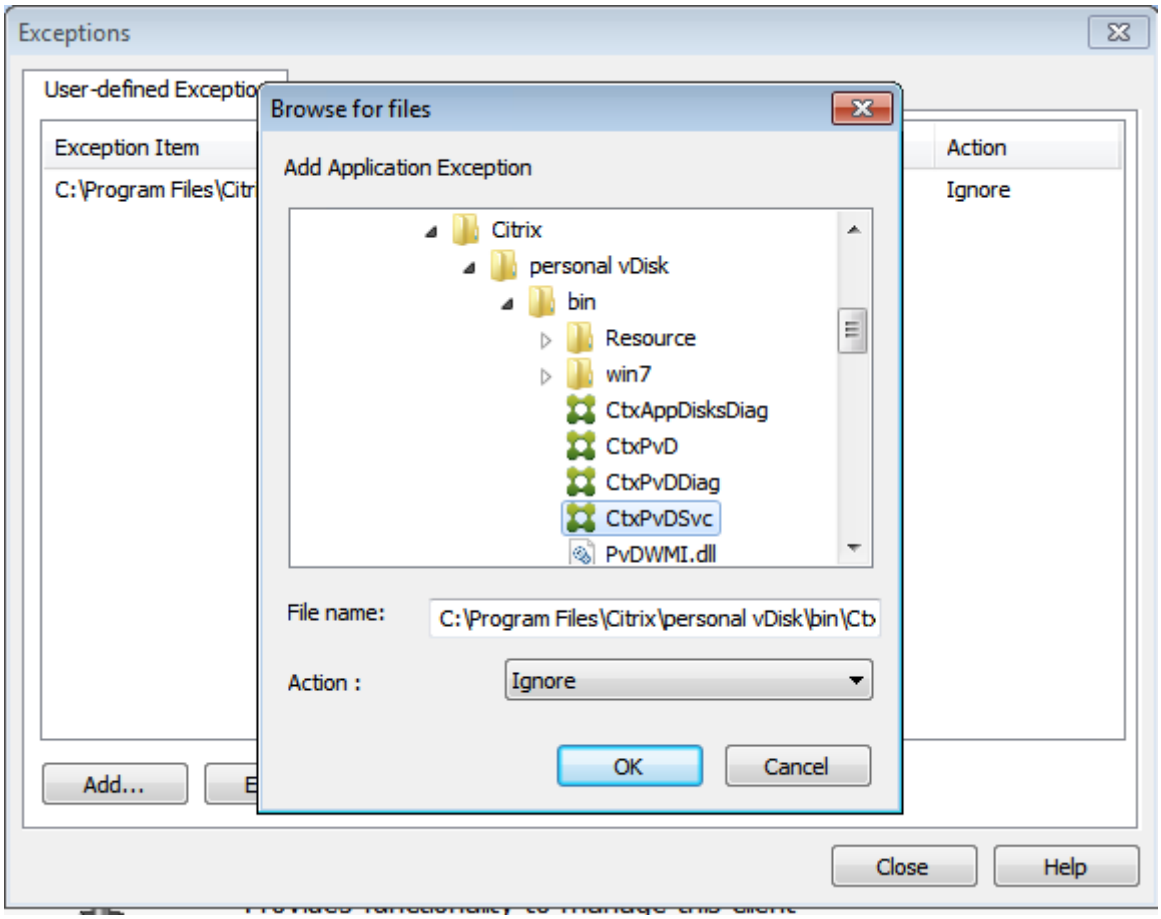


4. Klicken Sie im Bildschirm "Configure Settings"auf **Add**.
5. Es wird nun ein Kontextmenü zum Angeben des Typs "Anwendung"angezeigt. Wählen Sie **Application Exception**:

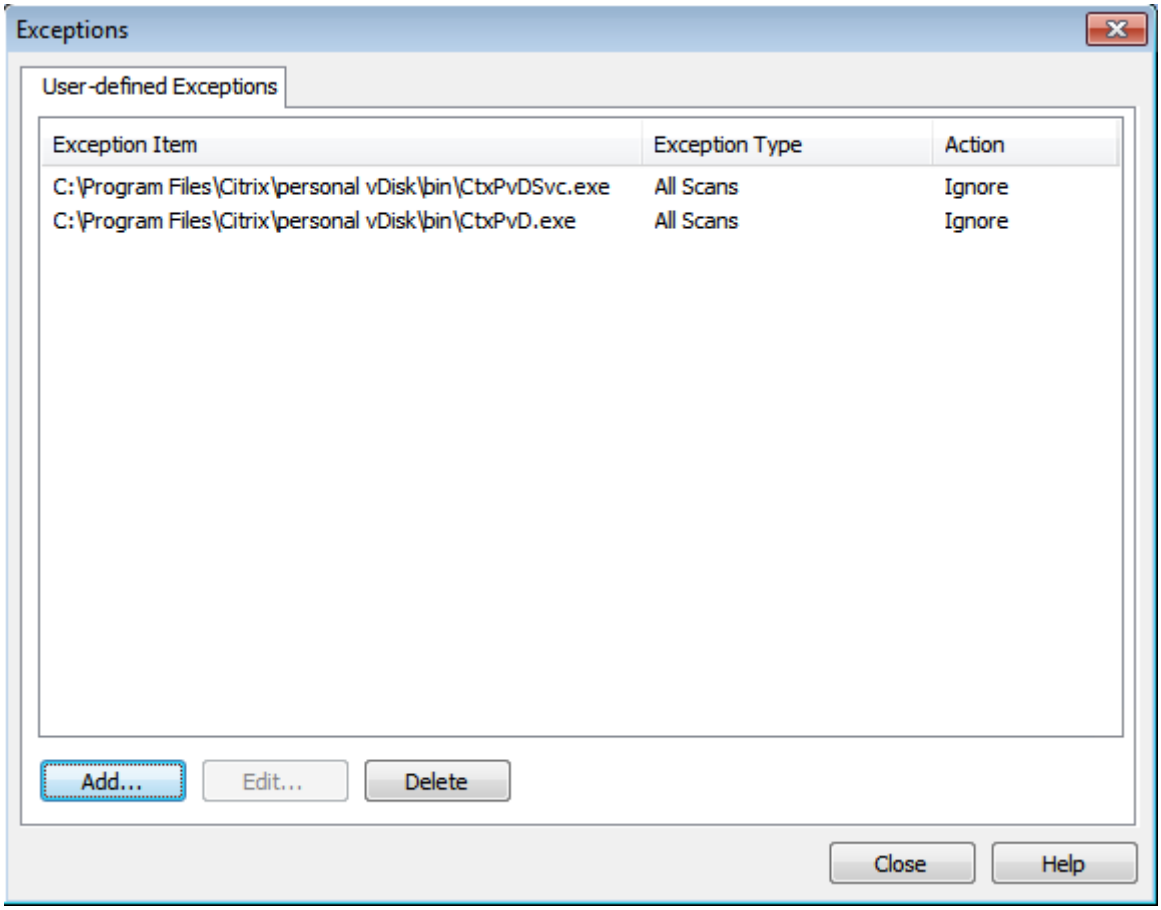


6. Geben Sie im Bildschirm "Exceptions"die folgenden AppDisk-Dateipfade ein und wählen Sie als Aktion **Ignore**:


```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```



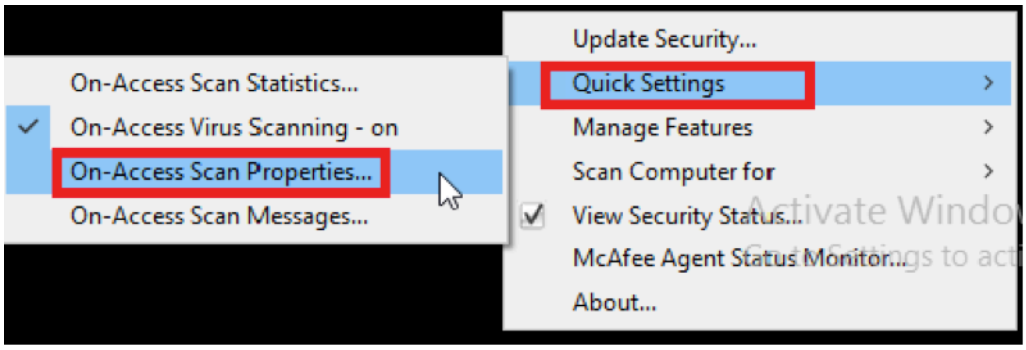
Die Ausnahmen werden der Liste hinzugefügt. Schließen Sie das Fenster, um die Änderungen anzuwenden:



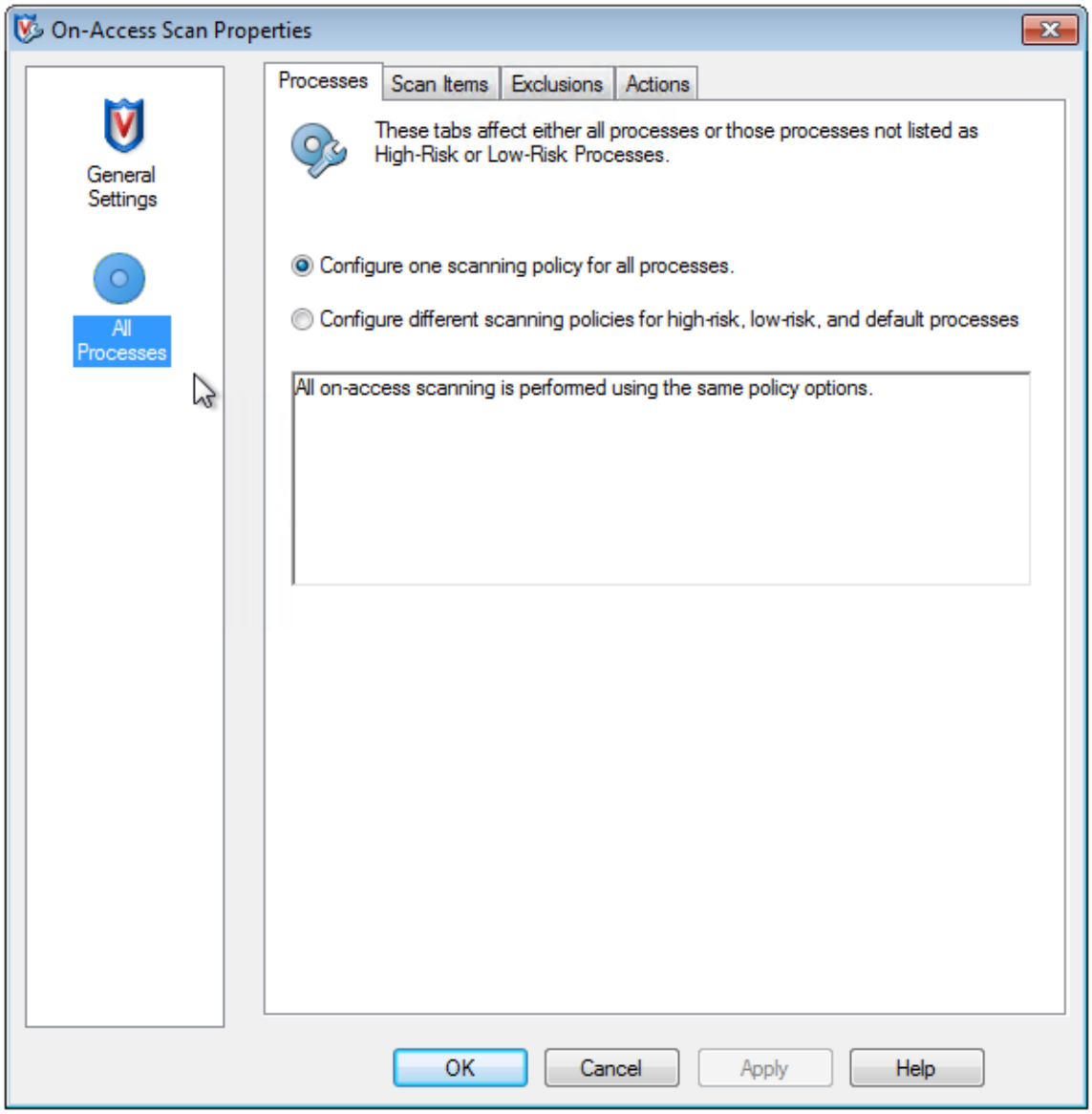
McAfee

Gehen Sie wie folgt vor, wenn auf der Basis-VM McAfee (Version 4.8) ausgeführt wird:

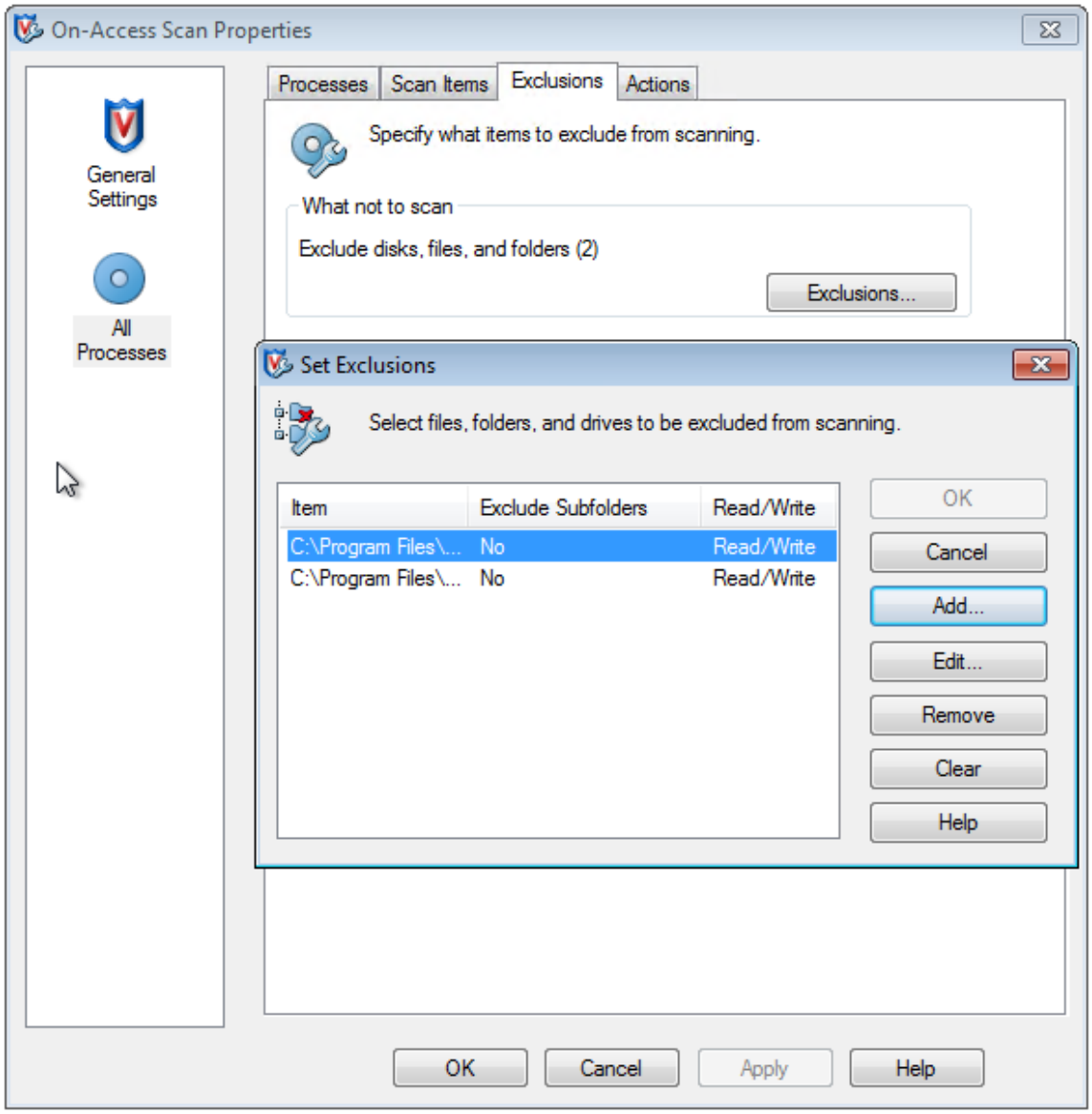
1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol und erweitern Sie die Option **Quick Settings**.
2. Wählen Sie **On-Access Scan Properties**:



3. Klicken Sie im Bildschirm **On-Access Scan Properties** auf **All Processes**:



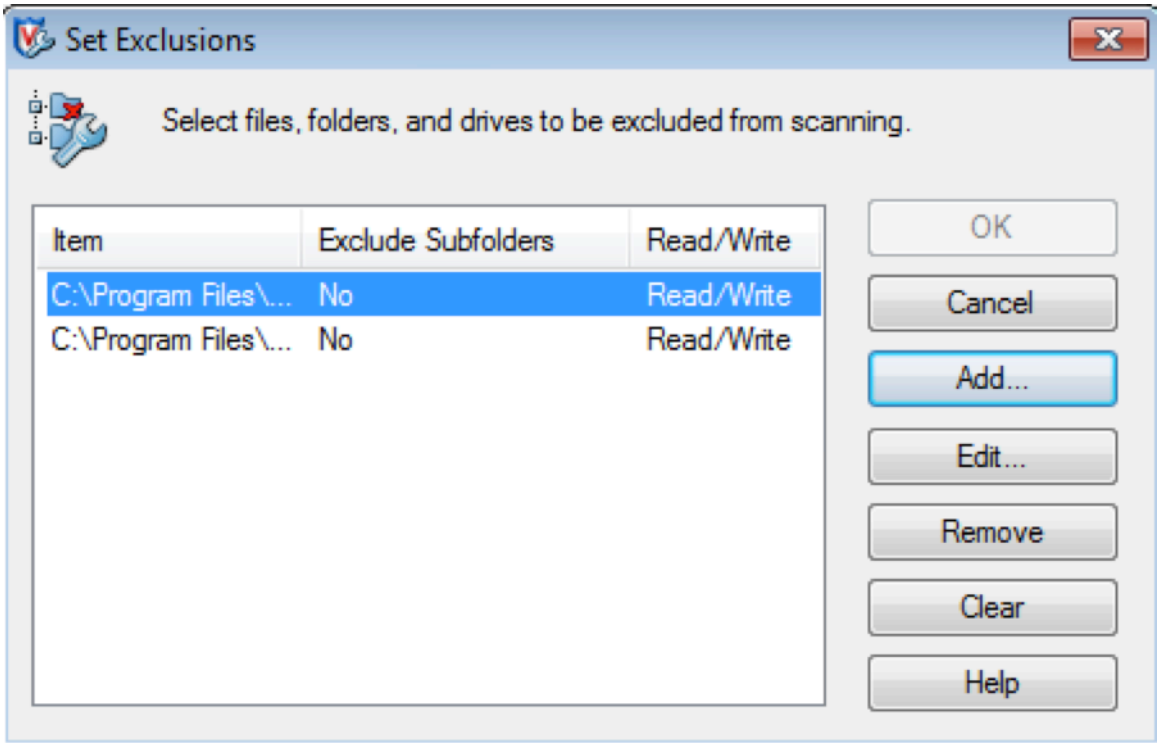
4. Wählen Sie die Registerkarte **Exclusions**.
5. Klicken Sie auf die Schaltfläche **Exclusions**.
6. Klicken Sie im Bildschirm **Set Exclusions** auf **Add**.



7. Wählen Sie im Bildschirm **Add Exclusion Item** die Option **By name/location (can include wild-cards * or ?)**. Klicken Sie auf **Browse**, um die ausführbaren Dateien zu suchen:

```
    C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
    C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
<!--NeedCopy-->
```

Klicken Sie auf **OK**. In dem Bildschirm **Set Exclusions** werden jetzt die hinzugefügten Ausschlüsse angezeigt. Klicken Sie auf **OK**, um die Änderungen anzuwenden:



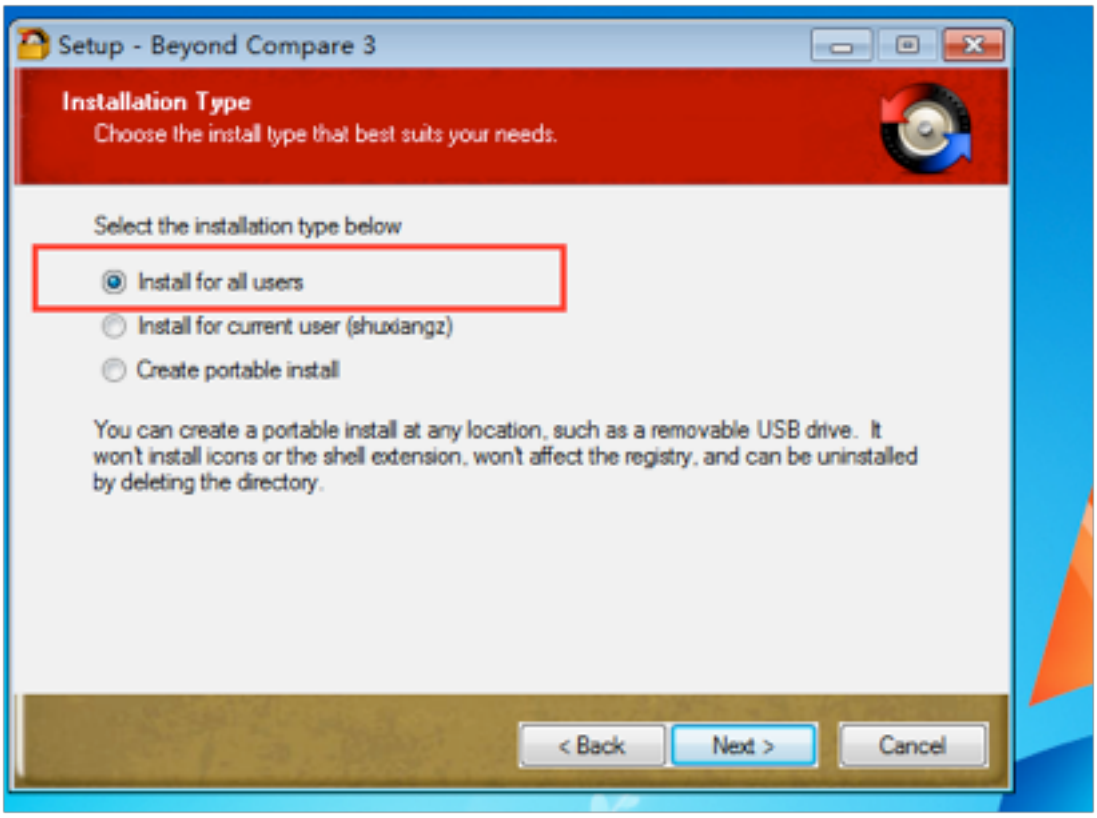
> **Hinweis:**
>
> Wenn Sie die Ausschlüsse konfiguriert haben, erstellen Sie die AppDisk.

Anzeige von Anwendungen im Startmenü

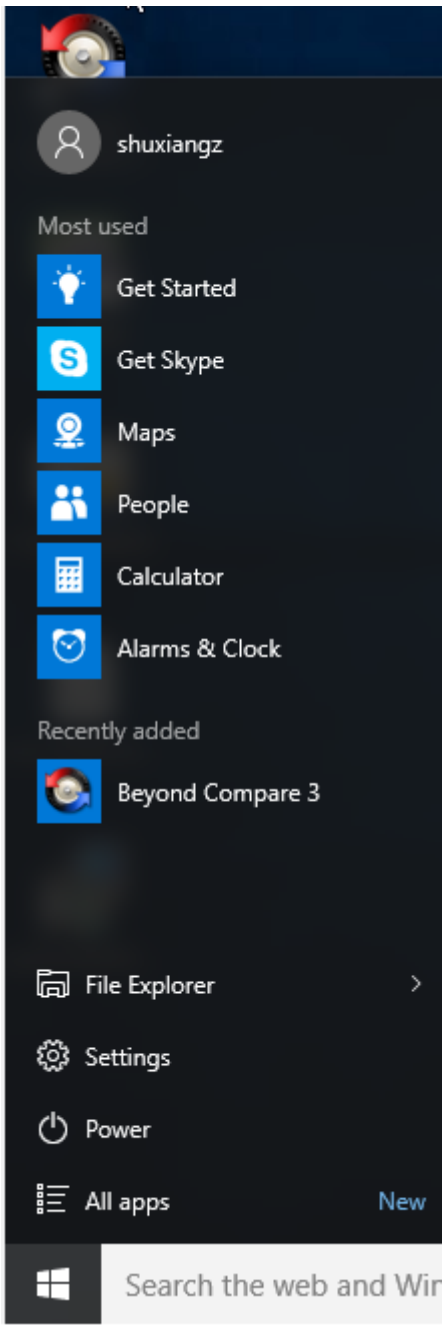
Wenn Sie eine neue AppDisk erstellen und eine Anwendung für alle Benutzer verfügbar machen, wird die AppDisk dem Desktop angefügt und eine Verknüpfung mit der Anwendung im Startmenü angezeigt. Wenn Sie eine AppDisk erstellen und nur für den aktuellen Benutzer installieren und die AppDisk dem Desktop angefügt wird, wird keine Verknüpfung mit der Anwendung im Startmenü angezeigt.

Erstellen einer neuen Anwendung mit Bereitstellung für alle Benutzer

1. Installieren Sie eine Anwendung auf der AppDisk (in diesem Beispiel *Beyond Compare*):

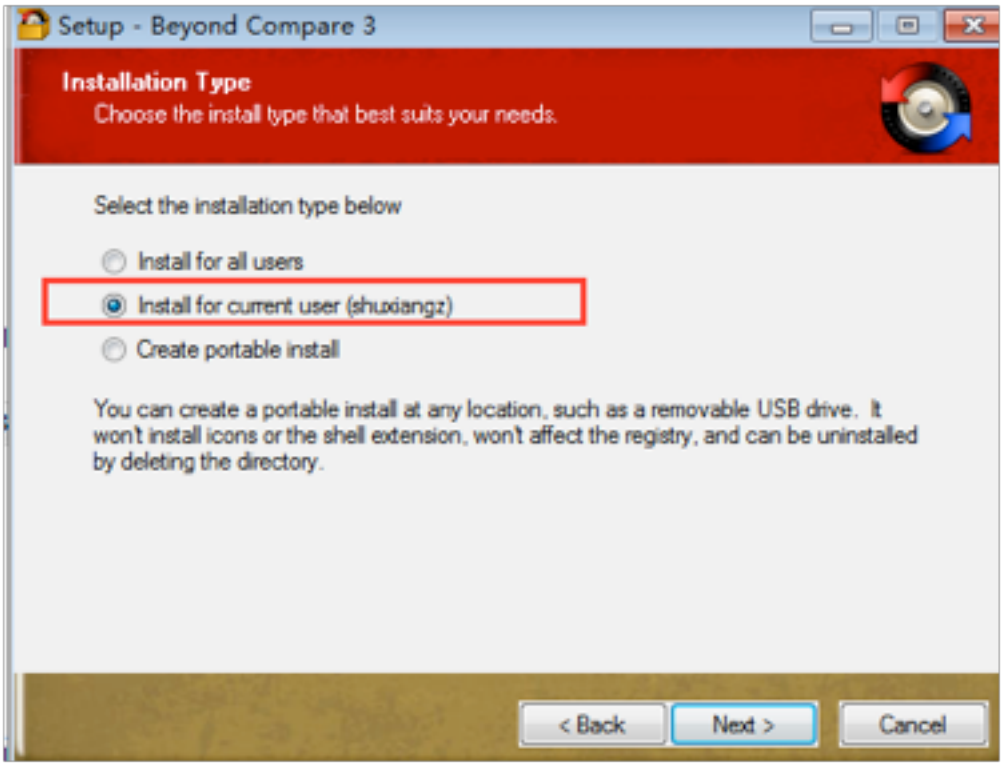


2. Fügen Sie die AppDisk dem Desktop an. Die Verknüpfung für das neu installierte *Beyond Compare* erscheint nun im Startmenü:

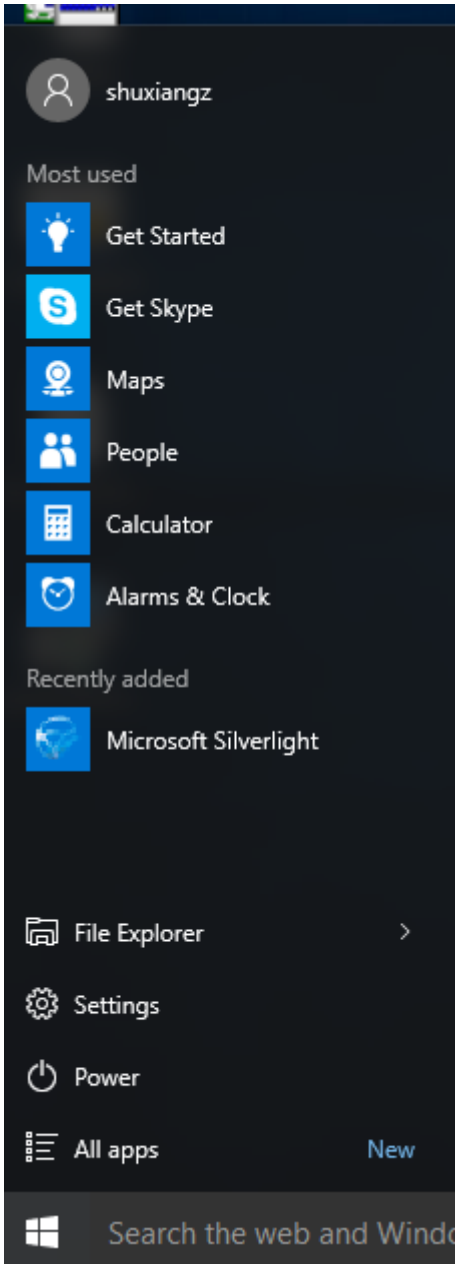


Installieren der Anwendung für den aktuellen Benutzer

1. Installieren Sie eine Anwendung auf der AppDisk und stellen Sie sie dem aktuellen Benutzer zur Verfügung:



2. Fügen Sie die AppDisk dem Desktop an. Die Verknüpfung der Anwendung erscheint nicht im Startmenü:



Neuerungen bei der AppDisk-Protokollierung

Dieses Release bietet eine Erweiterung des AppDisk-Protokollierungs- und Supportparadigmas. AppDisk-Benutzer können jetzt Diagnoseinformationen erhalten und optional auf die Citrix Insight Services (CIS)-Website hochladen.

Funktionsweise

Für die neu Funktion wird ein skriptbasierten PowerShell-Tool verwendet, das alle von AppDisk-PVD erstellten Protokolldateien identifiziert, die Ausgabe von PowerShell-Befehlen mit Informationen über das System (und Prozesse) sammelt, alle Elemente in einer organisierten Einzeldatei komprimiert und dann die Option zum Speichern der Datei lokal oder zum Hochladen an CIS (Citrix Insight Services) anbietet.

> **Hinweis:**
>
> CIS sammelt anonyme Diagnoseinformationen, die zur Verbesserung der AppDisk-/PvD-Funktionalität verwendet werden. Rufen Sie die Citrix Insight Services-Website auf, um das Diagnosepaket manuell hochzuladen. Sie müssen sich mit Ihren Citrix Anmeldeinformationen anmelden, um auf die Site zuzugreifen.

Verwenden von PowerShell-Skripts zum Sammeln von AppDisk-/PvD-Protokolldateien Das AppDisk-/PvD-Installationsprogramm bietet zwei neue Skripts für die Sammlung von Diagnosedaten:

- **Upload-AppDDiags.ps1** sammelt AppDisk-Diagnosedaten
- **Upload-PvDDiags.ps1** sammelt PvD-Diagnosedaten

> **Hinweis:**
>
> Die Skripts sind im Ordner C:\Programme\Citrix\personal vdisk\bin\scripts. Die PowerShell-Skripts müssen als Administrator ausgeführt werden.

Verwenden Sie **Upload-AppDDiags.ps1** zum Sammeln von Diagnosedaten für die AppDisk und optional zum manuellen Hochladen der Daten auf die CIS-Website.

```
SYNTAX
     Upload-AppDDiags [[-OutputFile] <string>] [-help] [<
        CommonParameters>]
         -OutputFile
             Local path for zip file instead of uploading to CIS
 EXAMPLES
     Upload-AppDDiags
         Upload diagnostic data to Citrix CIS website using credentials
             entered by interactive user.
     Upload-AppDDiags -OutputFile C:\MyDiags.zip
         Save AppDisk diagnostic data to the specified zip file. You
            can access https://cis.citrix.com/ to upload it later.
```

> **Tipp:**
>
> Wenn es kein Argument –**OutputFile** gibt, erfolgt der Upload. Wird –**OutputFile** angegeben, er-

> stellt das Skript eine ZIP-Datei, die Sie zu einem späteren Zeitpunkt manuell hochladen können.

Verwenden Sie **Upload-PvDDiags.ps1** zum Sammeln von Diagnosedaten für PvD und optional zum manuellen Hochladen der Daten auf die CIS-Website.

```
SYNTAX
 Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
     -OutputFile
         Local path for zip file instead of uploading to CIS
 EXAMPLES
     Upload-PvDDiags
         Upload PvD diagnostic data to Citrix CIS website using
            credentials entered by interactive user.
     Upload-PvDDiags -OutputFile C:\MyDiags.zip
         Save PvD diagnostic data to the specified zip file. You can
            access https://cis.citrix.com/ to upload it later.
```

> **Tipp:**
>
> Wenn es kein Argument –**OutputFile** gibt, erfolgt der Upload. Wird –**OutputFile** angegeben, erstellt das Skript eine ZIP-Datei, die Sie zu einem späteren Zeitpunkt manuell hochladen können.

Veröffentlichen von Inhalten

August 18, 2021

Sie können eine Anwendung veröffentlichen, die einfach aus einer URL oder einem UNC-Pfad zu einer Ressource besteht, z. B. zu einem Microsoft Word-Dokument oder einem Internet-Link. Dieses Feature wird als Veröffentlichung von Inhalten bezeichnet. Das Feature ermöglicht eine flexiblere Bereitstellung von Inhalten für Benutzer. Sie können die vorhandene Zugriffssteuerung und Anwendungsverwaltung nutzen. Außerdem können Sie festlegen, wie der Inhalt geöffnet werden soll: lokal oder als veröffentlichte Anwendung.

Die veröffentlichten Inhalte erscheinen genau wie andere Anwendungen in StoreFront und Citrix Receiver. Die Benutzer greifen auf die gleiche Art und Weise auf sie zu wie auf Anwendungen. Auf dem Client wird die Ressource wie gewohnt geöffnet.

- Wenn eine lokal installierte Anwendung geeignet ist, wird sie zum Öffnen der Ressource gestartet.
- Wenn eine Dateitypzuordnung definiert wurde, wird eine veröffentlichte Anwendung zum Öffnen der Ressource gestartet.

Zum Veröffentlichen von Inhalten verwenden Sie das PowerShell-SDK. (Mit Studio können Sie keinen Inhalt veröffentlichen. Allerdings können Sie mit Studio später die Anwendungseigenschaften bearbeiten, nachdem der Inhalt veröffentlicht wurde.)

Konfigurationsübersicht und Vorbereitung

Beim Veröffentlichen von Inhalten wird das Cmdlet "New-BrokerApplication"mit folgenden Haupteigenschaften verwendet. (In der Cmdlets-Hilfe finden Sie Beschreibungen aller Cmdlets-Eigenschaften.)

```
New-BrokerApplication –ApplicationType PublishedContent
\-CommandLineExecutable \<*location*> -Name \<*app-name*>
\-DesktopGroup \<*delivery-group-name*>
```

Die Eigenschaft "ApplicationType"muss PublishedContent sein.

Die Eigenschaft CommandLineExecutable gibt den Ort der veröffentlichten Inhalte an. Folgende Formate werden unterstützt (max. 255 Zeichen):

- HTML-Websiteadresse (z. B. `https://www.citrix.com`)
- Dokumentdatei auf einem Webserver (z. B. `https://www.citrix.com/press/pressrelease.doc`)
- Verzeichnis auf einem FTP-Server (z. B. `ftp://ftp.citrix.com/code`)
- Dokumentdatei auf einem FTP-Server (z. B. `ftp://ftp.citrix.com/code/Readme.txt`)
- UNC-Verzeichnispfad (z. B. `file://myServer/myShare` oder `\\myServer\myShare`)
- UNC-Dateipfad (z. B. `file://myServer/myShare/myFile.asf` oder `\\myServer\myShare\myFile.asf`)

Stellen Sie sicher, dass Sie das richtige SDK haben.

- Für XenApp und XenDesktop-Servicebereitstellungen laden Sie das XenApp und XenDesktop Remote PowerShell SDK herunter und installieren Sie es.
- Verwenden Sie bei lokalen XenApp und XenDesktop-Bereitstellungen das mit dem Delivery Controller installierte PowerShell-SDK. Das Hinzufügen von veröffentlichten Inhalten erfordert mindestens Version 7.11 eines Delivery Controllers.

Den nachfolgenden Anweisungen verwenden Beispiele. In den Beispielen:

- Es wurde ein Maschinenkatalog erstellt.
- Es wurde eine Bereitstellungsgruppe namens "PublishedContentApps"erstellt. Die Gruppe verwendet eine Serverbetriebssystemmaschine aus dem Maschinenkatalog. Die WordPad-Anwendung wurde der Gruppe hinzugefügt.
- Der Bereitstellungsgruppenname, der CommandLineExecutable-Speicherort und der Name der Anwendung wurden zugewiesen.

Erste Schritte

Öffnen Sie PowerShell auf der Maschine mit dem PowerShell-SDK.

Das folgende Cmdlet fügt das benötigte PowerShell-SDK-Snap-In hinzu und weist den zurückgegebenen Bereitstellungsgruppeneintrag zu.

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup -Name PublishedContentApps
<!--NeedCopy-->
```

Wenn Sie den XenApp und XenDesktop Service nutzen, authentifizieren Sie sich mit Ihren Citrix Cloud-Anmeldeinformationen. Wenn es mehrere Kunden gibt, wählen Sie einen.

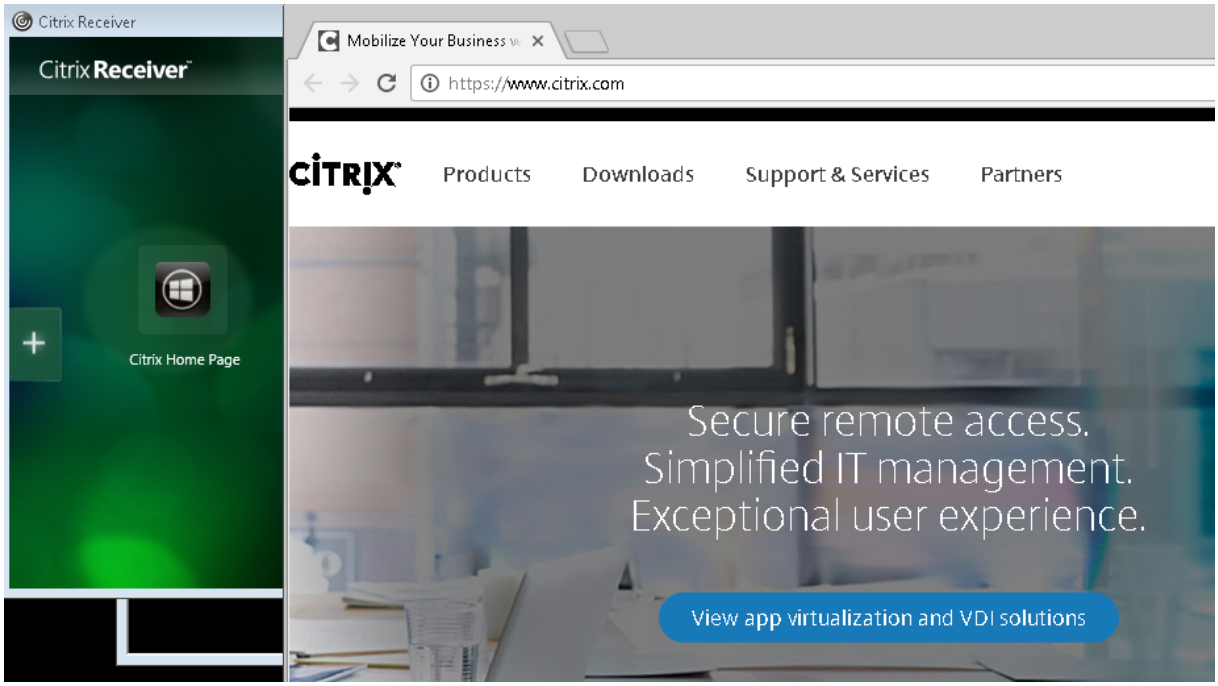
Veröffentlichen einer URL

Nach der Zuweisung von Standort und Anwendungsnamen veröffentlicht das folgende Cmdlet die Citrix Homepage als Anwendung.

```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $citrixURL -Name $appName
 -DesktopGroup $dg.Uid
<!--NeedCopy-->
```

Überprüfen des Vorgangs

- Öffnen Sie StoreFront und melden Sie sich als Benutzer mit Zugriff auf die Anwendungen in der Bereitstellungsgruppe “PublishedContentApps”an. Die neu erstellte Anwendung wird mit dem Standardsymbol angezeigt. Weitere Informationen zum Anpassen des Symbols finden Sie unter https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.
- Klicken Sie auf die Citrix Homepage-Anwendung. Die URL wird in einer neuen Registerkarte der lokal ausgeführten Instanz des Standardbrowsers geöffnet.



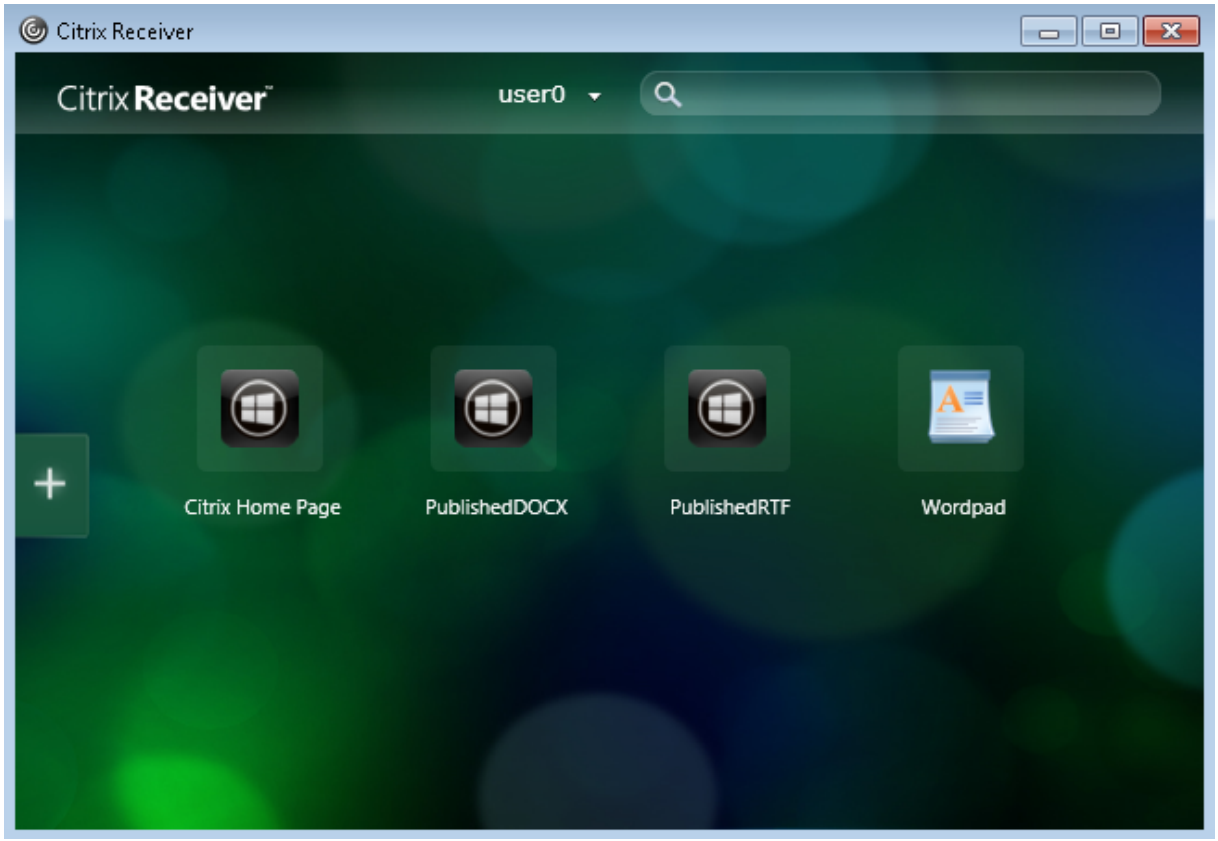
Veröffentlichen von Ressourcen mit UNC-Pfad

In diesem Beispiel hat der Administrator bereits eine Freigabe namens “PublishedResources”erstellt. Nach der Zuweisung von Speicherorten und Namen veröffentlichen die folgenden Cmdlets eine RTF-Datei und eine DOCX-Datei in der Freigabe als Ressource.

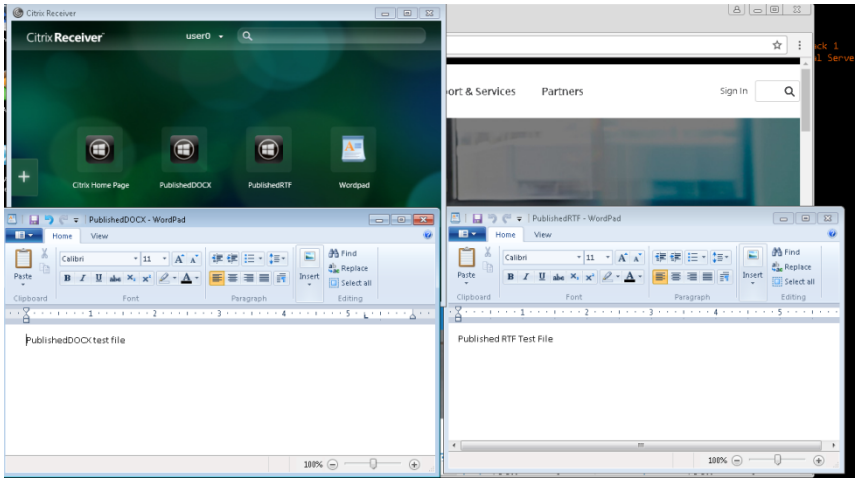
```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

Überprüfen des Vorgangs

- Aktualisieren Sie Ihr StoreFront-Fenster, um die neu veröffentlichten Dokumente anzuzeigen.

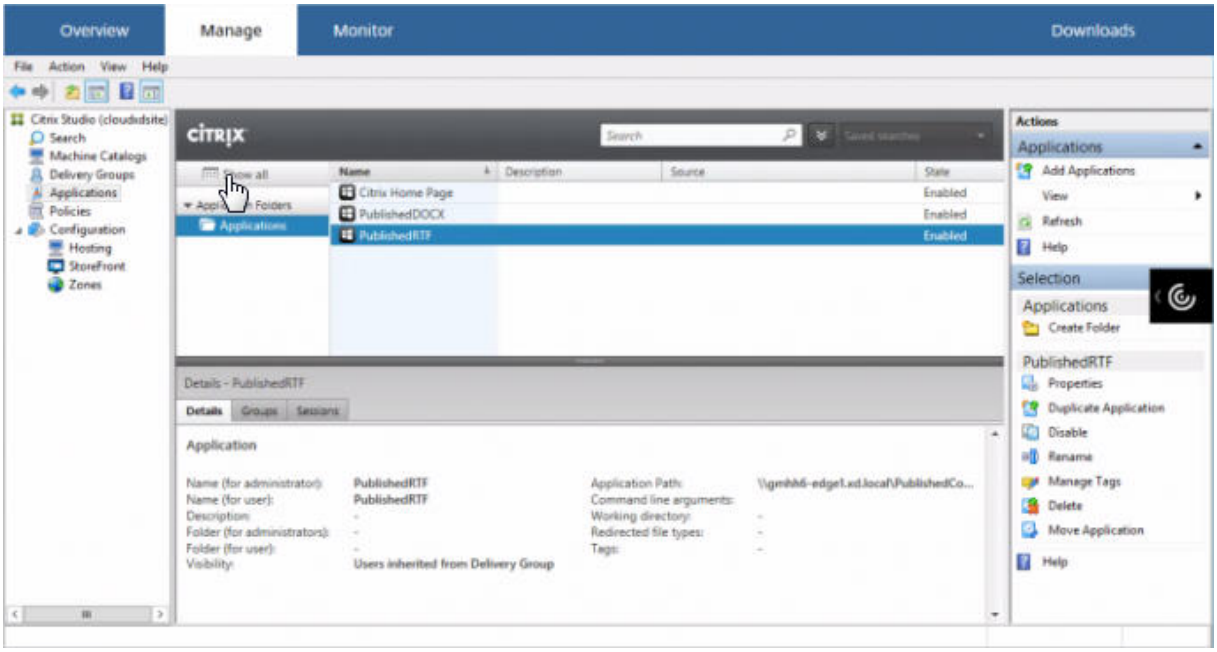


- Klicken Sie auf die Anwendungen PublishedRTF und PublishedDOCX. Beide Dokumente werden in einer lokal ausgeführten WordPad-Instanz geöffnet.

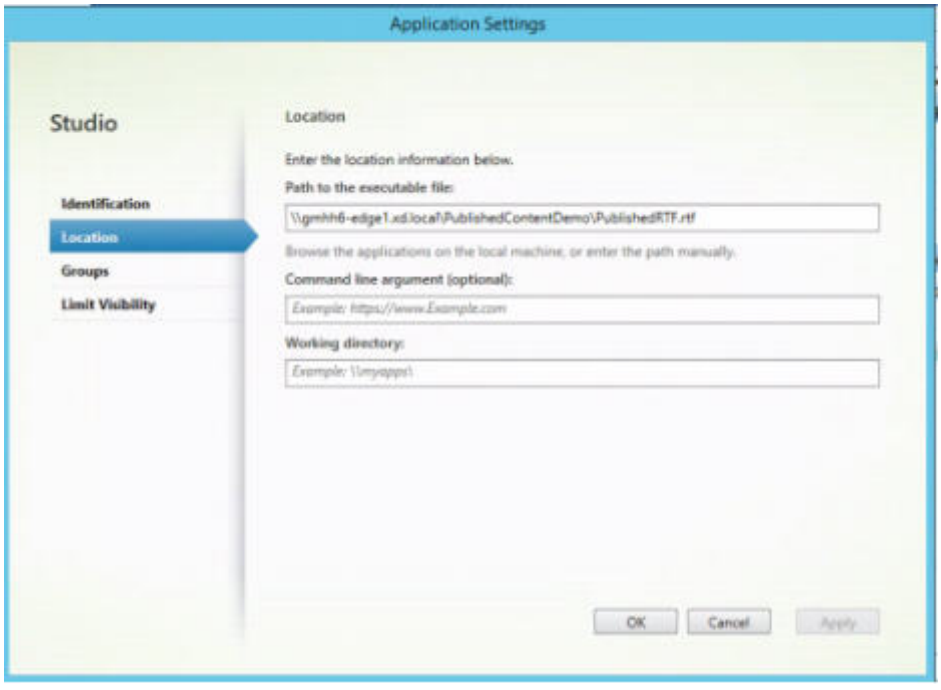


Anzeigen und Bearbeiten von Anwendungen mit veröffentlichtem Inhalt

Sie verwalten veröffentlichte Inhalte genauso wie andere Anwendungstypen. Veröffentlichte Inhalte erscheinen in der Liste Anwendungen in Studio und können dort bearbeitet werden.

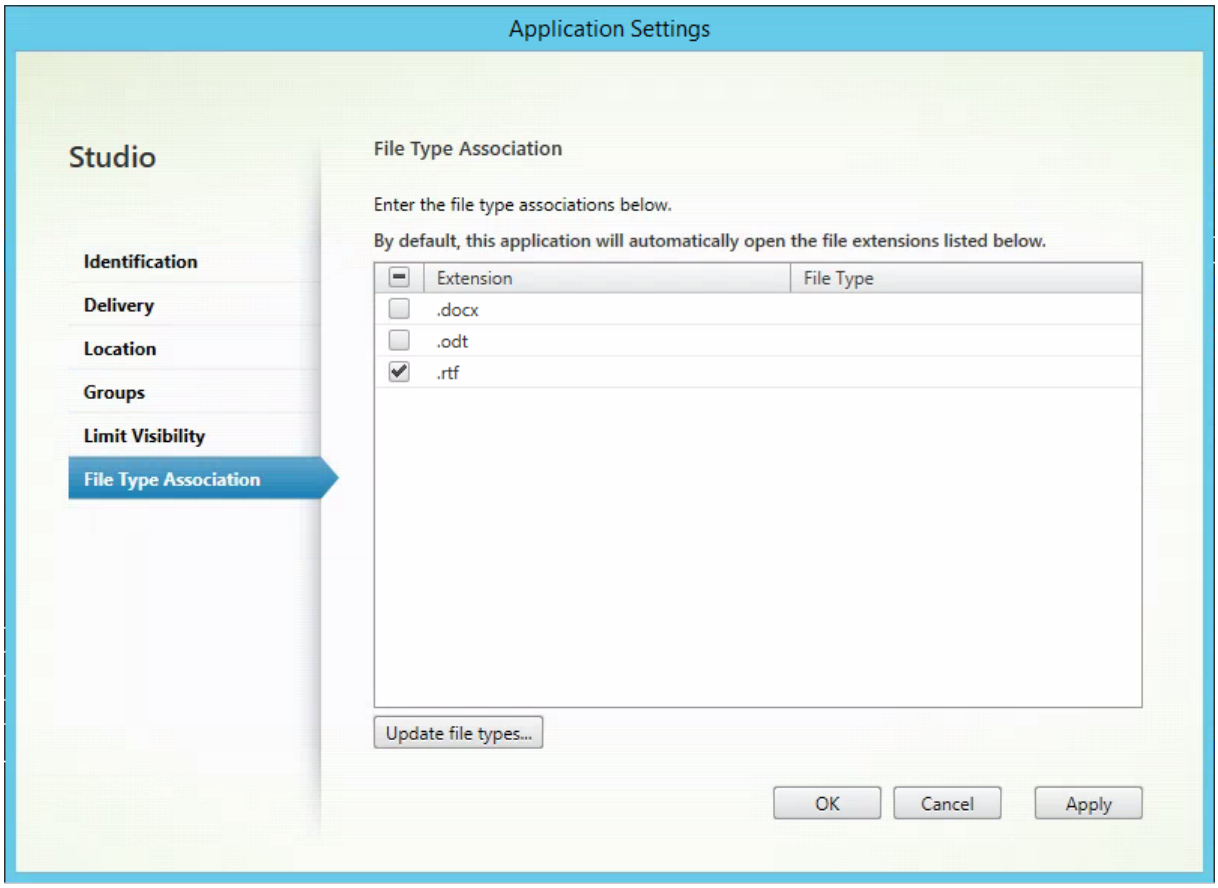


Anwendungseigenschaften (z. B. Benutzersichtbarkeit, Gruppenzuordnung und Verknüpfung) gelten für die veröffentlichten Inhalte. Befehlszeilenargumente und Arbeitsverzeichnis können Sie auf der Seite **Speicherort** jedoch nicht ändern. Zum Ändern der Ressource ändern Sie das Feld "Pfad zur ausführbaren Datei"auf dieser Seite.

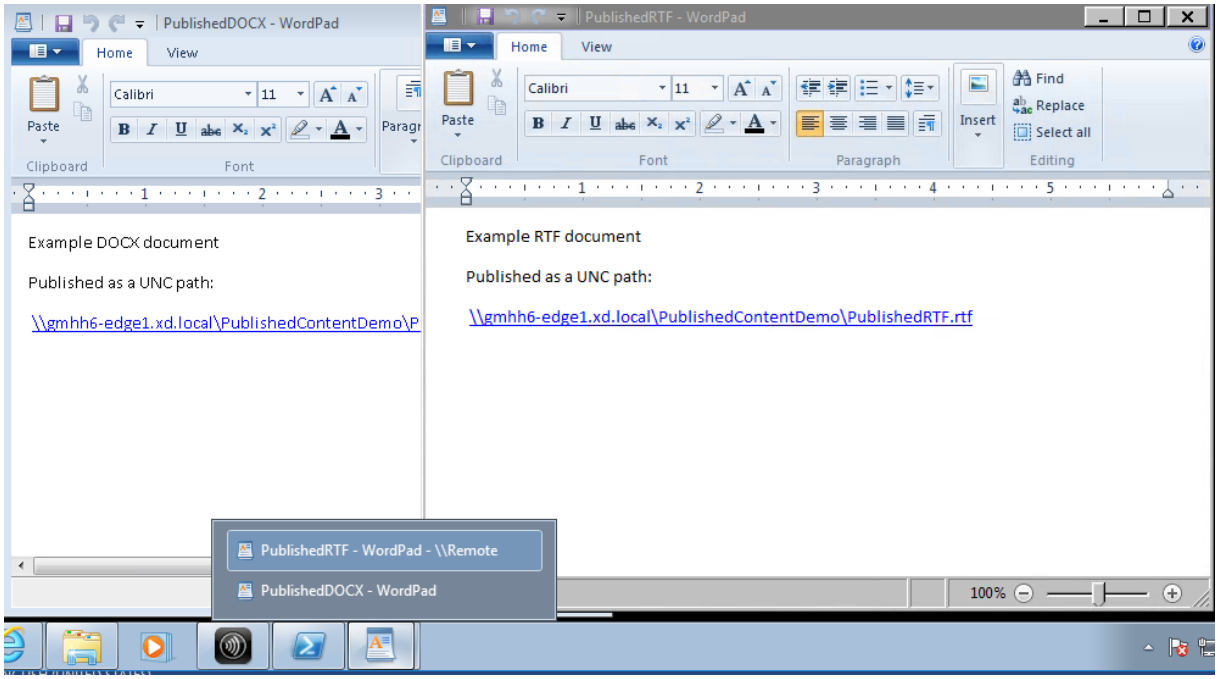


Um anstatt einer lokalen Anwendung eine veröffentlichte Anwendung zum Öffnen einer PublishedContent-Anwendung zu verwenden, bearbeiten Sie die Eigenschaft Dateitypzuordnung der veröffentlichten Anwendung. In diesem Beispiel wurde der veröffentlichten WordPad-Anwendung die Dateitypzuordnung für RTF-Dateien zugewiesen.

> **Wichtig:**
>
> Vor der Bearbeitung der Dateitypzuordnung versetzen Sie die Bereitstellungsgruppe in den Wartungsmodus. Nicht vergessen: Deaktivieren Sie den Wartungsmodus, wenn Sie fertig sind.



Aktualisieren Sie StoreFront, um die Änderungen an den Dateitypzuordnungen zu laden, und klicken Sie dann auf die Anwendungen PublishedRTF und PublishedDOCX. Beachten Sie den Unterschied. PublishedDOCX wird nach wie vor in der lokalen WordPad-Instanz geöffnet. PublishedRTF wird dagegen aufgrund der neuen Dateitypzuordnung in der veröffentlichten WordPad-Instanz geöffnet.



Weitere Informationen

- Erstellen von Maschinenkatalogen
- Erstellen von Bereitstellungsgruppen
- Ändern der Anwendungseigenschaften

Personal vDisk

February 4, 2020

Das Personal vDisk-Feature bietet die Einzelimageverwaltung für gepoolte und gestreamte Desktops, während Benutzer Anwendungen installieren und ihre Desktopeinstellungen anpassen können. Im Gegensatz zu traditionellen Virtual Desktop Infrastructure (VDI)-Bereitstellungen mit gepoolten Desktops, bei denen Benutzer Anpassungen und eigene Anwendungen verlieren, wenn der Administrator das Masterimage ändert, werden in Bereitstellungen mit persönlichen vDisks diese Änderungen beibehalten. Dies bedeutet, dass Administratoren die Masterimages auf einfache Weise zentral verwalten können, während Benutzer gleichzeitig von einer individuell angepassten Desktoperfahrung profitieren.

Persönliche vDisks erreichen diese Trennung, indem Sie alle auf der VM des Benutzers vorgenommenen Änderungen an einen separaten Datenträger, die persönliche vDisk, weiterleiten, die mit der VM des Benutzers verknüpft ist. Der Inhalt der persönlichen vDisk wird zur Laufzeit mit dem Inhalt des

Masterimages zusammengeführt, um eine einheitliche Erfahrung zu gewährleisten. Auf diese Weise können Benutzer immer noch auf die Anwendungen zugreifen, die der Administrator auf dem Masterimage zur Verfügung gestellt hat.

Persönliche vDisks bestehen aus zwei Teilen, die unterschiedliche Laufwerksbuchstaben verwenden und ungefähr gleich groß sind:

- Benutzerprofil: Dieser Teil enthält Benutzerdaten, Dokumente und das Benutzerprofil. Standardmäßig wird hierfür Laufwerk P: verwendet, Sie können aber einen anderen Laufwerksbuchstaben wählen, wenn Sie einen Maschinenkatalog mit Maschinen erstellen, die persönliche vDisks verwenden. Das verwendete Laufwerk hängt auch von der Einstellung für EnableUserProfileRedirection ab.
- Virtual Hard Disk-Datei (.vhd): Dieser Teil enthält alle anderen Objekte, z. B. Anwendungen, die unter C:\Programme installiert sind. Dieser Teil wird nicht in Windows Explorer angezeigt und benötigt seit Version 5.6.7 keinen Laufwerksbuchstaben.

Mit persönlichen vDisks können Anwendungen auf Abteilungsebene bereitgestellt werden und sie unterstützen auch Anwendungen, die von Benutzern heruntergeladen und installiert wurden, einschließlich solcher, für die Treiber (außer Phase-1-Treiber), Datenbanken und Maschinenverwaltungssoftware erforderlich ist. Wenn die Änderung eines Benutzers mit der Änderung eines Administrators kollidiert, können diese Änderungen mit einer persönlichen vDisk leicht und automatisch abgestimmt werden.

Außerdem können lokal verwaltete Anwendungen (z. B. solche, die von lokalen IT-Abteilungen bereitgestellt werden) auch in der Umgebung des Benutzers bereitgestellt werden. Der Benutzer bemerkt keine Unterschiede bei der Verwendung; mit persönlichen vDisks wird sichergestellt, dass alle Änderungen und alle installierten Anwendungen auf der vDisk gespeichert werden. In Fällen, bei denen eine Anwendung auf einer persönlichen vDisk genau mit einer Anwendung auf einem Masterimage übereinstimmt, wird die Version auf der persönlichen vDisk aus Platzspargründen verworfen, ohne dass der Benutzer den Zugriff auf die Anwendung verliert.

Persönliche vDisks werden physisch auf dem Hypervisor gespeichert, sie müssen sich aber nicht am gleichen Speicherort befinden wie andere auf dem virtuellen Desktop bereitgestellte Datenträger. Dadurch können sich die Kosten für persönlichen vDisk-Speicher verringern.

Wenn Sie während der Site-Erstellung eine Verbindung erstellen, legen Sie Speicherorte für die Datenträger fest, die von den virtuellen Maschinen verwendet werden. Sie können die persönlichen vDisks von den Datenträgern für das Betriebssystem trennen. Jede VM muss Zugriff auf den Speicherort der beiden Datenträger haben. Wenn Sie für beide lokalen Speicher verwenden, muss der Hypervisor in der Lage sein, auf beide zuzugreifen. Um dies zu gewährleisten, bietet Studio nur kompatible Speicherorte an. Später können Sie auch über **Konfiguration > Hosting** in Studio persönliche vDisks und Speicher dafür zu vorhandenen Hosts (aber nicht zu Maschinenkatalogen) hinzufügen.

Erstellen Sie regelmäßig ein Backup der persönlichen vDisks mit der bevorzugten Methode. vDisks

sind standardmäßige Volumes in der Speicherebene eines Hypervisors. Sie können genauso wie andere Volumes gesichert werden.

> **Hinweis:**
>
> Informationen zu PvD-Berichten, Nachrichten und bekannten Problemen finden Sie unter Problembehandlung.

Installation und Upgrade

August 18, 2021

Personal vDisk 7.x wird seit XenDesktop 5.6 bis zur aktuellen Version unterstützt. Für jede XenDesktop-Version werden in der Dokumentation unter "Systemanforderungen"die unterstützten Betriebssysteme für Virtual Delivery Agents (VDAs) sowie die unterstützten Versionen von Hosts (Virtualisierungsressourcen) und Provisioning Services aufgelistet. Weitere Informationen zu Provisioning Services-Aufgaben finden Sie in der aktuellen Dokumentation zu Provisioning Services.

Installieren und Aktivieren von PvD

Sie können PvD-Komponenten beim Installieren oder Aktualisieren eines VDAs für Desktopbetriebssysteme auf einer Maschine installieren und aktivieren. Die entsprechenden Aktionen werden auf den Seiten **Zusätzliche Komponenten** und **Features** des Installationsassistenten ausgewählt. Weitere Informationen finden Sie unter Installieren von VDAs.

Wenn Sie die PvD-Software nach der Installation des VDAs aktualisieren, verwenden Sie die PvD-MSI, die auf dem XenApp und XenDesktop-Installationsmedium verfügbar ist.

Aktivieren von PvD:

- PvD wird automatisch aktiviert, wenn Sie mit den Maschinenerstellungsdiensten (MCS) einen Maschinenkatalog erstellen, dessen Desktopbetriebssystemmaschinen eine persönliche vDisk verwenden.
- Wenn Sie Provisioning Services (PVS) verwenden, wird PvD automatisch aktiviert, wenn Sie während der Erstellung des Masterimages den Bestand aufnehmen oder wenn bei einem automatischen Update der Bestand aktualisiert wird.

Wenn Sie PvD-Komponenten installieren, aber während der VDA-Installation nicht aktivieren, können Sie daher mit demselben Image Desktops mit und ohne PvD erstellen, da PvD während der Katalogerstellung aktiviert wird.

Hinzufügen von persönlichen vDisks

Sie fügen Hosts persönliche vDisks hinzu, wenn Sie eine Site konfigurieren. Sie können denselben Speicher auf dem Host für VMs und persönliche vDisks verwenden oder Sie können einen anderen Speicher für persönliche vDisks auswählen.

Später können Sie auch persönliche vDisks und ihren Speicher vorhandenen Hosts (Verbindungen), jedoch nicht Maschinenkatalogen, hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich Konfiguration > Hosting.
2. Wählen Sie im Aktionsbereich Persönlichen vDisk-Speicher hinzufügen und geben Sie einen Speicherort an.

Aktualisieren von PvD

Die einfachste Methode, Personal vDisk von einer früheren 7.x-Version zu aktualisieren, ist das Aktualisieren der VDAs für Desktopbetriebssysteme mit der aktuellen XenDesktop-Version. Nehmen Sie anschließend den PvD-Bestand auf.

Deinstallieren von PvD

Sie können die PvD-Software mit einer der folgenden beiden Methoden deinstallieren:

- Deinstallieren Sie den VDA. Dabei wird die PvD-Software ebenfalls entfernt.
- Wenn Sie PvD mit der PvD-MSI aktualisiert haben, können Sie es über die Liste der Programme deinstallieren.

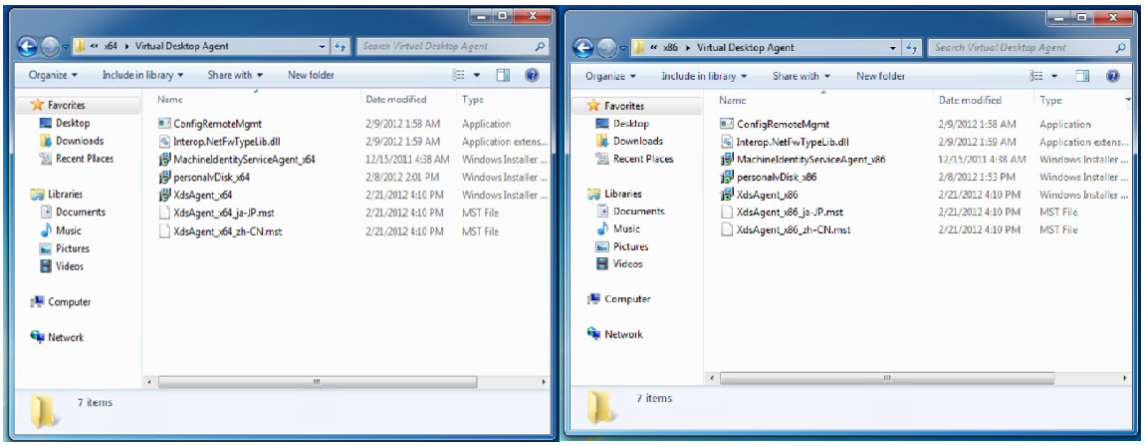
Wenn Sie PvD deinstallieren und dieselbe oder eine neuere Version neu installieren, erstellen Sie eine Sicherungskopie des Registrierungsschlüssels HKLM\Software\Citrix\personal vDisk\config, der Konfigurationseinstellungen für die Umgebung enthält, die sich geändert haben können. Nach der Installation von PvD können Sie die Registrierungswerte, die sich geändert haben, durch einen Vergleich mit der Sicherungskopie zurücksetzen.

Wichtige Hinweise zur Deinstallation von PvD

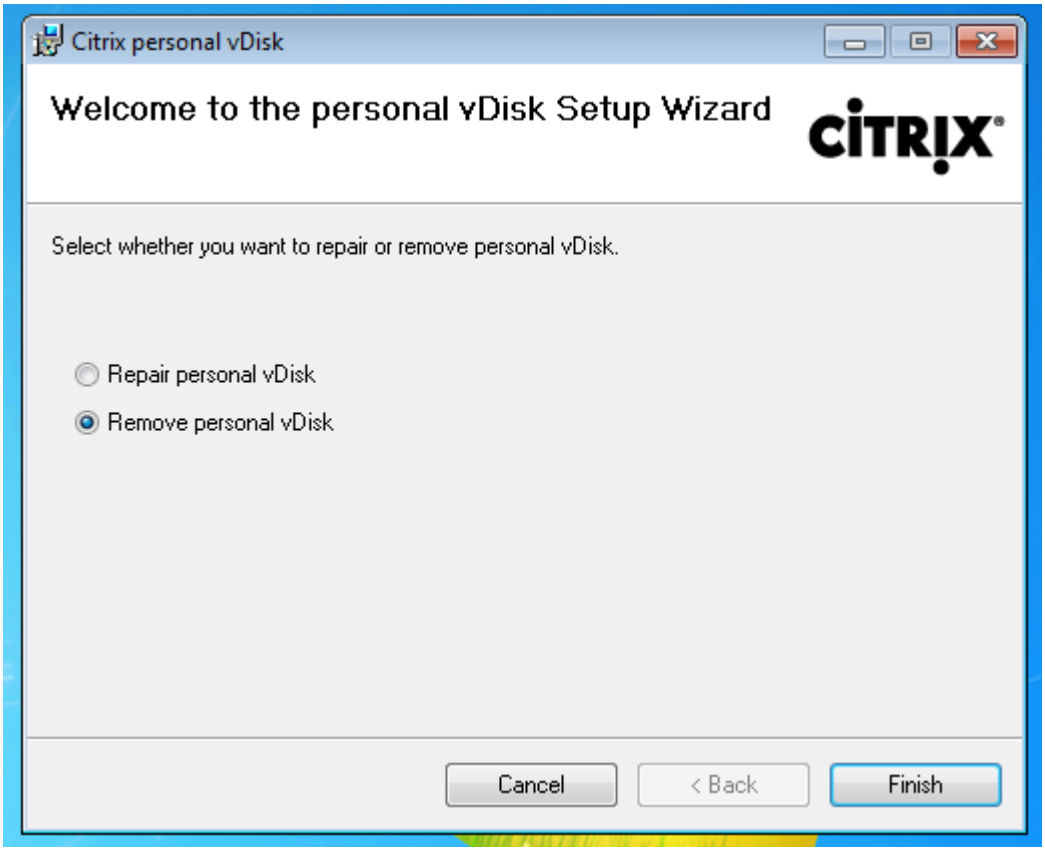
Die Deinstallation kann fehlschlagen, wenn eine persönliche vDisk mit Windows 7 (64 Bit) im Basisimage installiert ist. Um dieses Problem zu beheben, empfiehlt Citrix, die persönliche vDisk vor der Aktualisierung zu entfernen:

1. Wählen Sie die geeignete Kopie des vDisk-Installationsprogramms aus den XenApp/XenDesktop-Medien. Suchen Sie die aktuelle Version des MSI-Installationspakets für Personal vDisk im ISO-Image von XenApp/XenDesktop in einem der folgenden Verzeichnisse (je nachdem, ob die aktualisierte VM ein 32- oder 64-Bit-System verwendet):

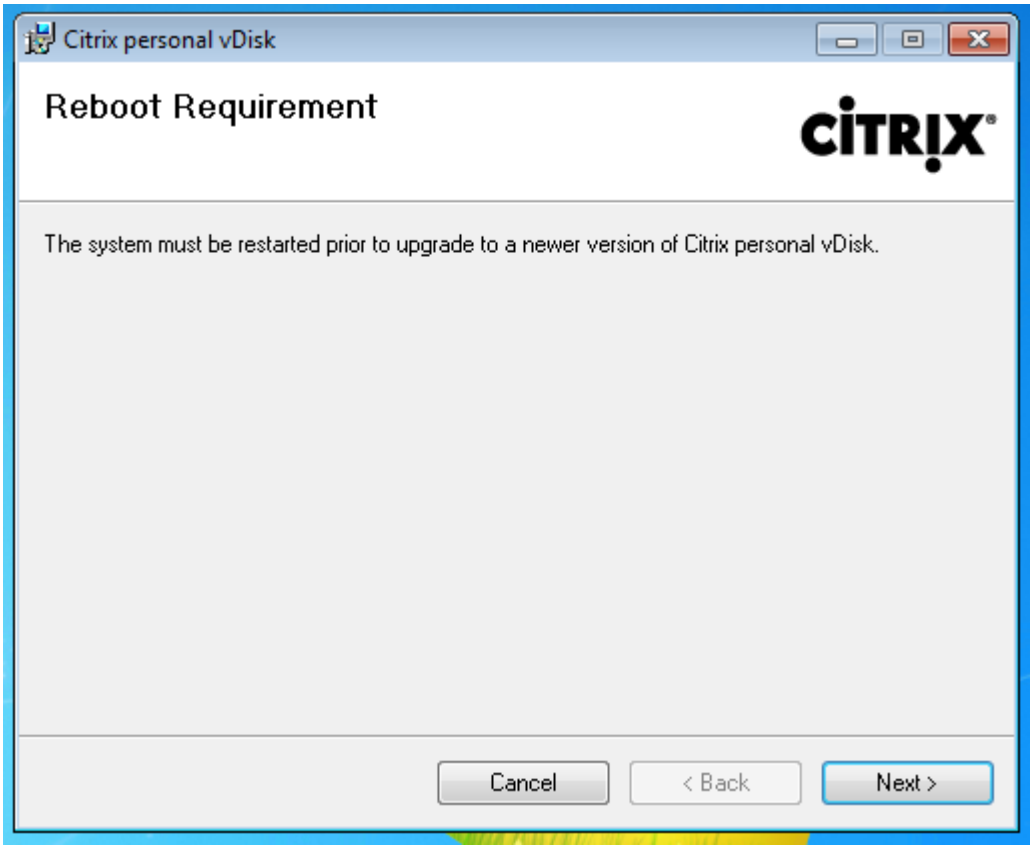
    - 32-Bit: XA und XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
    - 64-Bit: XA und XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



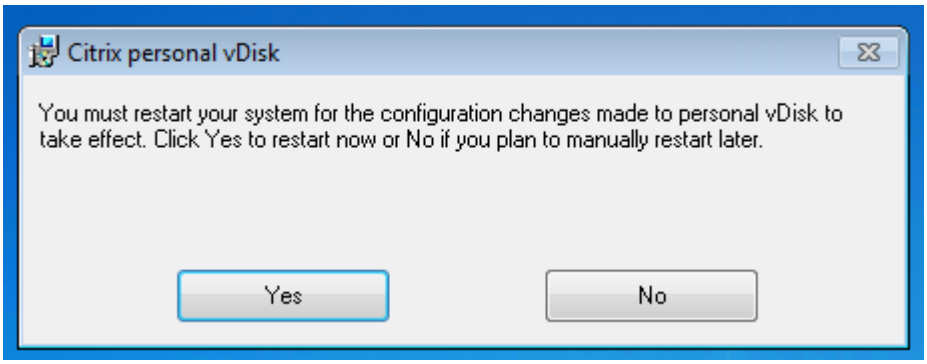
2. Entfernen Sie die installierte persönliche vDisk. Wählen Sie das MSI-Installationspaket für Personal vDisk, das in Schritt 1 gefunden wurde. Der Setupbildschirm für Personal vDisk wird angezeigt.
3. Wählen Sie Personal vDisk entfernen.
4. Klicken Sie auf **Fertig stellen**.



5. Die Seite zum erforderlichen Neustart wird angezeigt. Klicken Sie auf **Weiter**.



6. Klicken Sie auf **Ja**, um das System neu zu starten und die geänderte Konfiguration anzuwenden:



Konfigurieren und Verwalten

November 15, 2022

In diesem Abschnitt werden Themen erläutert, die beim Konfigurieren und Verwalten einer Personal vDisk (PvD)-Umgebung zu berücksichtigen sind. Darüber hinaus werden Best Practices und Aufgabenbeschreibungen behandelt.

Beachten Sie Folgendes beim Arbeiten in der Windows-Registrierung:

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Überlegungen zur Größe einer persönlichen vDisk

Die folgenden Faktoren beeinflussen die Größe des PvD-Hauptvolumes:

- **Größe der Anwendungen, die Benutzer auf ihren PvDs installieren**

  Bei Neustarts bestimmt PvD den im Anwendungsbereich verbleibenden freien Speicherplatz (UserData.v2.vhd). Wenn dieser Wert unter 10 % fällt, wird der Anwendungsbereich erweitert, indem ungenutzter Speicherplatz des Profilbereichs (standardmäßig der freie Speicherplatz auf dem Laufwerk P:) genutzt wird. Der zum Anwendungsbereich hinzugefügte Speicherplatz beträgt ungefähr 50 % des zusammengefassten freien Speicherplatzes von Anwendungs- und Profilbereich.

  Beispiel: Wenn der Anwendungsbereich auf einer 10 GB PvD, der standardmäßig eine Größe von 5 GB hat, den Wert 4,7 GB erreicht und der Profilbereich über 3 GB freien Speicherplatz verfügt, wird der zusätzliche Speicherplatz wie folgt berechnet:

  erweiterter Speicherplatz = (5,0 - 4,7) : 2 + 3,0 : 2 = 1,65 GB

  Der Wert für den zusätzlichen Speicherplatz kann nur ungefähr angegeben werden, da Abstriche für das Speichern von Protokollen und für Mehraufwand gemacht werden müssen. Die Berechnung und mögliche Größenänderung wird bei jedem Neustart ausgeführt.

- **Größe der Benutzerprofile (wenn keine separate Profilverwaltungslösung verwendet wird)**

  Zusätzlich zu dem für Anwendungen erforderlichen Speicherplatz muss auf persönlichen vDisks auch genügend Speicherplatz für das Speichern von Benutzerprofilen vorhanden sein. Schließen Sie alle nicht umgeleiteten speziellen Ordner (z. B. Dokumente und Musik) in Ihre Speicherplatzberechnungen ein. Vorhandene Profilgrößen sind in der Systemsteuerung (sysdm.cpl) verfügbar.

  Einige Profilumleitungslösungen speichern Stubdateien (Sentineldateien) anstelle echter Profildaten. Zu Beginn kann es aussehen, als würden die Profillösungen keine Daten speichern. Sie

nutzen jedoch einen Dateiverzeichniseintrag pro Stubdatei im Dateisystem, was ungefähr 4 KB pro Datei ausmacht. Wenn Sie eine solche Lösung verwenden, schätzen Sie die Größe anhand der echten Profildaten und nicht basierend auf den Stubdateien.

Unternehmensanwendungen zur Dateifreigabe, wie ShareFile und Dropbox, synchronisieren oder laden Daten möglicherweise auf die Profildatenbereiche der persönlichen vDisks von Benutzern herunter. Wenn Sie derartige Anwendungen verwenden, veranschlagen Sie genug Speicherplatz für diese Daten.

- **Mehraufwand durch die virtuelle Festplattenvorlage, die den PvD-Bestand enthält**

  Die virtuelle Festplattenvorlage enthält die PvD-Bestandsdaten (Sentineldateien, die zum Inhalt des Masterimages gehören). Der PvD-Anwendungsbereich wird von dieser virtuellen Festplatte erstellt. Da jede Sentineldatei bzw. jeder Sentinelordner einen Dateiverzeichniseintrag im Dateisystem enthält, nimmt der Inhalt der virtuellen Festplattenvorlage PvD-Anwendungsspeicherplatz in Anspruch, bevor der Endbenutzer überhaupt eine Anwendung installiert hat. Sie können die Größe der virtuellen Festplattenvorlage bestimmten, indem Sie zum Masterimage navigieren, nachdem der Bestand aufgenommen wurde. Sie können zur ungefähren Berechnung auch die folgende Formel verwenden:

  Größe der virtuellen Festplattenvorlage = (Anzahl der Dateien des Basisimage) x 4 KB

  Sie ermitteln die Anzahl der Dateien und Ordner, indem Sie mit der rechten Maustaste auf das Laufwerk C: des Images der Basis-VM klicken und Eigenschaften auswählen. Beispiel: Ein Image mit 250.000 Dateien ergibt eine virtuelle Festplattenvorlage von ungefähr 1.024.000.000 Bytes (nicht ganz 1 GB). Dieser Speicherplatz ist nicht für Anwendungsinstallationen im PvD-Anwendungsbereich verfügbar.

- **Mehraufwand für PvD-Imageupdatevorgänge**

  Während PvD-Imageupdatevorgänge ausgeführt werden, muss im Stammverzeichnis der PvD (standardmäßig P:) genug Speicherplatz vorhanden sein, um die Änderungen der zwei Imageversionen mit den Änderungen, die der Benutzer an der PvD vorgenommen hat, zusammenzuführen. Normalerweise reserviert die PvD einige Hundert MB für diesen Zweck. Durch Extradaten, die im Laufwerk P: gespeichert wurden, ist jedoch möglicherweise nicht genug Speicherplatz zum Durchführen des Imageupdates vorhanden. Mit dem PvD-Poolstatistikscript (auf dem XenDesktop-Installationsmedium im Ordner "Support/Tools/Scripts") oder mit dem Überwachungstool für PvD-Imageupdates (im Ordner "Support/Tools/PvdTool") können Sie die PvD-Datenträger in einem Katalog identifizieren, für die ein Update geplant ist und die fast voll sind.

  Das Vorhandensein von Antivirenprodukten kann sich darauf auswirken, wie lange das Durchführen einer Bestandsaktualisierung oder eines Updates dauert. Die Leistung kann verbessert werden, wenn Sie CtxPvD.exe und CtxPvDSvc.exe der Ausschlussliste des Antivirenprodukts hinzufügen. Diese Dateien befinden sich im Ordner C:\Programme\Citrix\personal

vdisk\bin. Durch das Ausschließen dieser ausführbaren Dateien vom Antivirenscan kann die Bestandsaktualisierungs- und Imageupdateleistung um das Zehnfache beschleunigt werden.

- **Mehraufwand für unerwartete Zunahme (unerwartete Anwendungsinstallationen usw.)**

  Kalkulieren Sie zusätzlichen Speicherplatz ein (entweder eine feste Menge oder einen Prozentsatz der vDisk-Größe), um auf unerwartete Anwendungsinstallationen von Benutzern während der Bereitstellung vorbereitet zu sein.

Konfigurieren von Größe und Zuordnung der persönlichen vDisk

Sie können den Algorithmus für die automatische Größenänderung, der die Größe der virtuellen Festplatte relativ zum Laufwerk P: festlegt, manuell anpassen, indem Sie die Ausgangsgröße der virtuellen Festplatte festlegen. Dies ist nützlich, wenn Sie beispielsweise wissen, dass Benutzer zahlreiche Anwendungen installieren werden, die nicht alle auf die virtuelle Festplatte passen werden, selbst wenn die Größe mit dem Algorithmus angepasst wurde. In dieser Situation können Sie die Ausgangsgröße des Anwendungsspeicherplatzes erhöhen, damit die vom Benutzer installierten Anwendungen genug Platz haben.

Passen Sie die Ausgangsgröße der virtuellen Festplatte am besten auf einem Masterimage an. Sie können die Größe der virtuellen Festplatte auch auf einem virtuellen Desktop anpassen, wenn ein Benutzer nicht genügend Speicherplatz für die Installation einer Anwendung hat. Sie müssen diesen Vorgang jedoch auf allen betroffenen virtuellen Desktops wiederholen, da Sie die Ausgangsgröße der virtuellen Festplatte nicht in einem bereits erstellten Katalog ändern können.

Stellen Sie sicher, dass die virtuelle Festplatte groß genug für das Speichern von Definitionsdateien von Antivirensoftware ist, da diese Dateien normalerweise sehr umfangreich sind.

Legen Sie die folgenden Registrierungsschlüssel in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config fest. (Ändern Sie keine anderen Einstellungen in diesem Registrierungsschlüssel.) Alle Einstellungen müssen auf dem Masterimage angegeben werden (außer für MinimumVHDSizeInMB, was auf einer individuellen Maschine geändert werden kann). Auf dem Masterimage angegebene Einstellungen werden bei der nächsten Aktualisierung des Images angewendet.

- **MinimumVHDSizeMB**

  Gibt die Mindestgröße (in Megabyte) des Anwendungsteils (C:) der persönlichen vDisk an. Die neue Größe muss größer als die vorhandene Größe und kleiner als die Größe des Datenträgers abzüglich PvDReservedSpaceMB sein.

  Durch das Erhöhen dieses Werts wird freier Speicherplatz vom Profilteil der vDisk dem Laufwerk C: zugeteilt. Diese Einstellung wird ignoriert, wenn ein geringerer Wert als die aktuelle Größe des Laufwerks C: verwendet wird oder wenn EnableDynamicResizeOfAppContainer auf 0 eingestellt ist.

Standard = 2048

- **EnableDynamicResizeOfAppContainer**

  Aktiviert oder deaktiviert den Algorithmus zur dynamischen Größenänderung.

  - Bei der Einstellung auf 1 wird der Anwendungsspeicherplatz auf C: automatisch geändert, wenn der freie Speicherplatz auf C: unter 10 % fällt. Zulässige Werte sind 1 und 0. Ein Neustart muss durchgeführt werden, damit die Änderungen wirksam werden.
  - Bei der Einstellung auf 0 wird die Größe der virtuellen Festplatte basierend auf der Methode ermittelt, die in XenDesktop-Versionen vor 7.x verwendet wurde.

  Standard = 1

- **EnableUserProfileRedirection**

  Aktiviert oder deaktiviert die Umleitung des Benutzerprofils auf die vDisk.

  - Bei der Einstellung auf 1 leitet PvD das Benutzerprofil auf die vDisk um (standardmäßig auf P:). Profile werden entsprechend einem Windows-Standardprofil im Allgemeinen nach P:\Users umgeleitet. Durch die Umleitung werden die Profile beibehalten, falls der PvD-Desktop zurückgesetzt werden muss.
  - Bei der Einstellung auf 0 ist der gesamte Speicherplatz auf der vDisk, abzüglich PvDReservedSpaceMB, dem Laufwerk C: (dem Anwendungsteil der vDisk) zugewiesen, und das vDisk-Laufwerk (P:) ist im Windows Explorer ausgeblendet. Citrix empfiehlt das Deaktivieren der Umleitung durch die Einstellung auf 0, wenn Sie Citrix Profilverwaltung oder eine andere Roamingprofillösung verwenden.

    Durch diese Einstellung bleiben die Profile in C:\Users erhalten statt auf die vDisk umgeleitet zu werden, und sie ermöglicht der Roamingprofillösung das Verwalten der Profile.

    Dieser Wert stellt sicher, dass der ganze Speicherplatz auf P: Anwendungen zugewiesen ist.

    Bei einer Einstellung dieses Werts auf 0 wird davon ausgegangen, dass eine Profilverwaltungslösung eingesetzt wird. Das Deaktivieren der Profilumleitung ohne eine Roamingprofillösung einzusetzen wird nicht empfohlen, da die Profile sonst bei nachfolgenden PvD-Zurücksetzungsvorgängen gelöscht werden.

  Ändern Sie diese Einstellung nicht, wenn das Image aktualisiert wird, da sie zwar nicht den Speicherort vorhandener Profile ändert, jedoch den gesamten Speicherplatz auf der PvD dem Laufwerk C: zuweist und die PvD ausblendet.

  Konfigurieren Sie diesen Wert vor dem Bereitstellen eines Katalogs. Nach dem Bereitstellen eines Katalogs können Sie diesen Wert nicht mehr ändern.

Wichtig: Ab XenDesktop 7.1 werden Änderungen an diesem Wert nicht angewendet, wenn Sie ein Imageupdate ausführen. Legen Sie den Wert des Schlüssels fest, wenn Sie die Kataloge erstellen, von denen die Profile erstellt werden. Sie können das Umleitungsverhalten später nicht mehr ändern.

Standard = 1

- **PercentOfPvDForApps**

  Legt die Teilung zwischen dem Anwendungsteil (C:) und dem Profilteil der vDisk fest. Dieser Wert wird beim Erstellen neuer VMs verwendet sowie während Imageupdates, wenn EnableDynamicResizeOfAppContainer auf 0 eingestellt ist.

  Das Ändern der Einstellung PercentOfPvDForApps macht nur einen Unterschied, wenn die Einstellung EnableDynamicResizeOfAppContainer auf 0 festgelegt ist. Standardmäßig ist EnableDynamicResizeOfAppContainer auf 1 (aktiviert) festgelegt, d. h. dass der AppContainer (Laufwerk C:) nur erweitert wird, wenn er fast voll ist (d. h. dynamisch), und zwar wenn weniger als 10 % freier Speicherplatz vorhanden ist.

  Durch das Erhöhen von PercentOfPvDForApps wird nur der Gesamtspeicherplatz für die Apps erhöht. Der Speicherplatz wird jedoch nicht sofort verfügbar gemacht. Sie müssen zudem die Zuordnungsteilung im Masterimage konfigurieren, die dann beim nächsten Imageupdate angewendet wird.

  Wenn Sie bereits einen Katalog mit Maschinen mit der Einstellung 1 für EnableDynamicResizeOfAppContainer generiert haben, ändern Sie die Einstellung im Masterimage für das nächste Update auf 0 und konfigurieren Sie die entsprechende Zuordnungsteilung. Die angeforderte Teilungsgröße wird eingehalten, solange sie größer als die aktuell zugeteilte Größe des Laufwerks C ist.

  Wenn Sie komplette Kontrolle über die Speicherplatzteilung haben möchten, legen Sie den Wert auf 0 fest. Damit haben Sie die komplette Kontrolle über die Größe des Laufwerks C und die Erweiterung des Laufwerks ist nicht davon abhängig, dass ein Benutzer eine bestimmte Menge Speicherplatz unter dem Schwellenwert in Anspruch nimmt.

  Standard = 50 % (beiden Teilen wird der gleiche Speicherplatz zugeteilt)

- **PvDReservedSpaceMB**

  Legt die Größe des reservierten Speicherplatzes (in MB) auf der vDisk für das Speichern von Personal vDisk-Protokollen und anderen Daten fest.

  Wenn in Ihrer Bereitstellung XenApp 6.5 (oder eine frühere Version) und Anwendungsstreaming verwendet wird, erhöhen Sie diesen Wert um die Größe des RadeCache.

  Standard = 512

- **PvDResetUserGroup**

Gilt nur für XenDesktop 5.6: Ermöglicht der angegebenen Gruppe von Benutzern, eine persönliche vDisk zurücksetzen. Höhere XenDesktop-Releases verwenden dafür die delegierte Administration.

Weitere Einstellungen:

- **Windows Update-Dienst:** Stellen Sie sicher, dass im Masterimage für Windows Updates die Einstellung "Nie auf Update prüfen"und für den Windows Update-Dienst die Einstellung "Deaktiviert"ausgewählt ist. Falls der Windows Update Service auf der PvD ausgeführt werden muss, wird durch die Einstellung Never Check for Update verhindert, dass die Updates auf den zugeordneten Maschinen installiert werden.

  Dieser Dienst wird von Windows 8 Store benötigt, um Modern UI-Apps installieren zu können.
- **Windows-Updates:** Diese schließen Updates für Internet Explorer ein und müssen auf das Masterimage angewendet werden.
- **Updates, die Neustarts erfordern:** Bei auf das Masterimage angewendeten Windows-Updates sind, abhängig von den im Update enthaltenen Patches, möglicherweise mehrere Neustarts erforderlich, damit die Installation vollständig ausgeführt wird. Stellen Sie vor der PvD-Bestandsaktualisierung sicher, dass Sie das Masterimage richtig neu starten, damit die Installation von ausgeführten Windows Updates vollständig abgeschlossen wird.
- **Anwendungsupdates:** Aktualisieren Sie Anwendungen, die auf dem Masterimage installiert sind, um Speicherplatz auf den vDisks von Benutzern zu sparen. Auf diese Weise vermeiden Sie den doppelten Aufwand, der durch das Durchführen von Updates auf den vDisks einzelner Benutzer entstehen würde.

Überlegungen zu Anwendungen auf dem Masterimage

Es kann zu Konflikten zwischen Software und der von PvD erstellten Benutzerumgebung kommen. Zum Vermeiden von Konflikten müssen Sie die Software auf dem Masterimage (nicht auf den individuellen Maschinen) installieren. Auch wenn es keine Konflikte zwischen der Software und der Ausführung von PvD gibt, empfiehlt Citrix, sie auf dem Masterimage zu installieren.

Folgende Anwendungen müssen auf dem Masterimage installiert werden:

- Agents und Clients (z. B. System Center Configuration Manager-Agent, App-V-Client, Citrix Receiver)
- Anwendungen, die vorrangige Starttreiber installieren oder ändern
- Anwendungen, die Drucker- oder Scannersoftware bzw. -treiber installieren
- Anwendungen, die den Windows-Netzwerkstapel ändern
- VM-Tools wie VMware Tools und XenServer Tools

Folgende Anwendungen sollten auf dem Masterimage installiert werden:

- Anwendungen, die einer großen Anzahl an Benutzern zur Verfügung gestellt werden. Deaktivieren Sie für die folgenden Fälle vor der Bereitstellung die Anwendungsupdates:
  - Unternehmensanwendungen, die Volumenlizenzierung verwenden, z. B. Microsoft Office und Microsoft SQL Server
  - Gängige Anwendungen wie Adobe Reader, Firefox und Chrome
- Große Anwendungen, z. B. SQL Server, Visual Studio und Anwendungsframeworks wie .NET

Die folgenden Empfehlungen und Einschränkungen gelten für Anwendungen, die Benutzer auf Maschinen mit persönlichen vDisks installiert haben. Einige dieser Empfehlungen können nicht durchgesetzt werden, wenn Benutzer Administratorrechte haben:

- Benutzer sollten Anwendungen nicht vom Masterimage deinstallieren und dann auf ihrer persönlichen vDisk neu installieren.
- Vorsicht beim Aktualisieren oder Deinstallieren von Anwendungen auf dem Masterimage. Nachdem Sie die Version einer Anwendung auf dem Image installiert haben, installiert ein Benutzer möglicherweise eine Add-On-Anwendung (z. B. ein Plug-In), das diese Version erfordert. Im Fall einer solchen Abhängigkeit kann es nach dem Aktualisieren oder Deinstallieren der Anwendung auf dem Image beim Add-On zu einer Fehlfunktion kommen. Beispiel: Microsoft Office 2010 ist auf einem Masterimage installiert und ein Benutzer installiert Visio 2010 auf der persönlichen vDisk. Bei einem Upgrade von Office auf dem Masterimage kann die lokal installierte Visio-Anwendung unbrauchbar werden.
- Software mit Lizenzen, die von Hardware abhängig sind (entweder durch ein Dongle oder signaturbasierte Hardware), wird nicht unterstützt.

Überlegungen zu Provisioning Services

Wenn Sie Provisioning Services mit PvD verwenden:

- Das SOAP-Dienstkonto muss zum Administratorknoten von Studio hinzugefügt werden und es muss über die Rolle "Maschinenadministrator"oder eine höhere Rolle verfügen. Dadurch wird sichergestellt, dass die PvD-Desktops in den Status "Preparing"versetzt werden, wenn die Provisioning Services (PVS) vDisk auf "Production"hochgestuft wird.
- Das Versionsverwaltungsfeature von Provisioning Services muss zum Aktualisieren der persönlichen vDisk verwendet werden. Wenn die Version auf "Production"hochgestuft wird, versetzt der SOAP-Dienst die PvD-Desktops in den Status "Preparing".
- Die Größe der persönlichen vDisk sollte immer größer als der Provisioning Services-Schreibcachedatenträger sein, da Provisioning Services sonst fälschlicherweise die persönliche vDisk als Schreibcache nehmen könnte.
- Nach dem Erstellen einer Bereitstellungsgruppe können Sie die persönliche vDisk mit dem Überwachungstool für PvD-Imageupdates oder den Größenänderungs- und poolstats-Skripts

(personal-vdisk-poolstats.ps1) überwachen.

Veranschlagen Sie genug Schreibcache. Bei normalem Betrieb werden die meisten Benutzerschreibvorgänge (Änderungen) von PvD erfasst und an die persönliche vDisk umgeleitet. Daher könnten Sie theoretisch die Größe des Provisioning Services-Schreibcache verringern. Wenn PvD jedoch nicht aktiv ist, z. B. während Imageupdatevorgängen, kann ein kleines Provisioning Services-Schreibcache schnell voll sein und den Absturz von Maschinen verursachen.

Citrix empfiehlt, dass Sie die Größe des Provisioning Services-Schreibcache entsprechend den Empfehlungen für Provisioning Services veranschlagen und dann Speicherplatz hinzufügen, der dem Doppelten der virtuellen Festplattenvorlage auf dem Masterimage entspricht (für Zusammenführungen). Es ist unwahrscheinlich, dass ein Zusammenführungsvorgang so viel Speicherplatz beansprucht, aber es ist möglich.

Wenn Sie mit Provisioning Services einen Katalog mit PvD-aktivierten Maschinen bereitstellen:

- Folgen Sie den Anweisungen in der Provisioning Services-Dokumentation.
- Sie können die Drosselungseinstellungen für Energieaktionen ändern, indem Sie die Verbindung in Studio bearbeiten.
- Zum Aktualisieren der Provisioning Services-vDisk installieren bzw. aktualisieren Sie Anwendungen und Software und starten Sie die vDisk neu. Aktualisieren Sie dann den PvD-Bestand und fahren Sie die VM herunter. Stufen Sie anschließend die neue Version auf "Production"hoch. Die PvD-Desktops im Katalog sollten automatisch in den Zustand "Preparing"versetzt werden. Wenn dies nicht der Fall ist, prüfen Sie, ob das SOAP-Dienstkonto Maschinenadministrator- oder höhere Privilegien auf dem Controller hat.

Mit dem Testmodusfeature von Provisioning Services können Sie einen Testkatalog mit Maschinen erstellen, die ein aktualisiertes Masterimage verwenden. Wenn die Tests die Funktionsfähigkeit des Katalogs bestätigen, stufen Sie ihn auf "Production"hoch.

Überlegungen zu den Maschinenerstellungsdiensten

Wenn Sie mit den Maschinenerstellungsdiensten (MCS) einen Katalog mit PvD-aktivierten Maschinen bereitstellen:

- Folgen Sie den Anweisungen in der XenDesktop-Dokumentation.
- Aktualisieren Sie nach dem Erstellen des Masterimages den PvD-Bestand und schalten Sie dann die VM aus (PvD funktioniert nicht ordnungsgemäß, wenn Sie die VM nicht ausschalten). Erstellen Sie einen Snapshot vom Masterimage.
- Geben Sie im Assistenten zum Erstellen von Maschinenkatalogen die Größe und den Laufwerksbuchstaben der persönlichen vDisk an.

- Nach dem Erstellen einer Bereitstellungsgruppe können Sie die persönliche vDisk mit dem Überwachungstool für PvD-Imageupdates oder den Größenänderungs- und poolstats-Skripts (personal-vdisk-poolstats.ps1) überwachen.
- Sie können die Drosselungseinstellungen für Energieaktionen ändern, indem Sie die Verbindung in Studio bearbeiten.
- Wenn Sie das Masterimage aktualisieren, nehmen Sie nach dem Aktualisieren der Anwendungen und der anderen Software auf dem Image den PvD-Bestand auf und schalten Sie anschließend die VM aus. Erstellen Sie einen Snapshot vom Masterimage.
- Überprüfen Sie mit dem Überwachungstool für PvD-Imageupdates oder mit dem Skript "personal-vdisk-poolstats.ps1", ob genügend Speicherplatz auf jeder PvD-aktivierten VM vorhanden ist, die das aktualisierte Masterimage verwendet.
- Nach dem Aktualisieren des Maschinenkatalogs werden die PvD-Desktops in den Zustand "Preparing"versetzt, während sie die Änderungen am neuen Masterimage verarbeiten. Die Desktops werden entsprechend der während des Maschinenupdates festgelegten Rolloutstrategie aktualisiert.
- Während die PvD im Zustand "Preparing"ist, überwachen Sie sie mit dem Überwachungstool für PvD-Imageupdates oder mit dem Skript "personal-vdisk-poolstats.ps1".

Ausschließen von Dateien und Ordner von vDisks

Mit Regeldateien schließen Sie Dateien und Ordner von vDisks aus. Dies ist möglich, während die persönlichen vDisks bereitgestellt werden. Die Regeldateien werden custom_*_rules.template.txt genannt und befinden sich im Ordner \config. Anmerkungen in den einzelnen Dateien erhalten zusätzliche Informationen.

Durchführen einer Bestandsaktualisierung beim Aktualisieren eines Masterimages

Wenn Sie PvD nach einer Aktualisierung des Masterimages aktivieren, muss der Bestand des Datenträgers aktualisiert und ein neuer Snapshot erstellt werden.

Wenn Sie eine Anwendung installieren, die Binärdateien im Benutzerprofil des Administrators ablegt, ist die Anwendung nicht für Benutzer freigegebener virtueller Desktops (einschließlich solcher, die auf gepoolten Maschinenkatalogen basieren und mit PvD-Maschinenkatalogen gepoolt sind) verfügbar, da Masterimages nicht von Benutzern sondern von Administratoren verwaltet werden. Benutzer müssen solche Anwendungen selber installieren.

Es ist ratsam, nach jedem Schritt in diesem Verfahren einen Snapshot des Images zu erstellen:

1. Aktualisieren Sie das Masterimage, indem Sie auf der Maschine Anwendungen oder Betriebssystemupdates installieren und das System konfigurieren.

Bei Masterimages, die auf Windows XP basieren und die Sie mit persönlichen vDisks bereitstellen möchten, müssen Sie sicherstellen, dass keine Dialogfelder offen sind (z. B. Meldungen zur Bestätigung von Softwareinstallationen oder Aufforderungen, nicht signierte Treiber zu verwenden). Offene Dialogfelder auf Masterimages in dieser Umgebung verhindern, dass sich der VDA beim Delivery Controller registriert. Sie können Aufforderungen für nicht signierte Treiber in der Systemsteuerung verhindern. Navigieren Sie zu "System > Hardware > Treibersignierung" und wählen Sie die Option zum Ignorieren von Warnungen.

2. Fahren Sie die Maschine herunter. Klicken Sie bei Windows 7-Maschinen auf Abbrechen, wenn Citrix Personal vDisk das Herunterfahren behindert.
3. Klicken Sie im Citrix Personal vDisk-Dialogfeld auf Bestand aktualisieren. Dieser Vorgang kann einige Minuten dauern.

   Wichtig: Wenn Sie das anschließende Herunterfahren unterbrechen (selbst wenn Sie nur eine kleine Änderung am Image vornehmen), stimmt der Bestand der persönlichen vDisk nicht mehr mit dem Masterimage überein. Dies führt dazu, dass das Personal vDisk-Feature nicht mehr funktioniert. Wenn Sie das Herunterfahren unterbrechen, müssen Sie die Maschine neu starten, herunterfahren und auf "Bestand aktualisieren"klicken, wenn Sie dazu aufgefordert werden.
4. Erstellen Sie, nachdem der Bestandvorgang die Maschine heruntergefahren hat, einen Snapshot des Masterimages.

Sie können einen Bestand in eine Netzwerkfreigabe exportieren und ihn anschließend in ein Masterimage importieren. Weitere Informationen finden Sie unter Exportieren und Importieren eines PvD-Bestands.

Konfigurieren von Drosselungseinstellungen für Verbindungen

Der Citrix Brokerdienst steuert den Energiezustand der Maschinen, die Desktops und Anwendungen bereitstellen. Der Brokerdienst kann mehrere Hypervisors über einen Delivery Controller steuern. Die Interaktion zwischen einem Controller und dem Hypervisor wird durch Broker-Energieaktionen gesteuert. Aktionen, die den Energiezustand einer Maschine ändern, wird eine Priorität zugewiesen und dann werden sie über einen Drosselungsmechanismus an den Hypervisor gesendet, damit es nicht zur Überlastung kommt. Die folgenden Einstellungen wirken sich auf die Drosselung aus. Diese Werte werden festgelegt, indem Sie eine Verbindung (Seite "Erweitert") in Studio bearbeiten.

Konfigurieren von Drosselungswerten für eine Verbindung

1. Wählen Sie im Studio-Navigationsbereich Konfiguration > Hosting.
2. Wählen Sie die Verbindung und dann im Bereich Aktionen die Option Verbindung bearbeiten.
3. Sie können die folgenden Werte ändern:

- **Gleichzeitige Aktionen (alle Typen):** das zulässige Maximum für gleichzeitig ausgeführte Energieaktionen. Diese Einstellung wird als absoluter Wert und als Prozentsatz der Verbindung mit dem Hypervisor angegeben. Der niedrigere der beiden Werte wird verwendet.

  Standard = 100 absolut, 20%
- **Gleichzeitige Updates für Personal vDisk-Bestand:** das zulässige Maximum für gleichzeitige Personal vDisk-Energieaktionen. Diese Einstellung wird als absoluter Wert und als Prozentsatz der Verbindung angegeben. Der niedrigere der beiden Werte wird verwendet.

  Standard = 50 absolut, 25 %

  Sie kalkulieren den absoluten Wert, indem Sie den Gesamtwert für IOPS (TIOPS) bestimmen, den der Datenträger des Endbenutzers unterstützt (dies sollte vom Hersteller festgelegt sein oder berechnet werden). Veranschlagen Sie 350 IOPS pro VM (IOPS/VM), um die Anzahl der VMs zu bestimmen, die jeweils auf dem Datenträger aktiv sein können. Sie berechnen diesen Wert, indem Sie den Gesamtwert für IOPS durch IOPS/VM teilen.

  Beispiel: Wenn der Wert für den Datenträger des Endbenutzers 14.000 IOPS ist, ist die Anzahl der aktiven VMs 14.000 IOPS : 350 IOPS/VM = 40.
- **Höchstanzahl neue Aktionen pro Minute:** maximale Anzahl der neuen Energieaktionen, die pro Minute an den Hypervisor gesendet werden können. Sie wird als absoluter Wert angegeben.

  Default= 10

Identifizieren der optimalen Werte für diese Einstellungen in der Bereitstellung:

1. Messen Sie mit den Standardwerten die Reaktionszeit für das Imageupdate eines Testkatalogs. Dies ist die Differenz zwischen der Startzeit eines Imageupdates (T1) und dem Zeitpunkt, wenn der VDA auf der letzten Maschine des Katalogs beim Controller registriert wird (T2). Reaktionszeit = T2-T1.
2. Messen Sie die Ein- und Ausgabevorgänge pro Sekunde (IOPS) auf dem Hypervisorspeicher während des Imageupdates. Diese Daten können als Benchmark für die Optimierung dienen. (Die Standardwerte sind möglicherweise die beste Einstellung. Unter Umständen erreicht das System den maximalen IOPS-Wert, sodass die Einstellungswerte herabgesetzt werden müssen.)
3. Ändern Sie den Wert für "Gleichzeitige Updates für Personal vDisk-Bestand"wie unten beschrieben und lassen Sie alle anderen Einstellungen unverändert.

   a) Erhöhen Sie den Wert um 10 und messen Sie die Reaktionszeit nach jeder Änderung. Fahren Sie fort, den Wert um 10 zu erhöhen und messen Sie das Ergebnis, bis die Reaktionszeit abnimmt oder keine Änderung mehr auftritt.

   b) Wenn durch das Erhöhen des Werts im vorherigen Schritt keine Verbesserung erzielt wurde, verringern Sie den Wert schrittweise um 10 und messen Sie die Reaktionszeit

nach jeder Verringerung. Wiederholen Sie diesen Vorgang, bis sich die Reaktionszeit nicht mehr ändert oder verbessert. Dieser Wert ist wahrscheinlich der optimale Wert für die PvD-Energieaktion.

4. Wenn Sie den Einstellungswert für die PvD-Energieaktion festgelegt haben, optimieren Sie nacheinander die Werte für die gleichzeitigen Aktionen (alle Typen) und die Höchstanzahl der neuen Aktionen pro Minute. Folgen Sie den oben erläuterten Schritten (schrittweises Erhöhen und Verringern der Werte), um verschiedene Werte zu testen.

Verwenden von Microsoft System Center Configuration Manager 2007 mit PvD

System Center Configuration Manager (Configuration Manager) 2012 erfordert keine besondere Konfiguration und kann auf die gleiche Weise wie alle anderen Anwendungen auf dem Masterimage installiert werden. Die folgenden Informationen gelten nur für System Center Configuration Manager 2007. Configuration Manager-Versionen vor Configuration Manager 2007 werden nicht unterstützt.

Führen Sie die folgenden Schritte aus, um die Configuration Manager 2007 Agent-Software in einer PvD-Umgebung zu verwenden.

1. Installieren Sie den Client-Agent auf dem Masterimage.
    a) Installieren Sie den Configuration Manager-Client auf dem Masterimage.
    b) Beenden Sie den ccmexec-Dienst (SMS-Agent) und deaktivieren Sie ihn.
    c) Löschen Sie SMS- oder Clientzertifikate wie folgt aus dem Zertifikatspeicher des lokalen Computers:
        - Gemischter Modus: Certificates (Lokaler Computer)\SMS\Certificates
        - Einheitlicher Modus
            - Certificates (Lokaler Computer)\Personal\Certificates
            - Löschen Sie das Clientzertifikat, das von Ihrer Zertifizierungsstelle ausgestellt wurde (normalerweise eine interne PKI).
    d) Löschen Sie C:\Windows\smscfg.ini oder benennen Sie die Datei um.
2. Entfernen Sie Informationen, die den Client eindeutig identifizieren.
    a) (Optional) Löschen Sie die Protokolldateien unter C:\Windows\System32\CCM\Logs oder verschieben Sie sie.
    b) Installieren Sie ggf. den Virtual Delivery Agent und nehmen Sie den PvD-Bestand auf.
    c) Fahren Sie das Masterimage herunter, erstellen Sie einen Snapshot und erstellen Sie dann mit diesem Snapshot einen Maschinenkatalog.
3. Überprüfen Sie Personal vDisk und starten Sie die Dienste. Führen Sie diese Schritte einmal auf jedem PvD-Desktop aus, nachdem er zum ersten Mal gestartet wurde. Dazu können Sie beispielsweise ein Domänen-GPO verwenden.

- Bestätigen Sie, dass PvD aktiv ist, indem Sie prüfen, ob der Registrierungsschlüssel HKLM\Software\Citrix\personal vDisk\config\virtual vorhanden ist.
- Stellen Sie den ccmexec-Dienst (SMS-Agent) auf "Automatic"ein und starten Sie den Dienst. Der Configuration Manager-Client kontaktiert den Configuration Manager-Server und ruft neue, eindeutige Zertifikate und GUIDs ab.

Tools

May 14, 2021

Mit den folgenden Tools und Hilfsprogrammen können Sie PvD-Vorgänge anpassen, vereinfachen und überwachen.

Benutzerdefinierte Regeldateien

Mit den von PvD bereitgestellten benutzerdefinierten Regeldateien können Sie das folgende Standardverhalten von PvD-Imageupdates ändern:

- Die Sichtbarkeit von Dateien auf der PvD
- Die Art der Zusammenführung von vorgenommenen Änderungen
- Einstellungen zur Beschreibbarkeit der Dateien

Detaillierte Anweisungen zu den benutzerdefinierten Regeldateien und dem CoW-Feature finden Sie in den Kommentaren zu den Dateien, die sich unter C:\ProgramData\Citrix\personal vDisk\Config auf der Maschine befinden, auf der PvD installiert ist. Die Dateien mit dem Namen custom_* erläutern die Regeln und wie sie aktiviert werden.

Ändern der Größe und poolstats-Skripts

Es gibt zwei Skripts zum Überwachen und Verwalten der Größe der PvDs. Sie befinden sich im Ordner "Support\Tools\Scripts"auf dem XenDesktop-Installationsmedium. Sie können auch das Überwachungstool für PvD-Imageupdates im Ordner Support\Tools\Scripts\PvdTool verwenden.

Verwenden Sie "resize-personalvdisk-pool.ps1"zum Vergrößern der PvDs in allen Desktops eines Katalogs. Die folgenden Snap-Ins oder Module für den Hypervisor müssen auf der Maschine installiert werden, auf der Studio ausgeführt wird:

- XenServer erfordert XenServerPSSnapin
- vCenter erfordert vSphere PowerCli
- System Center Virtual Machine Manager erfordert die VMM-Konsole

Mit "personal-vdisk-poolstats.ps1"können Sie den Status von Imageupdates überprüfen sowie den Speicherplatz für Anwendungen und Benutzerprofile in einer PvD-Gruppe. Führen Sie das Skript vor dem Update eines Images aus, um zu prüfen, ob Desktops genug Speicherplatz haben. Dadurch werden Fehler während des Updates verhindert. Für das Skript muss die Windows Management Instrumentation (WMI-In)-Firewall auf den PvD-Desktops aktiviert sein. Sie können die Firewall auf dem Masterimage aktivieren oder über GPO.

Wenn ein Imageupdate fehlschlägt, zeigt der Eintrag in der Spalte "Update"die Ursache an.

Zurücksetzen des Anwendungsbereichs

Wenn ein Desktop durch die Installation einer fehlerhaften Anwendung oder aus einem anderen Grund beschädigt wird, können Sie den Anwendungsbereich der PvD auf den (leeren) Herstellerstandard zurücksetzen. Beim Zurücksetzen bleiben die Benutzerprofildaten erhalten.

Zurücksetzen des Anwendungsbereichs der PvD:

- Melden Sie sich am Desktop des Benutzers als Administrator an. Starten Sie eine Eingabeaufforderung und führen Sie den Befehl **C:\Programme\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset** aus.
- Navigieren Sie in Citrix Director zum Desktop des Benutzers. Klicken Sie auf **Reset Personal vDisk** und anschließend auf **OK**.

Exportieren und Importieren eines PvD-Bestands

Der Imageupdateprozess ist ein zentraler Teil der Bereitstellung neuer Images auf PvD-Desktops und umfasst Anpassungen, damit vorhandene persönliche vDisks mit dem neuen Basisimage funktionieren. Bei Bereitstellungen, die Maschinenerstellungsdienste (MCS) verwenden, können Sie einen Bestand von einer aktiven VM auf eine Netzwerkfreigabe exportieren und dann in ein Masterimage importieren. Mit diesem Bestand auf dem Masterimage wird eine Differenz berechnet. Obwohl das Feature zum Exportieren bzw. Importieren des Bestands nicht verwendet werden muss, kann es die Leistung des Imageupdateprozesses verbessern.

Sie müssen ein Administrator sein, um das Feature zum Exportieren/Importieren des Bestands zu verwenden. Falls erforderlich, authentifizieren Sie sich bei der Dateifreigabe für den Export/Import mit "net use". Der Benutzerkontext muss auf alle für den Export/Import verwendeten Dateifreigaben zugreifen können.

Exportieren

- Führen Sie zum Exportieren eines Bestands den Exportbefehl als Administrator auf einer Maschine aus, auf der sich ein VDA mit aktivierter PvD befindet (Mindestversion 7.6):


```
Ctxpvdsvc.exe exportinventory "\<path-to-export-location>"
```

Die Software erkennt den Speicherort des aktuellen Bestands und exportiert den Bestand an den angegebenen Speicherort in einen Ordner mit dem Namen "ExportedPvdInventory". Auszug aus der Befehlsausgabe:

```
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
    exportinventory
\share location\ExportedInventory
Current inventory source location C:\CitrixPvD\Settings\Inventory
    \VER-LAS
...
Exporting current inventory to location \ ... .
...
Deleting any pre-existing inventory folder at \ ... .
.Successfully exported current inventory to location \ ... .
    Error code = OPS
<!--NeedCopy-->
```

- Zum Importieren eines zuvor exportierten Bestands führen Sie den Importbefehl als Administrator auf dem Masterimage aus:

Importieren

Führen Sie den Importbefehl als Administrator auf dem Masterimage aus.

```
Ctxpvdsvc.exe importinventory "\<path-to-exported-inventory>"
```

Der <Pfad zum exportierten Bestand> muss der vollständige Pfad für die Bestandsdateien sein; in der Regel ist das <Netzwerkspeicherort\ExportedPvdInventory>.

Der Bestand wird aus dem Importspeicherort abgerufen (zuvor wurde er mit dem Befehl zum Exportieren des Bestands hierher exportiert) und in den Bestandsspeicher auf dem Masterimage importiert. Auszug aus der Befehlsausgabe:

```
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
    importinventory
\share location\ExportedInventory\ExportedPvdInventory
Importing inventory \share location\ExportedInventory\
    ExportedPvdInventory
...
Successfully added inventory \share location\ExportedInventory\
    ExportedPvdInventory to the
store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
<!--NeedCopy-->
```

Nach dem Exportvorgang sollte die Netzwerkfreigabe die folgenden Dateinamen enthalten. Nach dem Importvorgang sollte der Bestandsspeicher auf dem Masterimage die gleichen Dateinamen enthalten.

- Components.DAT
- files_rules
- folders_rules
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Anzeigen, Meldungen und Problembehandlung

August 18, 2021

Überwachen von PvD über Berichte

Sie können ein Diagnosetool zum Überwachen der Änderungen verwenden, die von Benutzern an beiden Bereichen persönlicher vDisks (Benutzerdaten- und Anwendungsbereiche) vorgenommen werden. Zu diesen Änderungen gehören Anwendungen, die von Benutzern installiert wurden, und von ihnen geänderte Dateien. Die Änderungen werden in einer Reihe von Berichten erfasst.

1. Führen Sie auf der zu überwachenden Maschine **C:\Programme\Citrix\personal vDisk\bin\CtxPvdDiag.ex** aus.
2. Navigieren Sie zu dem Speicherort, an dem die Berichte und Protokolle gespeichert werden sollen, legen Sie fest, welche Berichte generiert werden sollen, und klicken Sie auf **OK**. Die verfügbaren Berichte sind unten aufgeführt.

Softwarestrukturbericht: Dieser Bericht generiert die beiden Dateien Software.Dat.Report.txt und Software.Dat.delta.txt.

In Software.Dat.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Software"vorgenommen wurden. Der Bericht besteht aus den folgenden Abschnitten:

- List of applications installed on the base: Anwendungen, die auf Ebene 0 installiert wurden

- List of user installed software: Anwendungen, die vom Benutzer im Anwendungsbereich der persönlichen vDisk installiert wurden
- List of software uninstalled by user: ursprünglich auf Ebene 0 installierte Anwendungen, die vom Benutzer entfernt wurden

Weitere Informationen zu Software.Dat.delta.txt finden Sie im Strukturdeltabericht.

Systemstrukturbericht: In der Datei SYSTEM.CurrentControlSet.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\System"vorgenommen wurden. Der Bericht besteht aus den folgenden Abschnitten:

- List of user installed services: vom Benutzer installierte Dienste und Treiber
- Startup of following services were changed: Dienste und Treiber, deren Starttyp vom Benutzer geändert wurde

Sicherheitsstrukturbericht: In der Datei SECURITY.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Security"vorgenommen wurden.

Strukturbericht für die Sicherheitskontenverwaltung (SAM): In der Datei SAM.DAT.Report.txt werden die Änderungen erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\SAM" vorgenommen wurden.

Strukturdeltabericht: In der Datei Software.Dat.delta.txt werden alle hinzugefügten und entfernten Registrierungsschlüssel und alle Werte erfasst, die vom Benutzer an der Struktur "HKEY_LOCAL_MACHINE\Software"geändert wurden.

Personal vDisk-Protokolle: Die Protokolldateien Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log und vDeskService-<[#]>.log werden standardmäßig im Ordner *P:\Users\<Benutzerkonto>\AppData\Local\Temp\PVDLOGS* erstellt, jedoch an den ausgewählten Speicherort verschoben.

Windows-Betriebssystemprotokolle:

- EvtLog_App.xml und EvtLog_System.xml sind die Anwendungs- und Systemereignisprotokolle im XML-Format aus dem Personal vDisk-Volume.
- Die Protokolle Setupapi.app.log und setuperr.log enthalten Protokollmeldungen bezüglich der Ausführung von msiexec.exe bei der Installation von Personal vDisk.
- Setupapi.dev.log enthält Protokollmeldungen über die Geräteinstallation.
- Msinfo.txt enthält die Ausgabe von msinfo32.exe. Informationen hierzu finden Sie in der Dokumentation von Microsoft.

Dateisystembericht: In der Datei FileSystemReport.txt werden die Änderungen erfasst, die vom Benutzer in folgenden Bereichen des Dateisystems vorgenommen wurden:

- Files Relocated: Dateien auf Ebene 0, die vom Benutzer zur vDisk verschoben wurden. Dateien der Ebene 0 sind Dateien, die aus dem Masterimage von der Maschine geerbt wurden, der die

persönliche vDisk angefügt ist.
- Files Removed: Dateien auf Ebene 0, die durch eine Benutzeraktion (z. B. Entfernen einer Anwendung) verborgen wurden.
- Files Added (MOF,INF,SYS): Dateien mit der Erweiterung "mof", "inf"oder "sys", die vom Benutzer der Personal vDisk hinzugefügt wurden (z. B. bei der Installation einer Anwendung wie Visual Studio 2010, bei der eine MOF-Datei für die automatische Wiederherstellung registriert wird).
- Files Added Other: andere Dateien, die der vDisk vom Benutzer hinzugefügt wurden (z. B. beim Installieren einer Anwendung).
- Base Files Modified But Not Relocated: Dateien auf Ebene 0, die vom Benutzer geändert wurden, jedoch nicht von den Personal vDisk-Kernelmodustreibern in der vDisk erfasst wurden.

Imageupdates

Wenn Sie in Studio eine PvD-aktivierte Maschine in einem Maschinenkatalog auswählen, können Sie auf der Registerkarte "PvD"den Überwachungsstatus während Imageupdates sowie die geschätzte Abschlusszeit und den Fortschritt verfolgen. Folgende Zustandsanzeigen sind während eines Imageupdates möglich: Ready, Preparing, Waiting, Failed und Requested.

Ein Imageupdate kann aus verschiedenen Gründen fehlschlagen, einschließlich zu wenig Speicherplatz oder weil ein Desktop die PvD nicht rechtzeitig findet. Wenn Studio angibt, dass ein Imageupdate fehlgeschlagen ist, wird ein Fehlercode mit beschreibendem Text angezeigt, um Sie bei der Problembehandlung zu unterstützen. Verwenden Sie das Überwachungstool für PvD-Imageupdates oder das Skript "personal-vdisk-poolstats.ps1"zum Überwachen des Imageupdatevorgangs und um Fehlercodes für das Problem zu erhalten.

Wenn ein Imageupdate fehlschlägt, finden Sie in den folgenden Protokolldateien weitere Informationen zur Problembehandlung:

- PvD-Dienstprotokoll: C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- PvD-Aktivierungsprotokoll: P:\PVDLOGS\PvDActivation.log.txt

Der aktuelle Inhalt ist am Ende der Protokolldatei.

Fehlermeldungen: 7.6 und höher

Die folgenden Fehler gelten nur für PvD Version 7.6 und höher:

- **Ein interner Fehler ist aufgetreten. Weitere Informationen finden Sie in den Personal vDisk-Protokollen. Fehlercode %d (% s)**

Dieser Code gilt für alle nicht kategorisierten Fehler und hat daher keinen numerischen Wert. Alle unerwarteten Fehler während der Bestandserstellung oder Personal vDisk-Updates haben diesen Fehlercode.

  - Sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.
  - Wenn dieser Fehler während der Aktualisierung des Katalogs auftritt, führen Sie ein Rollback des Katalogs auf die vorherige Version des Masterimages aus.

- **Die Regeldateien enthalten Syntaxfehler. Weitere Informationen finden Sie in den Protokollen.**

  Fehlercode 2. Die Regeldatei enthält Syntaxfehler. Die Personal vDisk-Protokolldatei enthält den Namen der Regeldatei und die Zeile, in der der Syntaxfehler gefunden wurde. Beheben Sie den Syntaxfehler in der Regeldatei und wiederholen Sie den Vorgang.

- **Der in Personal vDisk gespeicherte Bestand, der der vorherigen Version des Masterimages entspricht, ist beschädigt oder nicht lesbar.**

  Fehlercode 3. Der letzte Bestand ist unter *\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST\UserData.V2.vhd* gespeichert. Stellen Sie den Bestand entsprechend der letzten Version des Masterimages wieder her, indem Sie den Ordner "VER-LAST"von einer funktionierenden PvD-Maschine importieren, die der vorherigen Version des Masterimages zugeordnet ist.

- **Der in Personal vDisk gespeicherte Bestand, der der vorherigen Version des Masterimages entspricht, ist eine höhere Version.**

  Fehlercode 4. Die Ursache ist eine PvD-Versionsinkompatibilität zwischen dem letzten Masterimage und dem aktuellen Masterimage. Installieren Sie die aktuelle Version von Personal vDisk auf dem Masterimage und aktualisieren Sie den Katalog erneut.

- **Änderungsjournalüberlauf erkannt.**

  Fehlercode 5. Ein USN-Journalüberlauf wurde durch zahlreiche Änderungen am Masterimage während der Bestandserstellung verursacht. Wenn dieses Problem nach mehreren Versuchen weiterhin auftritt, ermitteln Sie mit Process Monitor, ob die Drittanbietersoftware während der Erstellung des Bestands zahlreiche Dateien erstellt oder löscht.

- **Personal vDisk konnte keinen an das System angeschlossenen Datenträger zum Speichern von Benutzerdaten finden.**

  Fehlercode 6. Überprüfen Sie zunächst, ob die PvD über die Hypervisor-Konsole mit der VM verbunden ist. Dieser Fehler wird in der Regel durch Software ausgelöst, die zum Vermeiden von Datenverlust den Zugriff auf die PvD verhindert. Wenn die PvD mit der VM verbunden ist, fügen Sie eine Ausnahme für den verbundenen Datenträger in der Konfiguration der Software zum Vermeiden von Datenverlust hinzu.

- **Das System wurde nach der Installation noch nicht neu gestartet. Starten Sie es neu, damit die Änderungen übernommen werden.**

  Fehlercode 7. Starten Sie den Desktop neu und wiederholen Sie den Vorgang.

- **Beschädigte Installation. Installieren Sie Personal vDisk neu.**

  Fehlercode 8. Installieren Sie Personal vDisk neu und versuchen Sie es noch einmal.

- **Der Personal vDisk-Bestand ist nicht auf dem aktuellen Stand. Aktualisieren Sie den Bestand auf dem Masterimage und versuchen Sie es noch einmal.**

  Fehlercode 9. Der Personal vDisk-Bestand wurde vor dem Herunterfahren des Desktops nicht auf dem Masterimages aktualisiert. Starten Sie das Masterimage neu und fahren Sie den Desktop mit der Option "Persönliche vDisk aktualisieren"herunter. Erstellen Sie dann einen neuen Snapshot und aktualisieren Sie damit den Katalog.

- **Beim Start von Personal vDisk ist ein interner Fehler aufgetreten Weitere Informationen finden Sie in den Personal vDisk-Protokollen.**

  Fehlercode 10. Die Ursache ist möglicherweise, dass der PvD-Treiber aufgrund eines internen Fehlers oder Beschädigung der persönlichen vDisk keine Virtualisierungssitzung starten kann. Starten Sie den Desktop über den Controller neu. Wenn das Problem weiterhin auftritt, sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.

- **Personal vDisk-Timeout bei dem Versuch, ein Speichermedium für die Personalisierungseinstellungen der Benutzer zu finden.**

  Fehlercode 11. Dieser Fehler tritt auf, wenn der PvD-Treiber den PvD-Datenträger nicht innerhalb von 30 Sekunden nach dem Neustart findet. Die Ursache ist normalerweise ein nicht unterstützter SCSI-Controllertyp oder Speicherlatenz. Wenn dieses Problem bei allen Desktops im Katalog auftritt, ändern Sie den der Vorlagen-VM bzw. Master-VM zugeordneten SCSI-Controllertyp in einen Typ, der von Personal vDisk unterstützt wird. Wenn dieses Problem nur bei einigen Desktops im Katalog auftritt, wird dies möglicherweise durch Speicherlatenz-Spitzen verursacht, weil zahlreiche Desktops gleichzeitig gestartet werden. Beschränken Sie die Einstellung für die maximale Anzahl aktiver Energieaktionen für die Hostverbindung.

- **Personal vDisk wurde deaktiviert, da das System nicht sicher heruntergefahren wurde. Starten Sie die Maschine neu.**

  Fehlercode 12. Möglicherweise kann ein Desktop bei aktivierter PvD den Startvorgang nicht abschließen. Starten Sie den Desktop neu. Wenn das Problem weiterhin auftritt, beobachten Sie den Startvorgang des Desktops über die Hypervisor-Konsole und prüfen Sie, ob der Desktop abstürzt. Wenn ein Desktop während des Starts abstürzt, stellen Sie die PvD aus einem Backup (wenn vorhanden) wieder her oder setzen Sie die PvD zurück.

- **Der zum Bereitstellen von Personal vDisk angegebene Laufwerksbuchstabe ist nicht verfügbar.**

Fehlercode 13. Die Ursache ist möglicherweise, dass Personal vDisk den PvD-Datenträger nicht über das vom Administrator angegebene Laufwerk bereitstellen kann. Der PvD-Datenträger kann nicht bereitgestellt werden, wenn der Laufwerksbuchstabe bereits von anderer Hardware verwendet wird. Wählen Sie einen anderen Buchstaben als Bereitstellungspunkt für die persönliche vDisk aus.

- **Fehler beim Installieren von Personal vDisk-Kernelmodustreibern.**

  Fehlercode 14. Personal vDisk installiert Treiber während der ersten Bestandsaktualisierung nach der Installation. Einige Antivirenprodukte verhindern die Installation von Treibern außerhalb eines Installationsprogramms. Deaktivieren Sie vorübergehend den in Echtzeit ausgeführten Antivirenscan oder fügen Sie der Antivirensoftware während der ersten Bestandserstellung Ausnahmen für die PvD-Treiber hinzu.

- **Es konnte kein Snapshot des Systemvolumes erstellt werden. Stellen Sie sicher, dass der Volumeschattenkopie-Dienst aktiviert ist.**

  Fehlercode 15. Dieser Fehler kann auftreten, weil der Volumeschattenkopie-Dienst deaktiviert ist. Aktivieren Sie den Volumeschattenkopie-Dienst und versuchen Sie noch einmal, den Bestand aufzunehmen.

- **Fehler beim Aktivieren des Änderungsjournals. Warten Sie einige Minuten und versuchen Sie es noch einmal.**

  Fehlercode 16. Personal vDisk verwendet das Änderungsjournal für das Verfolgen von Änderungen am Masterimage. Wenn PvD bei einer Bestandsaktualisierung erkennt, dass das Änderungsjournal deaktiviert ist, versucht PvD, es zu aktivieren. Der Fehler tritt auf, wenn die Aktivierung fehlschlägt. Warten Sie ein paar Minuten und versuchen Sie es noch einmal.

- **Nicht genügend freier Speicherplatz auf dem Systemvolume.**

  Fehlercode 17. Für das Imageupdate ist nicht genug freier Speicherplatz auf dem Laufwerk C des Desktops vorhanden. Erweitern Sie das Systemvolume oder entfernen Sie nicht verwendete Dateien vom Systemvolume. Das Imageupdate sollte nach dem nächsten Neustart erneut beginnen.

- **Es ist nicht genügend freier Speicherplatz im Personal vDisk-Speicher. Erweitern Sie den Personal vDisk-Speicher.**

  Fehlercode 18. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk während des Imageupdatevorgangs vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher. Das Imageupdate sollte nach dem nächsten Neustart erneut beginnen.

- **Der Personal vDisk-Speicher ist überbucht. Erweitern Sie den Personal vDisk-Speicher.**

  Fehlercode 19. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk für die in vollem Umfang bereitgestellte “UserData.V2.vhd”vorhanden. Erweitern Sie

den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher.

- **Fehlerhafte Systemregistrierung.**

  Fehlercode 20. Die Systemregistrierung ist beschädigt, nicht lesbar oder fehlt. Setzen Sie die persönliche vDisk zurück oder stellen Sie sie von einem früheren Backup wieder her.

- **Beim Zurücksetzen von Personal vDisk ist ein interner Fehler aufgetreten. Weitere Informationen finden Sie in den Personal vDisk-Protokollen.**

  Fehlercode 21. Dieser Code gilt für alle Fehler, die beim Zurücksetzen von Personal vDisk auftreten. Sammeln Sie die Protokolle und wenden Sie sich an den Citrix Support.

- **Personal vDisk konnte nicht zurückgesetzt werden, da nicht genügend freier Speicherplatz im persönlichen vDisk-Speicher ist.**

  Fehlercode 22. Es ist nicht genug freier Speicherplatz auf dem Laufwerk der persönlichen vDisk während eines Zurücksetzungsvorgangs vorhanden. Erweitern Sie den Personal vDisk-Speicher oder entfernen Sie nicht verwendete Dateien aus dem Personal vDisk-Speicher.

Fehlermeldungen: vor Version 7.6

Die folgenden Fehler gelten nur für PvD 7.x-Versionen vor Version 7.6:

- **Start fehlgeschlagen. Personal vDisk konnte kein Speichermedium für die Personalisierungseinstellungen der Benutzer finden.**

  Die PvD-Software konnte die Personal vDisk (standardmäßig Laufwerk P:) nicht finden oder nicht als den vom Administrator bei der Erstellung des Katalogs ausgewählten Bereitstellungspunkt bereitstellen.

  - Prüfen Sie, ob Sie im PvD-Dienstprotokoll den folgenden Eintrag finden: "PvD 1 status –> 18:183".
  - Wenn Sie eine ältere Version als PvD Version 5.6.12 verwenden, löst ein Upgrade auf die aktuelle Version das Problem.
  - Wenn Sie Version 5.6.12 oder höher verwenden, prüfen Sie mit dem Datenträgerverwaltungstool (diskmgmt.msc), ob das Laufwerk P: als nicht bereitgestelltes Volume vorhanden ist. Wenn es vorhanden ist, führen Sie chkdsk auf dem Volume aus, um festzustellen, ob es fehlerhaft ist. Versuchen Sie, das Volume mit chkdsk wiederherzustellen.

- **Start fehlgeschlagen. Fehler beim Start von Citrix Personal vDisk. Weitere Informationen …Statuscode: 7, Fehlercode: 0x70**

  Statuscode 7 bedeutet, dass ein Fehler beim Update der PvD aufgetreten ist. Es gibt die folgenden Fehler:

Fehlercode	Beschreibung
0x20000001	Fehler beim Speichern des Vergleichspakets, wahrscheinlich aufgrund von Speicherplatzmangel auf der virtuellen Festplatte.
0x20000004	Unzureichende Privilegien zum Aktualisieren der PvD.
0x20000006	Fehler beim Laden der Struktur aus dem PvD-Image oder dem PvD-Bestand, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands.
0x20000007	Fehler beim Laden des Dateisystembestands, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands.
0x20000009	Fehler beim Öffnen der Datei mit dem Dateisystembestand, wahrscheinlich aufgrund eines fehlerhaften PvD-Images oder PvD-Bestands.
0x2000000B	Fehler beim Speichern des Vergleichspakets, wahrscheinlich aufgrund von Speicherplatzmangel auf der virtuellen Festplatte.
0x20000010	Fehler beim Laden des Vergleichspakets.
0x20000011	Regeldateien fehlen.
0x20000021	Fehlerhafter PvD-Bestand.
0x20000027	Der Katalog “MojoControl.dat”ist fehlerhaft.
0x2000002B	PvD-Bestand fehlerhaft oder fehlt.
0x2000002F	Fehler beim Registrieren des vom Benutzer installierten MOF beim Imageupdate. Lösung: Upgrade auf Version 5.6.12.
0x20000032	Suchen Sie in PvDactivation.log.txt nach dem letzten Eintrag mit einem Win32-Fehlercode.
0x20	Fehler beim Bereitstellen des Anwendungscontainers für Imageupdate. Lösung: Upgrade auf Version 5.6.12.

0x70	Nicht genügend Speicherplatz auf dem Datenträger.

- **Start fehlgeschlagen. Fehler beim Start von Citrix Personal vDisk [oder Personal vDisk hat einen internen Fehler festgestellt]. Weitere Informationen …Statuscode 20, Fehlercode 0x20000028**

  Die persönliche vDisk wurde gefunden, eine PvD-Sitzung konnte jedoch nicht erstellt werden.

  Sammeln Sie die Protokolle und prüfen Sie das Protokoll "SysVol-IvmSupervisor.log"auf Sitzungserstellungsfehler:

  1. Suchen Sie nach dem Protokolleintrag "IvmpNativeSessionCreate: failed to create native session, status XXXXX".
  2. Wenn der Status 0xc00002cf ist, können Sie das Problem lösen, indem Sie eine neue Version des Masterimages zum Katalog hinzufügen. Dieser Statuscode bedeutet, dass ein USN-Journalüberlauf aufgrund zahlreicher Änderungen nach einer Bestandsaktualisierung aufgetreten ist.
  3. Starten Sie den betroffenen virtuellen Desktop neu. Wenn das Problem weiterhin besteht, wenden Sie sich an den technischen Support von Citrix.

- **Start fehlgeschlagen. Citrix Personal vDisk wurde deaktiviert, da das System nicht sicher heruntergefahren wurde. Wählen Sie "Noch einmal versuchen". Wenn das Problem weiterhin besteht, wenden Sie sich an den Systemadministrator.**

  Die gepoolte VM kann den Start nicht ausführen, solange die PvD aktiviert ist. Stellen Sie zuerst fest, warum der Start nicht ausgeführt werden kann. Eine mögliche Ursache ist die Anzeige eines blauen Bildschirms aus einem der folgenden Gründe:

  - Ein nicht kompatibles Antivirenprodukt ist auf dem Masterimage vorhanden, z.B. alte Versionen von Trend Micro.
  - Der Benutzer hat Software installiert, die mit PvD nicht kompatibel ist. Dies ist zwar unwahrscheinlich, aber Sie können es überprüfen, indem Sie dem Katalog eine neue Maschine hinzufügen und testen, ob sie neu startet.
  - Das PvD-Image ist fehlerhaft. Dieser Fehler wurde in Version 5.6.5 beobachtet.

  Prüfen, ob die gepoolte VM einen blauen Bildschirm anzeigt oder ob sie vorzeitig neu startet:

  - Melden Sie sich bei der Maschine über die Hypervisor-Konsole an.
  - Klicken Sie auf Noch einmal versuchen und warten Sie, bis die Maschine heruntergefahren ist.
  - Starten Sie die Maschine über Studio.
  - Beobachten Sie die Maschinenkonsole während des Starts mit der Hypervisor-Konsole.

Weitere Problembehandlungsschritte:

- Senden Sie das Speicherabbild der Maschine, die den blauen Bildschirm hat, zur Analyse an den technischen Support von Citrix.
- Prüfen Sie auch die der PvD zugeordneten Ereignisprotokolle auf Fehler:
  1. Stellen Sie "UserData.V2.vhd"(im Stamm von Laufwerk P:) mit DiskMgmt.msc bereit, indem Sie auf "Aktion"> "Virtuelle Festplatte anfügen"klicken.
  2. Starten Sie "Eventvwr.msc".
  3. Öffnen Sie das Systemereignisprotokoll (Windows\System32\winevt\logs\system.evtx) aus UserData.V2.vhd, indem Sie auf Aktion > Gespeichertes Protokoll öffnen klicken.
  4. Öffnen Sie das Anwendungsereignisprotokoll (Windows\System32\winevt\logs\application.evtx) aus UserData.V2.vhd, indem Sie auf Aktion > Gespeichertes Protokoll öffnen klicken.

- **Die persönliche vDisk kann nicht gestartet werden. Die persönliche vDisk konnte nicht gestartet werden, da der Bestand nicht aktualisiert worden ist. Aktualisieren Sie den Bestand auf dem Masterimage und versuchen Sie es noch einmal. Statuscode: 15, Fehlercode: 0x0**

  Der Administrator hat beim Erstellen oder Aktualisieren des PvD-Katalogs den falschen Snapshot ausgewählt (d. h. das Masterimage wurde beim Erstellen des Snapshots nicht mit Persönliche vDisk aktualisieren heruntergefahren).

Von Personal vDisk protokollierte Ereignisse

Wenn Personal vDisk nicht aktiviert ist, können Sie die folgenden Ereignisse in der Windows-Ereignisanzeige anzeigen. Wählen Sie im linken Bereich den Knoten Anwendungen, die Quelle im rechten Bereich ist Citrix Personal vDisk. Wenn Personal vDisk aktiviert ist, werden diese Ereignisse nicht angezeigt.

Die Ereignis-ID1 bedeutet, dass es sich um eine Informationsmeldung handelt. ID2 steht für einen Fehler. Möglicherweise werden nicht alle Ereignisse in jeder Personal vDisk-Version verwendet.

Ereignis-ID	Beschreibung
1	Status von Personal vDisk: Bestandsaktualisierung gestartet.
1	Status von Personal vDisk: Bestandsaktualisierung abgeschlossen. GUID: %s.
1	Status von Personal vDisk: Imageupdate gestartet.

Ereignis-ID	Beschreibung
1	Status von Personal vDisk: Imageupdate abgeschlossen.
1	Zurücksetzen wird durchgeführt.
1	OK.
2	Status von Personal vDisk: Bestandsaktualisierung fehlgeschlagen mit: %s.
2	Status von Personal vDisk: Imageupdate fehlgeschlagen mit: %s.
2	Status von Personal vDisk: Imageupdate fehlgeschlagen, interner Fehler.
2	Status von Personal vDisk: Bestandsaktualisierung fehlgeschlagen: interner Fehler.
2	Personal vDisk wurde unsachgemäß beendet und daher deaktiviert.
2	Imageupdate fehlgeschlagen. Fehlercode %d.
2	Personal vDisk hat einen internen Fehler festgestellt. Statuscode [%d] Fehlercode [0x%X].
2	Zurücksetzung von Personal vDisk fehlgeschlagen.
2	Datenträger zum Speichern der angepassten Benutzereinstellungen kann nicht gefunden werden.
2	Auf dem Speichermedium ist nicht genügend Speicher vorhanden, um einen Personal vDisk-Container zu erstellen.

Release-unabhängige bekannte Probleme

Die folgenden PvD-Probleme wurden identifiziert:

- Wenn eine Anwendung auf einer persönlichen vDisk (PvD) mit einer auf dem Masterimage installierten anderen Anwendung derselben Version verbunden ist, funktioniert die Anwendung auf der PvD nach einem Imageupdate möglicherweise nicht mehr. Dieses Problem tritt auf, wenn die Anwendung vom Masterimage deinstalliert oder auf eine neuere Version aktualisiert wird, da durch diese Aktion die Dateien entfernt werden, die die Anwendung auf der PvD vom Mas-

terimage benötigt. Um dies zu verhindern, lassen Sie die Anwendung mit den Dateien, die von der Anwendung auf der PvD benötigt werden, auf dem Masterimage.

Beispiel: Das Masterimage enthält Office 2007 und ein Benutzer installiert Visio 2007 auf der PvD. Die Office-Anwendungen und Visio funktionieren einwandfrei. Später ersetzt der Administrator Office 2007 durch Office 2010 auf dem Masterimage und aktualisiert anschließend alle betroffenen Maschinen mit dem aktualisierten Image. Visio 2007 funktioniert nicht mehr. Um dies zu verhindern, lassen Sie Office 2007 auf dem Masterimage. [320915]

- Wenn Personal vDisk verwendet wird, verwenden Sie bei der Bereitstellung von McAfee Virus Scan Enterprise (VSE) die Version 8.8 Patch 4 oder höher auf einem Masterimage. [303472]
- Wenn eine Verknüpfung für eine Datei auf dem Masterimage nicht mehr funktioniert, weil das Verknüpfungsziel in PvD umbenannt wurde, erstellen Sie die Verknüpfung neu. [367602]
- Verwenden Sie keine absoluten bzw. festen Links auf einem Masterimage. [368678]
- Das mit Windows 7 verfügbare Feature "Sichern und Wiederherstellen"wird auf der persönlichen vDisk nicht unterstützt. [360582]
- Nach der Anwendung eines aktualisierten Masterimages ist kein Zugriff auf die Konsole für lokale Benutzer und Gruppen möglich oder sie zeigt inkonsistente Daten an. Um das Problem zu lösen, setzen Sie die Benutzerkonten auf der VM zurück. Dazu muss die Sicherheitsstruktur zurückgesetzt werden. Dieses Problem wurde im Release 7.1.2 behoben und löst auch das Problem für VMs in späteren Releases, aber nicht für VMs, die mit einer früheren Version erstellt und dann aktualisiert wurden. [488044]
- Bei der Verwendung einer gepoolten VM in einer ESX Hypervisor-Umgebung wird Benutzern eine Neustartaufforderung angezeigt, wenn der ausgewählte SCSI-Controllertyp ein "VMware Paravirtual"ist. Verwenden Sie als Workaround einen LSI SCSI-Controller. [394039]
- Nach dem Zurücksetzen von PvD auf einem mit Provisioning Services erstellten Desktop wird Benutzern nach der Anmeldung an der VM u. U. eine Neustartaufforderung angezeigt. Um dieses Problem zu umgehen, starten Sie den Desktop neu. [340186]
- Benutzer von Windows 8.1-Desktops können sich u. U. nicht an ihren PvDs anmelden. Einem Administrator wird möglicherweise die Meldung "PvD was disabled due to unsafe shutdown" angezeigt und das PvDActivation-Protokoll enthält u. U. die Meldung "Failed to load reg hive [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]."Dieses Problem tritt auf, wenn die VM nicht sicher heruntergefahren wird. Setzen Sie als Workaround die persönliche vDisk zurück. [474071]

Entfernen von Komponenten

August 18, 2021

Zum Entfernen von Komponenten empfiehlt Citrix die Verwendung der Windows-Funktion zum Entfernen oder Ändern von Programmen. Alternativ können Sie Komponenten über die Befehlszeile oder mit einem auf dem Installationsmedium enthaltenen Skript entfernen.

Beim Entfernen von Komponenten werden keine Voraussetzungen entfernt und keine Firewalleinstellungen geändert. Wenn Sie einen Controller entfernen, werden die SQL-Serversoftware und die Datenbanken nicht entfernt.

Bevor Sie einen Controller entfernen, müssen Sie ihn aus der Site entfernen. Vor dem Entfernen von Studio oder Director empfiehlt Citrix das Schließen dieser Anwendungen.

Wenn Sie einen Controller von einer früheren Bereitstellung mit dem Web Interface aktualisiert haben, müssen Sie zuerst die Webinterface-Komponente separat entfernen. Das Webinterface kann nicht mit dem Installationsprogramm entfernt werden.

Nach dem Entfernen eines VDAs wird die Maschine in der Standardeinstellung automatisch neu gestartet.

Entfernen von Komponenten mit der Windows-Funktion zum Entfernen oder Ändern von Programmen

Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:

- Zum Entfernen eines Controllers, von Studio, Director, eines Lizenzservers oder von StoreFront wählen Sie Citrix XenApp <*Version*> oder Citrix XenDesktop <*Version*>, klicken Sie mit der rechten Maustaste und wählen Sie **Deinstallieren**. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren. Alternativ können Sie StoreFront entfernen, indem Sie mit der rechten Maustaste auf **Citrix StoreFront** klicken und dann **Deinstallieren** auswählen.
- Klicken Sie zum Entfernen eines VDAs auf**Citrix Virtual Delivery Agent**<*Version*>, klicken Sie mit der rechten Maustaste und wählen Sie **Deinstallieren**. Das Installationsprogramm wird gestartet und Sie können die zu entfernenden Komponenten markieren.
- Zum Entfernen des universellen Druckservers wählen Sie **Citrix Universeller Druckserver**, klicken Sie mit der rechten Maustaste und wählen Sie **Deinstallieren**.

Entfernen von Kernkomponenten über die Befehlszeile

Führen Sie auf dem Installationsmedium im Setupverzeichnis \x64\XenDesktop den Befehl **XenDesktopServerSetup.exe** aus.

- Zum Entfernen einer oder mehrerer Komponenten verwenden Sie die Optionen "/remove"und "/components".
- Zum Entfernen aller Komponenten verwenden Sie die Option "/removeall".

Informationen zu Befehl und Parametern finden Sie unter Installieren über die Befehlszeile.

Mit dem folgenden Befehl wird beispielsweise Studio entfernt:

```
1 \x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
     studio
```

Entfernen eines VDAs über die Befehlszeile

Führen Sie auf dem Installationsmedium im Setupverzeichnis \x64\XenDesktop den Befehl **XenDesktopServerSetup.exe** aus.

- Zum Entfernen einer oder mehrerer Komponenten verwenden Sie die Optionen "/remove"und "/components".
- Zum Entfernen aller Komponenten verwenden Sie die Option "/removeall".

Informationen zu Befehl und Parametern finden Sie unter Installieren über die Befehlszeile.

Mit dem folgenden Befehl werden beispielsweise der VDA und Citrix Receiver entfernt:

```
1 \x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

Informationen zum Entfernen von VDAs mit einem Skript in Active Directory finden Sie unter Installieren oder Entfernen von Virtual Delivery Agents mit Skripts.

Upgrade und Migration

August 18, 2021

Upgrade

Bei Upgrades werden Bereitstellungen auf die neuesten Komponentenversionen aktualisiert, ohne dass neue Maschinen oder Sites erstellt werden müssen. Ein solches Upgrade wird als direktes Upgrade bezeichnet. Ein Upgrade auf die aktuelle Version ist möglich.

- XenDesktop 5.6 *
- XenDesktop 7.0
- XenDesktop 7.1
- XenApp/XenDesktop 7.5
- XenApp/XenDesktop 7.6
- XenApp/XenDesktop 7.6 LTSR
- XenApp/XenDesktop 7.7
- XenApp/XenDesktop 7.8
- XenApp/XenDesktop 7.9
- XenApp/XenDesktop 7.11
- XenApp/XenDesktop 7.12
- XenApp/XenDesktop 7.13
- XenApp/XenDesktop 7.14
- XenApp/XenDesktop 7.15 LTSR

*Für ein Upgrade von XenDesktop 5.6 führen Sie zuerst ein Upgrade auf 7.6 LTSR (mit dem neuesten CU) und dann ein Upgrade auf 7.15 LTSR (mit dem neuesten CU) aus.

Sie können auch einen XenApp 6.5-Workerserver auf einen aktuellen VDA für Windows-Serverbetriebssysteme aktualisieren. Dies ist eine zusätzliche Aktivität bei der Migration von XenApp 6.5. Siehe Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.

Ausführen des Upgrades

1. Führen Sie das Installationsprogramm auf den Maschinen aus, auf denen die Kernkomponenten und VDAs installiert sind. Die Software ermittelt, ob ein Upgrade zur Verfügung steht und installiert die aktuelle Version.
2. Verwenden Sie das aktualisierte Studio zum Aktualisieren der Datenbank und der Site.

Informationen finden Sie unter Upgrade einer Bereitstellung.

Weitere Informationen zur Installation von Hotfixes für Controller finden Sie unter CTX205921.

Migration

Durch Migration werden Daten von einer früheren Bereitstellung auf eine neuere Version verschoben. Sie können eine Migration von XenApp 6.x zu XenApp 7.6 durchführen. Eine Migration umfasst die Installation aktueller Komponenten und das Erstellen einer neuen Site, das Exportieren der Daten aus der älteren Farm und dann das Importieren der Daten in die neue Site.

Informationen zu Änderungen an Architektur, Komponenten und Features in den 7.x-Versionen finden Sie unter Änderungen in Version 7.x.

Weitere Informationen zur Migration finden Sie unter Migrieren von XenApp 6.x.

Änderungen in Version 7.x

August 18, 2021

Mit den 7.x-Releases ändern sich XenApp- und XenDesktop-Architektur, Terminologie und Features. Wenn Sie nur frühere Versionen (vor 7.x) kennen, können Sie sich mit diesem Artikel über die Änderungen informieren.

Änderungen an Versionen ab 7.x werden unter Neue Features behandelt.

In diesem Abschnitt bezieht sich die Angabe *7.x* auf XenApp ab Version 7.5 und auf XenDesktop ab Version 7.

Dieser Abschnitt enthält eine Übersicht. Umfassende Informationen zum Upgrade von Versionen vor 7.x auf die aktuelle Version finden Sie unter Upgrade auf XenApp 7.

Änderungen an den Elementen nach XenApp 6

Die folgende Tabelle erleichtert das Zuordnen der Funktionselemente von XenApp 6.5 und vorherigen Versionen zu XenApp und XenDesktop ab Version 7.x: Die Unterschiede an der Architektur werden weiter unten beschrieben.

XenApp 6.x und früher	Version 7.x
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Farm	Site
Workergruppe	Maschinenkatalog und Bereitstellungsgruppe
Worker	Virtual Delivery Agent (VDA), Serverbetriebssystemmaschine, Serverbetriebssystem-VDA, Desktopbetriebssystemmaschine, Desktopbetriebssystem-VDA
Remotedesktopdienste (RDS) oder Terminaldienste-Maschine	Serverbetriebssystemmaschine, VDA für Serverbetriebssystem
Zonen- und Datensammelpunkt	Delivery Controller
Delivery Services Console	Citrix Studio und Citrix Director
Veröffentlichen von Anwendungen	Bereitstellen von Anwendungen
Datenspeicher	Datenbank
Lastauswertungsprogramm	Lastverwaltungsrichtlinie

XenApp 6.x und früher	Version 7.x
Administrator	Delegierter Administrator, Rolle, Bereich

Änderungen an der Architektur

Ab Version 7.x basieren XenApp und XenDesktop auf der FlexCast Management Architecture (FMA). FMA ist eine dienstorientierte Architektur, die über Citrix Technologien übergreifend Interoperabilität und Verwaltungsmodularität ermöglicht FMA bietet eine Plattform für die Anwendungsbereitstellung, Mobilität, Dienste, flexible Bereitstellung und Cloudverwaltung.

FMA ersetzt die Independent Management Architecture (IMA) in XenApp 6.5 und Vorversionen.

Dies sind die Hauptelemente der FMA gegenüber den Elementen von XenApp 6.5 und Vorversionen:

- **Bereitstellungssites:** Farmen waren die Objekte der obersten Ebene in XenApp 6.5 und Vorversionen. In XenApp 7.x und XenDesktop 7.x ist dies die Site. Über Sites werden Benutzergruppen Anwendungen und Desktops angeboten. Die FMA erfordert, dass Sie in einer Domäne sind, um eine Site bereitzustellen. Beispiel: Zum Installieren der Server muss Ihr Konto lokale Administratorrechte haben und in Active Directory ein Domänenbenutzer sein.
- **Maschinenkataloge und Bereitstellungsgruppen:** Maschinen, auf denen Anwendungen gehostet werden, gehörten in XenApp 6.5 und Vorversionen zu Workergruppen, um eine effiziente Verwaltung von Anwendungen und Serversoftware zu ermöglichen. Administratoren konnten für die Anwendungsverwaltung und für den Lastausgleich alle Maschinen in einer Workergruppe als eine Einheit behandeln. Ordner wurden verwendet, um Anwendungen und Maschinen zu organisieren. In XenApp 7.x und XenDesktop 7.x verwenden Sie eine Kombination aus Maschinenkatalogen, Bereitstellungsgruppen und Anwendungsgruppen, um Maschinen, den Lastausgleich und gehostete Anwendungen oder Desktops zu verwalten. Sie können auch Anwendungsordner verwenden.
- **VDAs:** In XenApp 6.5 und Vorversionen wurden auf Maschinen in Workergruppen Anwendungen für die Benutzer ausgeführt und die Maschinen kommunizierten mit Datensammelpunkten. In XenApp 7.x und XenDesktop 7.x kommuniziert der VDA mit Delivery Controllern, die die Benutzerverbindungen verwalten.
- **Delivery Controller:** In XenApp 6.5 und Vorversionen war ein Zonenmaster für Verbindungsanfragen von Benutzern und die Kommunikation mit Hypervisors zuständig. In XenApp 7.x und XenDesktop 7.x verteilen und handhaben Controller in der Site Verbindungsanfragen. In XenApp 6.5 und Vorversionen ermöglichten Zonen das Aggregieren von Servern und Replizieren von Daten über WAN-Verbindungen. Zonen und Zonenpräferenz in XenApp 7.x und XenDesktop 7.x sind zwar keine exakte Entsprechung, dennoch können Sie mit ihnen Benutzern an entfernten Standorten eine Verbindung mit Ressourcen ermöglichen, ohne dass diese große WAN-

Segmente durchqueren muss.

- **Studio und Director:** Mit der Studio-Konsole können Sie Umgebungen konfigurieren und Benutzern Zugriff auf Anwendungen und Desktops gewähren. Studio ersetzt die Delivery Services Console in XenApp 6.5 und Vorversionen. Administratoren verwenden Director, um die Umgebung zu überwachen, Benutzergeräte zu spiegeln und IT-Probleme zu behandeln. Zum Spiegeln von Benutzern muss die Microsoft-Remoteunterstützung aktiviert sein; sie ist standardmäßig aktiviert, wenn der VDA installiert ist.
- **Bereitstellung von Anwendungen:** In XenApp 6.5 und Vorversionen wurden mit dem Assistenten zur Anwendungsveröffentlichung Anwendungen vorbereitet und für Benutzer bereitgestellt. In XenApp 7.x und XenDesktop 7.x erstellen Sie Anwendungen mit Studio und stellen Sie den Benutzern in einer Bereitstellungsgruppe und, optional, in einer Anwendungsgruppe zur Verfügung. In Studio konfigurieren Sie zunächst eine Site, erstellen und geben Maschinenkataloge an und dann erstellen Sie Bereitstellungsgruppen, die Maschinen aus diesen Maschinenkatalogen verwenden. Mit Bereitstellungsgruppen wird festgelegt, welche Benutzer Zugriff auf die bereitgestellten Anwendungen haben. Sie können alternativ zu mehreren Bereitstellungsgruppen optional Anwendungsgruppen erstellen.
- **Datenbank:** XenApp 7.x und XenDesktop 7.x speichern die Konfigurationsinformationen nicht im IMA-Datenspeicher. Stattdessen werden Konfigurations- und Sitzungsinformationen in einer Microsoft SQL Server-Datenbank gespeichert.
- **Lastverwaltungsrichtlinie:** In XenApp 6.5 und Vorversionen verwenden Lastauswertungsprogramme vordefinierte Messungen zur Bestimmung der Last auf einer Maschine. Benutzerverbindungen konnten weniger ausgelasteten Maschinen zugeordnet werden. In XenApp 7.x und XenDesktop 7.x erfolgt der Lastausgleich auf Maschinen mit Lastverwaltungsrichtlinien.
- **Delegierte Administration:** In XenApp 6.5 und Vorversionen wurden benutzerdefinierte Administratoren erstellt und ihnen wurden Berechtigungen auf der Basis von Ordnern und Objekten zugewiesen. In XenApp 7.x und XenDesktop 7.x basieren benutzerdefinierte Administratoren auf Rollen- und Geltungsbereichspaaren. Eine Rolle repräsentiert eine Stellenfunktion. Ihr sind definierte Berechtigungen zugewiesen, die eine Delegierung erlauben. Ein Geltungsbereich steht für eine Sammlung von Objekten. Vordefinierte Administratorrollen haben spezifische Berechtigungssätze, z. B. für Helpdesk, Anwendungen, Hosting und Kataloge. Beispiel: Helpdeskadministratoren können nur mit einzelnen Benutzern in bestimmten Sites arbeiten, während Volladministratoren die gesamte Bereitstellung überwachen und systemweite IT-Probleme behandeln können.

Featurevergleich

Der Übergang zu FMA bedeutet außerdem, dass einige in XenApp 6.5 und Vorversionen verwendete Features möglicherweise anders implementiert worden sind oder dass Sie sie eventuell durch andere

Features, Komponenten oder Tools ersetzen müssen, um das gleiche Ziel zu erreichen.

XenApp 6.5 und Vorversionen	7.x
Sitzungsvorabstart und Sitzungsfortbestehen	Sitzungsvorabstart und Sitzungsfortbestehen, die durch Bearbeiten der Bereitstellungsgruppeneinstellungen konfiguriert sind. Wie in XenApp 6.5 ermöglichen diese Features Benutzern einen schnellen Zugriff auf Anwendungen, indem Sitzungen gestartet werden, bevor sie angefordert werden (Sitzungsvorabstart), und aktiv bleiben, nachdem ein Benutzer alle Anwendungen geschlossen hat (Sitzungsfortbestehen). In XenApp und XenDesktop 7.x aktivieren Sie die Features für bestimmte Benutzer, indem Sie diese Einstellungen für vorhandene Bereitstellungsgruppen konfigurieren.
Unterstützung für nicht authentifizierte (anonyme) Benutzer erfolgt durch Zuweisen von Rechten für anonyme Benutzer beim Festlegen der Eigenschaften für veröffentlichte Anwendungen	Unterstützung für nicht authentifizierte (anonyme) Benutzer erfolgt durch Konfigurieren dieser Option, wenn Sie die Benutzereigenschaften einer Bereitstellungsgruppe festlegen.
Lokaler Hostcache ermöglicht das Funktionieren eines Workerservers, selbst wenn eine Verbindung zum Datenspeicher nicht verfügbar ist	Der lokale Hostcache ermöglicht die Fortsetzung des Verbindungsbrokerings, wenn die Verbindung zwischen einem Controller und der Sitedatenbank getrennt wird. Diese Implementierung ist robuster und erfordert weniger Wartung. Siehe Lokaler Hostcache.
Anwendungsstreaming	Citrix App-V stellt gestreamte Anwendungen bereit, die mit Studio verwaltet werden. Siehe App-V.
Webinterface	Citrix empfiehlt, dass Sie StoreFront einsetzen.
SmartAuditor zum Aufzeichnen der Bildschirmaktivitäten in der Sitzung eines Benutzers	Ab Version 7.6 Feature Pack 1 wurde diese Funktion durch die Sitzungsaufzeichnung ersetzt. Sie können auch alle Sitzungsaktivitäten aus einer administrativen Perspektive mit der Konfigurationsprotokollierung aufzeichnen.

XenApp 6.5 und Vorversionen	7.x
Energie- und Kapazitätsverwaltung zur Verringerung des Stromverbrauchs und Verwaltung der Serverkapazität	Microsoft Configuration Manager

Unterstützung von und Änderungen an Features

Die folgenden Features werden zurzeit nicht angeboten, nicht mehr unterstützt oder haben sich ab XenApp/XenDesktop 7.x-Versionen erheblich geändert.

SecureICA-Verschlüsselung unter 128 Bit: In Releases vor 7.x war eine Verschlüsselung von Clientverbindungen für Basic-, 40-Bit-, 56-Bit- und 128-Bit-Verschlüsselung durch SecureICA möglich. In Releases aber Version 7 steht die SecureICA-Verschlüsselung nur für die 128-Bit-Verschlüsselung zur Verfügung.

Legacydrucken: Die folgenden Druckfunktionen werden für Releases 7.x nicht unterstützt:

- Abwärtskompatibilität für DOS-Clients und 16-Bit-Drucker.
- Unterstützung für mit Windows 95 und Windows NT verbundene Drucker, einschließlich verbesserter erweiterter Druckereigenschaften und Win32FavorRetainedSetting.
- Möglichkeit zum Aktivieren oder Deaktivieren automatisch gespeicherter und automatisch wiederhergestellter Drucker.
- DefaultPrnFlag, eine Registrierungseinstellung für Server zum Aktivieren/Deaktivieren automatisch gespeicherter und automatisch wiederhergestellter Drucker, die in Benutzerprofilen auf dem Server gespeichert werden.

Ältere Clientdruckernamen werden unterstützt.

Secure Gateway: In Releases vor 7.x wurden mit Secure Gateway sichere Verbindungen zwischen dem Server und den Benutzergeräten hergestellt. Die Sicherung externer Verbindungen erfolgt nun mit NetScaler Gateway.

Spiegeln von Benutzern: In Releases vor 7.x steuerten Administratoren die Benutzer-zu-Benutzer-Spiegelung mit Richtlinien. In 7.x-Releases ist das Spiegeln von Endbenutzern ein integriertes Feature in Director, wobei die Windows-Remoteunterstützung den Administratoren das Spiegeln und Beheben von Problemen auf nahtlos bereitgestellten Anwendungen und virtuellen Desktops gestattet.

Flash v1-Umleitung Bei Clients, die nicht die Flash-Umleitung der zweiten Generation unterstützen erfolgt ein Fallback auf serverseitige Wiedergabe für Legacyfeatures der Flash-Umleitung. VDAs in 7.x-Releases unterstützen die Flash-Umleitungsfeatures der zweiten Generation.

Lokales Textecho: Dieses Feature wurde mit früheren Windows-Anwendungstechnologien zur Beschleunigung der Anzeige eingegebenen Texts auf Benutzergeräten bei Verbindungen mit hoher Latenz eingesetzt. Aufgrund von Verbesserungen am Grafiksubsystem und HDX SuperCodec ist dieses Feature in 7.x-Releases nicht enthalten.

Single Sign-On: Dieses Feature, das Kennwortsicherheit bietet, wird für Windows 8-, Windows Server 2012 und Umgebungen mit neueren unterstützen Windows-Betriebssystemen nicht unterstützt. Es wird noch für Windows 2008 R2- und Windows 7-Umgebungen unterstützt, ist aber nicht in 7.x-Releases enthalten. Es ist auf der Downloadwebsite von Citrix verfügbar: https://citrix.com/downloads.

Oracle-Datenbankunterstützung: 7.x-Releases benötigen eine SQL Server-Datenbank.

Systemüberwachung und -wiederherstellung (HMR): In Releases vor 7.x konnten von HMR Tests auf den Servern einer Serverfarm durchgeführt werden, um deren Zustand zu überwachen und mögliche Integritätsrisiken zu ermitteln. In 7.x-Releases bietet Director eine zentrale Ansicht der Systemintegrität, da die Überwachungs- und Warnfunktionen für die ganze Infrastruktur innerhalb der Director-Konsole dargestellt werden.

Benutzerdefinierte ICA-Dateien: Benutzerdefinierte ICA-Dateien wurden verwendet, um direkte Verbindungen von Benutzergeräten (mit der ICA-Datei) zu einer bestimmten Maschine herzustellen. In 7.x-Releases ist dieses Feature standardmäßig deaktiviert, kann aber für die normale Verwendung mit einer lokalen Gruppe aktiviert werden, oder im Modus für hohe Verfügbarkeit verwendet werden, falls der Controller nicht mehr verfügbar ist.

Management Pack für System Center Operations Manager (SCOM) 2007: Das Management Pack für die Überwachung der Aktivität von XenApp-Farmen mit SCOM unterstützt 7.x-Releases nicht. Siehe aktuelles Citrix SCOM Management Pack für XenApp und XenDesktop.

CNAME-Funktion: Die CNAME-Funktion war in Versionen vor 7.x standardmäßig aktiviert. Bereitstellungen, die von CNAME-Einträgen für FQDN-Umleitung und von der Verwendung von NetBIOS-Namen abhängig sind schlagen möglicherweise fehl. In 7.x-Releases aktualisiert die automatische Delivery Controller-Aktualisierung die Liste der Controller dynamisch und benachrichtigt VDAs, wenn Controller der Site hinzugefügt und aus ihr entfernt werden. Das Feature für automatische Controller-Updates ist in den Citrix Richtlinien standardmäßig aktiviert, kann jedoch deaktiviert werden. Alternativ können Sie die CNAME-Funktion in der Registrierung wieder aktivieren, um mit der vorhandenen Bereitstellung fortzufahren und FQDN-Umleitung und die Verwendung von NetBIOS-Namen zuzulassen. Weitere Informationen finden Sie unter CTX137960.

Assistent für schnelles Bereitstellen: In XenDesktop-Releases vor 7.x konnte mit dieser Studio-Option eine vollständig installierte XenDesktop-Bereitstellung schnell bereitgestellt werden. Durch den neuen vereinfachten Installations- und Konfigurationsworkflow in XenDesktop 7.x ist der Assistent für schnelles Bereitstellen nicht mehr nötig.

Konfigurationsdatei für Remote PC-Dienst und PowerShell-Skript für die automatische Verwaltung: Remote-PC-Zugriff ist jetzt in Studio und den Controller integriert.

Workflow Studio: In Releases vor 7.x war Workflow Studio die grafische Oberfläche für den Aufbau von Workflows für XenDesktop. Das Feature wird in 7.x-Releases nicht unterstützt.

Starten nicht-veröffentlichter Programme bei Clientverbindung: In Releases vor 7.x wurde über diese Citrix-Richtlinieneinstellung angegeben, ob Startanwendungen oder veröffentlichte Anwendungen über ICA oder RDP auf dem Server gestartet werden sollten. In 7.x-Releases wird mit dieser Einstellung nur festgelegt, ob Startanwendungen oder veröffentlichte Anwendungen über RDP auf dem Server gestartet werden.

Desktop starten: In Releases vor 7.x wird mit dieser Citrix-Richtlinieneinstellung angegeben, ob Benutzer, die keine Administratoren sind, eine Verbindung zu einer Desktopsitzung herstellen dürfen. In 7.x-Releases müssen Benutzer ohne Administratorrechte zur Gruppe der Benutzer mit direktem Zugriff für eine VDA-Maschine gehören, um Verbindungen zu Sitzungen auf diesem VDA herzustellen. Die Einstellung Desktop starten ermöglicht Benutzern ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine ICA-Verbindung eine Verbindung zum VDA herzustellen. Die Einstellung Desktop starten hat keine Auswirkungen auf RDP-Verbindungen. Unabhängig von dieser Einstellung können Benutzer, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine RDP-Verbindung eine Verbindung zum VDA herstellen.

Farbtiefe: In Studio-Releases vor 7.6 wurde die Farbtiefe in den Benutzereinstellungen einer Bereitstellungsgruppe angegeben. Ab Version 7.6 kann die Farbtiefe für Bereitstellungsgruppen über das PowerShell-Cmdlet "New-BrokerDesktopGroup"oder "Set-BrokerDesktopGroup"festgelegt werden.

Für Fingereingabe optimierten Desktop starten: Diese Einstellung ist deaktiviert und für Maschinen mit Windows 10 und Windows Server 2016 nicht verfügbar. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Mobilerfahrung".

Nicht in der Citrix Workspace-App enthaltene Features oder Features mit anderen Standardwerten

- **COM-Portzuordnung:** Mit der COM-Portzuordnung wurde der Zugriff auf COM-Ports auf Benutzergeräten zugelassen oder verhindert. Die COM-Portzuordnung wurde zuvor standardmäßig aktiviert. In 7.x-Versionen von XenDesktop und XenApp ist die COM-Portzuordnung standardmäßig deaktiviert. Einzelheiten finden Sie unter Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung.
- **LPT-Portzuordnung:** Mit der LPT-Portzuordnung wird der Zugriff von Legacyanwendungen auf LPT-Ports gesteuert. Die LPT-Portzuordnung wurde zuvor standardmäßig aktiviert. In 7.x-Releases ist die LPT-Portzuordnung standardmäßig deaktiviert.

- **PCM-Audiocodec:** In 7.x-Releases wird der PCM-Audiocodec nur von HTML5-Clients unterstützt.
- **Unterstützung für Microsoft ActiveSync.**
- **Proxyunterstützung für ältere Versionen** einschließlich:
  - Microsoft Internet Security und Acceleration (ISA) 2006 (Windows Server 2003)
  - Oracle iPlanet-Proxyserver 4.0.14 (Windows Server 2003)
  - Squid-Proxyserver 3.1.14 (Ubuntu Linux Server 11.10)

Weitere Informationen finden Sie in der Dokumentation der Citrix Workspace-App.

Upgrade einer Bereitstellung

November 15, 2022

Einführung

Sie können bestimmte Bereitstellungen aktualisieren, ohne zunächst neue Maschinen oder Sites erstellen zu müssen. Dieser Prozess wird als direktes Upgrade bezeichnet. Unter Upgrade finden Sie eine Liste der Versionen, die Sie aktualisieren können.

Sie können mit dem aktuellen XenApp-Installationsprogramm auch einen XenApp 6.5-Workerserver auf einen aktuellen VDA für Windows-Serverbetriebssysteme aktualisieren. Dies ist eine zusätzliche Aktivität bei der Migration von XenApp 6.5. Siehe Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.

Zum Starten eines Upgrades führen Sie das Installationsprogramm in der neuen Version aus, um zuvor installierte Kernkomponenten (Delivery Controller, Citrix Studio, Citrix Director, Citrix Lizenzserver) sowie Virtual Delivery Agents zu aktualisieren. Anschließend führen Sie ein Upgrade der Sitedatenbanken und der Site durch.

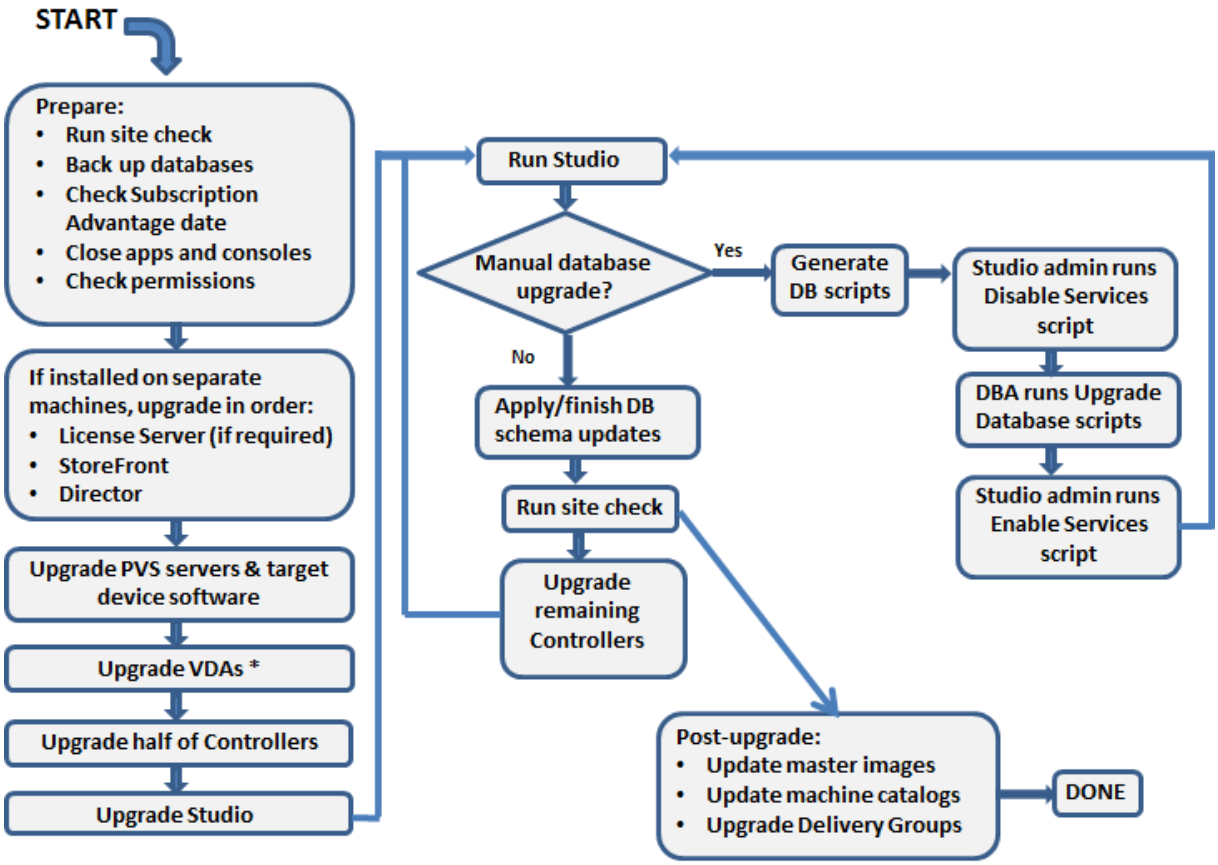
Lesen Sie vor dem Upgrade alle Informationen in diesem Artikel.

(Beim Upgrade auf 7.16 oder höher finden Sie Anleitungen unter Upgrade einer Bereitstellung.)

Aktualisierungsreihenfolge

Die folgende Abbildung zeigt die Upgradereihenfolge. Einzelheiten finden Sie weiter unten unter Upgradeverfahren. Wenn beispielsweise mehrere Kernkomponenten auf einem Server installiert sind, werden durch die Ausführung des Installationsprogramms auf der Maschine alle Komponenten aktualisiert, für die es eine neue Version gibt. Sie sollten ein Upgrade des VDAs in einem Masterimage und

dann ein Update des Images durchführen. Anschließend aktualisieren Sie den Maschinenkatalog, der das Masterimage verwendet und die Bereitstellungsgruppe, die den Katalog verwendet. Zudem wird das automatische und manuelle Upgrade der Sitedatenbanken und der Site behandelt.



* You might upgrade VDAs later when updating a master image

Aktualisierbare Produktkomponenten

Mit dem Produktinstallationsprogramm können Sie folgende Komponenten aktualisieren:

- Citrix License Server, Studio und StoreFront
- Delivery Controller 7.0 und höher.
- VDA 5.6 oder höher
  - Im Gegensatz zu früheren VDA-Releases müssen Sie für das Upgrade der VDAs das Produktinstallationsprogramm verwenden, MSI-Dateien können nicht verwendet werden.
  - Wenn das Installationsprogramm auf der Maschine Receiver für Windows erkennt (Receiver.exe), erfolgt ein Upgrade auf die Receiver-Version auf dem Installationsmedium des Produkts.

  - VDA 5.6 bis 7.8: Wenn das Installationsprogramm Receiver für Windows Enterprise (CitrixReceiverEnterprise.exe) auf der Maschine erkennt, erfolgt ein Upgrade auf Receiver für Windows Enterprise 3.4.

- Director 1 oder höher
- Datenbank: Bei dieser Aktion in Studio erfolgen ein Upgrade des Schemas und eine Migration der Daten der Sitedatenbank (sowie der Konfigurationsprotokollierungsdatenbank und der Überwachungsdatenbank, sofern eine frühere 7.x-Version aktualisiert wird).
- Personal vDisk

Hinweis: Für ein Upgrade von XenDesktop 5.6 führen Sie zuerst ein Upgrade auf 7.6 LTSR (mit dem neuesten CU) und dann ein Upgrade auf dieses Release aus.

Aktualisieren Sie, falls erforderlich, anhand der Informationen in der Feature-/Produktdokumentation die folgenden Elemente:

- Provisioning Services (für XenApp 7.x und XenDesktop 7.x empfiehlt Citrix, dass Sie die aktuelle, freigegebene Version verwenden; die unterstützte Mindestversion ist Provisioning Services 7.0).
  - Aktualisieren Sie den Provisioning Services-Server mit dem parallelen Serverupgrade und die Clients mit der vDisk-Versionsverwaltung. Citrix empfiehlt, Server vor Zielgeräten zu aktualisieren. Weitere Informationen finden Sie unter Aktualisieren von Provisioning-Servern
  - Provisioning Services 7.x unterstützt nicht das Erstellen von neuen Desktops mit Versionen von XenDesktop 5. Obwohl vorhandene Desktops weiterhin funktionieren, können Sie daher mit Provisioning Services 7.x erst dann neue Desktops erstellen, wenn Sie für XenDesktop ein Upgrade durchgeführt haben. Wenn Sie eine heterogene Umgebung mit XenDesktop 5.6 und XenDesktop 7.x-Sites planen, führen Sie daher kein Upgrade von Provisioning Services auf Version 7 durch.
- Host-Hypervisorversion
- StoreFront
- Profilverwaltung
- Verbundauthentifizierungsdienst

Einschränkungen

Die folgenden Einschränkungen gelten für Upgrades:

- **Selektive Installation von Komponenten:** Wenn Sie Komponenten auf die neue Version aktualisieren, andere Komponenten (auf anderen Maschinen) jedoch nicht, wird von Studio eine Erinnerung ausgegeben. Angenommen ein Upgrade enthält neue Versionen für Controller und Studio. Sie aktualisieren den Controller, führen das Installationsprogramm jedoch nicht auf

der Maschine aus, auf der Studio installiert ist. Sie können die Site dann in Studio erst wieder verwalten, wenn Sie ein Upgrade von Studio durchgeführt haben.

Ein Upgrade der VDAs ist nicht erforderlich, Citrix empfiehlt dies jedoch, damit Sie alle verfügbaren Features nutzen können.

- **XenApp-Versionen vor 7.5:** Sie können kein Upgrade einer XenApp-Version vor 7.5 durchführen. Sie können eine Migration von XenApp 6.x durchführen (siehe Migrieren von XenApp 6.x). Sie können zwar kein Upgrade einer XenApp 6.5-Farm durchführen, doch ist es möglich, die XenApp 6.5-Software unter Windows Server 2008 R2 durch einen aktuellen VDA für Serverbetriebssysteme zu ersetzen. Informationen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA.
- **XenDesktop-Versionen vor 5.6:** Sie können kein Upgrade einer XenDesktop-Version vor 5.6 durchführen.
- **XenDesktop Express Edition:** Ein Upgrade der XenDesktop Express Edition nicht möglich. Beschaffen und installieren Sie eine Lizenz für eine derzeit unterstützte Edition und führen Sie anschließend ein Upgrade durch.
- **Early Release- oder Technology Preview-Versionen von XenApp oder XenDesktop:** Sie können kein Upgrade einer Early Release-, Technology Preview- oder Preview-Version durchführen.
- **Windows XP/Vista:** Wenn Sie VDAs unter Windows XP oder Windows Vista installiert haben, lesen Sie den Abschnitt VDAs auf Maschinen mit Windows XP oder Windows Vista.
- **Produktauswahl:** Beim Upgrade einer älteren 7.x-Version legen Sie nicht das Produkt (XenApp oder XenDesktop) fest, das bei der ersten Installation festgelegt wurde.
- **Heterogene Umgebungen:** Wenn Sie Sites einer früheren Version neben Sites der aktuellen Version beibehalten müssen, lesen Sie die Hinweise zu heterogenen Umgebungen.

Vorbereitung

Führen Sie vor Beginn des Upgrades folgenden Schritte aus:

- **Auswahl von Installationsprogramm und Schnittstelle:** Verwenden Sie das Produktinstallationsprogramm auf dem XenApp- oder XenDesktop-ISO-Image zum Aktualisieren der Kernkomponenten. VDAs können Sie mit dem Komplettinstallationsprogramm oder einem der eigenständigen VDA-Installationsprogramme aktualisieren. Alle Installationsprogramme bieten eine grafische Oberfläche und eine Befehlszeilenschnittstelle. Weitere Informationen finden Sie unter Installationsprogramme.

  Ein Upgrade durch Importieren oder Migrieren von Daten aus einer aktualisierbaren Version ist nicht möglich. Hinweis: Einige viel ältere Versionen müssen anstelle eines Upgrades migriert werden (Informationen zu aktualisierbaren Versionen siehe Upgrade und Migration).

Wenn Sie einen Desktop-VDA ursprünglich mit dem Installationsprogramm VDAWorkstationCoreSetup.exe installiert haben, empfiehlt Citrix die Verwendung dieses Installationsprogramms zum Durchführen des Upgrades. Wenn Sie das Komplettinstallationsprogramm oder das Installationsprogramm VDAWorkstationSetup.exe für das Upgrade des VDAs verwenden, werden ursprünglich ausgeschlossene Komponenten möglicherweise installiert, es sei denn, Sie schließen sie mit "omit/exclude"ausdrücklich vom Upgrade aus.

Beispiel: Wenn Sie einen VDA der Version 7.13 mit VDAWorkstationCoreSetup.exe installiert haben und dann ein Upgrade mit dem vollständigen Produktinstallationsprogramm auf Version 7.14 durchführen, werden Komponenten, die ursprünglich von der Installation ausgeschlossen waren (z. B. Profilverwaltung oder persönliche vDisk) ggf. installiert, wenn Sie die Standardeinstellungen übernehmen oder die Befehlszeilenoption "/exclude"nicht verwenden.

- **Überprüfen der Siteintegrität:** Stellen Sie vor dem Upgrade sicher, dass die Site stabil und funktionsfähig ist. Bestehen bei einer Site Probleme, werden diese durch ein Upgrade nicht behoben. Stattdessen kann das Upgrade zusätzliche Probleme verursachen, die sich nur schwer beheben lassen. Zum Testen der Site wählen Sie im Studio-Navigationsbereich **Site**. Klicken Sie im mittleren Bereich unter "Sitekonfiguration"auf **Site testen**.
- **Sichern der Site-, Überwachungs- und Konfigurationsprotokollierungsdatenbank:** Folgen Sie den Anweisungen unter CTX135207. Wenn nach dem Upgrade Probleme entdeckt werden, können Sie das Backup wiederherstellen.

  Optional können Sie Vorlagen sichern und evtl. Hypervisors aktualisieren.

  Erledigen Sie sämtliche anderen, zur Gewährleistung der Betriebskontinuität erforderlichen Vorbereitungsaufgaben.
- **Überprüfen der Citrix Lizenzen:** Stellen Sie vor dem Upgrade sicher, dass Ihr Customer Success Services/Software Maintenance/Subscription Advantage-Datum für die neue Produktversion gültig ist. Wenn Sie ein Upgrade einer früheren 7.x-Produktversion durchführen, muss das Datum mindestens 2017.0801 lauten. (Dieses Datum gilt für die Version 7.15 LTSR, nicht für die kumulativen Updates (CUs).)
- **Stellen Sie sicher, dass Ihr Citrix Lizenzserver kompatibel ist:** Stellen Sie sicher, dass Ihr Citrix Lizenzserver mit der neuen Version kompatibel ist. Dies kann mit zwei Möglichkeiten erreicht werden:

  - Führen Sie vor dem Upgrade anderer Citrix-Komponenten das Installationsprogramm auf der Maschine aus, auf der der Lizenzserver ist. Wenn ein Upgrade erforderlich ist, initiiert das Installationsprogramm es.
  - Führen Sie auf dem Installationsmedium im XenDesktop-Setupverzeichnis folgenden Befehl aus: `.\LicServVerify.exe -h \<License-Server-fqdn> -p 27000 –v`. Der resultierende Bildschirm zeigt, ob der Lizenzserver kompatibel ist. Wenn der Lizen-

zserver nicht kompatibel ist, führen Sie das Installationsprogramm auf dieser Maschine aus, um ihn zu aktualisieren.

- **Backup jeglicher StoreFront-Änderungen:** Wenn Sie Änderungen an Dateien in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` gemacht haben, z. B. *default.ica* und *usernamepassword.tfrm*, legen Sie für jeden Store ein Backup an. Nach dem Upgrade können Sie sie wiederherstellen, um Ihre Änderungen wieder anzuwenden.
- **Anwendungen und Konsolen schließen:** Bevor Sie ein Upgrade durchführen, schließen Sie alle Programme, die Dateisperren verursachen können, einschließlich Verwaltungskonsolen und PowerShell-Sitzungen. (Das Neustarten der Maschine stellt sicher, dass alle Dateisperren aufgehoben werden und keine Windows-Updates ausstehen.)

  Vor Durchführung eines Upgrades beenden Sie Überwachungsdienste von Drittanbietern und deaktivieren Sie sie.
- **Sicherstellen, dass die erforderlichen Berechtigungen vorliegen:** Auf den Maschinen, auf denen Sie die Produktkomponenten aktualisieren, müssen Sie sowohl Domänenbenutzer als auch lokaler Administrator sein.

Sitedatenbank und Site können automatisch oder manuell aktualisiert werden. Für ein automatisches Datenbankupgrade müssen die Berechtigungen des Studio-Benutzers die Berechtigung zum Aktualisieren des SQL Server-Datenbankschemas umfassen (z. B. Datenbankrolle "db_securityadmin" oder "db_owner"). Weitere Informationen finden Sie unter Datenbanken. Hat der Studio-Benutzer diese Berechtigungen nicht, werden bei einem manuellen Datenbankupgrade Skripts generiert. Der Studio-Benutzer führt einige dieser Skripts über Studio aus, andere werden vom Datenbankadministrator mit einem Tool wie SQL Server Management Studio ausgeführt.

Hinweise zu heterogenen Umgebungen

Wenn Ihre Umgebung Sites/Farmen mit mehreren Produktversionen enthält (heterogene Umgebung), empfiehlt Citrix die Verwendung von StoreFront zum Aggregieren von Anwendungen und Desktops aus den unterschiedlichen Produktversionen (Beispiel: Sie haben eine XenDesktop 7.13-Site und eine XenDesktop 7.14-Site). Weitere Informationen finden Sie in der Dokumentation zu StoreFront.

- Verwenden Sie in einer heterogenen Umgebung weiterhin Studio und Director für das jeweilige Release. Die verschiedenen Versionen müssen jedoch auf separaten Maschinen installiert sein.
- Wenn Sie XenDesktop 5.6 und XenDesktop 7.x-Sites parallel ausführen und für beide Provisioning Services verwenden möchten, stellen Sie entweder eine neue Version von Provisioning Services für die Verwendung mit der 7.x-Site bereit oder aktualisieren Sie die aktuelle Version von Provisioning Services. In diesem Fall können Sie jedoch keine neuen Arbeitslasten in der XenDesktop 5.6-Site mehr bereitstellen.

Citrix empfiehlt, in einer Site jeweils alle Komponenten zu aktualisieren. Sie können zwar von einigen Komponenten die früheren Versionen verwenden, jedoch sind u. U: nicht alle Features einer aktuellen Version verfügbar. Beispiel: Sie können zwar aktuelle VDAs in Bereitstellungen mit älteren Controllerversionen verwenden, jedoch sind die neuen Features des aktuellen Releases möglicherweise nicht verfügbar. Bei der Registrierung des VDAs können beim Verwenden nicht aktueller Versionen ebenfalls Probleme auftreten.

- Sites mit Controllern der Version 5.x und VDAs der Version 7.x sollten in diesem Zustand nur vorübergehend verbleiben. Im Idealfall sollten Sie das Upgrade aller Komponenten so schnell wie möglich durchführen.
- Führen Sie ein Upgrade einer eigenständigen Studio-Version erst dann durch, wenn Sie zur Verwendung der neuen Version bereit sind.

VDAs auf Maschinen mit Windows XP oder Windows Vista

Sie können kein Upgrade von VDAs auf Maschinen mit Windows XP oder Windows Vista auf eine 7.x-Version durchführen. Sie müssen VDA 5.6 FP1 mit bestimmten Hotfixes verwenden. Anweisungen hierfür finden Sie unter CTX140941. Obwohl ältere VDAs in einer 7.x-Site funktionieren, können zahlreiche Features nicht verwendet werden. Beispiele:

- Features in Studio, die eine neuere VDA-Version erfordern
- Konfiguration von App-V-Anwendungen über Studio
- Konfiguration von StoreFront-Adressen über Studio
- Automatische Unterstützung der Microsoft Windows-KMS-Lizenzierung bei Verwendung von Maschinenerstellungsdiensten Weitere Informationen finden Sie unter CTX128580.
- Informationen in Director:
  - Anmeldezeiten und Anmeldeende-Ereignisse, die sich auf die Anmeldungsdauer auswirken, in den Ansichten “Dashboard”, “Trends”und “Benutzerdetails”
  - Eine Aufschlüsselung der Anmeldedauer für HDX-Verbindungs- und Authentifizierungszeiten sowie Zeitdauerangaben für Profil- und GPO-Ladevorgänge, Anmeldeskript und die Herstellung interaktiver Sitzungen
  - Einige Kategorien der Fehlerraten für Maschinen und Verbindungen
  - Aktivitätsmanager in der Ansicht “Helpdesk”und “Benutzerdetails”

Citrix empfiehlt ein Reimaging der Windows XP- und Windows Vista-Maschinen unter einer unterstützten Betriebssystemversion und die anschließende Installation der aktuellen VDA-Version.

VDAs auf Maschinen mit Windows 8.x oder Windows 7

Für ein Upgrade von VDAs auf Maschinen mit Windows 8.x oder Windows 7 auf Windows 10 empfiehlt Citrix ein Reimaging der Windows 7- und Windows 8.x-Maschinen auf Window 10. Anschließend instal-

lieren Sie den unterstützten VDA für Windows 10. Ist ein Reimaging nicht möglich, deinstallieren Sie den VDA vor dem Upgrade des Betriebssystems, da er ansonsten einen nicht unterstützten Zustand annimmt.

Unterstützung gemischter VDAs

Für ein Upgrade des Produkts auf eine neuere Version empfiehlt Citrix, dass Sie alle Kernkomponenten und VDAs aktualisieren, damit Sie alle neuen und verbesserten Features der Edition verwenden können.

In einigen Umgebungen ist ein Upgrade aller VDAs auf die aktuelle Version möglicherweise nicht möglich. In diesem Fall können Sie beim Erstellen eines Maschinenkatalogs die auf den Maschinen installierte VDA-Version angeben. Standardmäßig ist für diese Einstellung die neueste empfohlene VDA-Version festgelegt. Sie müssen eine Änderung dieser Einstellung nur dann in Betracht ziehen, wenn der Maschinenkatalog Maschinen mit früheren VDA-Versionen enthält. Die Verwendung mehrerer VDA-Versionen in einem Maschinenkatalog wird nicht empfohlen.

Wenn ein Maschinenkatalog mit der standardmäßig empfohlenen VDA-Versionseinstellung erstellt wird und auf Maschinen in dem Katalog eine frühere VDA-Version installiert ist, können sich diese Maschinen nicht beim Controller registrieren und funktionieren nicht.

Weitere Informationen finden Sie unter VDA-Versionen und Funktionsebenen.

Controller unter früheren Betriebssystemen

Citrix empfiehlt, dass alle Delivery Controller einer Site unter dem gleichen Betriebssystem ausgeführt werden. Durch die folgende Upgradereihenfolge wird der Zeitraum, während dessen verschiedene Controller unter unterschiedlichen Betriebssystemen ausgeführt werden, möglichst kurz gehalten.

1. Erstellen Sie einen Snapshot aller Delivery Controller in der Site und sichern Sie die Sitedatenbank.
2. Installieren Sie neue Delivery Controller auf sauberen Servern mit einem unterstützten Betriebssystem.
3. Fügen Sie der Site die neuen Controller hinzu.
4. Entfernen Sie die Controller, die unter für die neue Version nicht mehr gültigen Betriebssystemen ausgeführt werden.

Informationen zum Hinzufügen und Entfernen von Controllern finden Sie unter Delivery Controller.

Upgradeverfahren

Zum Ausführen der grafischen Oberfläche des Installationsprogramms melden Sie sich bei der Maschine an und legen Sie anschließend das Installationsmedium ein oder stellen Sie das ISO-Laufwerk für das neue Release bereit. Doppelklicken Sie auf **AutoSelect**. Anweisungen zur Verwendung der Befehlszeilenschnittstelle finden Sie unter Installieren über die Befehlszeile.

1. Wenn mehrere Kernkomponenten (z. B. Controller, Studio und Lizenzserver) auf dem gleichen Server installiert sind und für mehrere dieser Komponenten eine neue Version verfügbar ist, werden alle beim Ausführen des Installationsprogramms auf dem Server aktualisiert.

   Wenn Kernkomponenten auf anderen Maschinen als dem Controller installiert sind, führen Sie das Installationsprogramm auf diesen Maschinen aus. Empfohlene Reihenfolge: Lizenzserver, StoreFront, Director.

   Wenn Sie noch nicht geprüft haben, ob Ihr Lizenzserver mit der neuen Version kompatibel ist (siehe Vorbereitung), sollten Sie das Installationsprogramm auf der Lizenzserver ausführen, bevor Sie andere Kernkomponenten aktualisieren.

   Wenn Sie manuelle Änderungen an StoreFront-Stores beibehalten möchten, machen Sie ein Backup der Storedateien vor dem Upgrade von StoreFront (siehe Vorbereitung).

2. Wenn Sie Provisioning Services verwenden, aktualisieren Sie die PVS-Server und -Zielgeräte. Anweisungen hierzu finden Sie in der Dokumentation zu Provisioning Services.

3. Führen Sie das Produktinstallationsprogramm auf Maschinen mit VDAs aus. (Bei Verwendung von Masterimages und Maschinenerstellungsdienste s. Schritt 12.)

4. Führen Sie das Produktinstallationsprogramm auf der Hälfte der Controller aus. (Damit werden auch alle anderen Kernkomponenten auf diesen Servern aktualisiert.) Wenn Ihre Site beispielsweise vier Controller enthält, führen Sie das Installationsprogramm auf zwei Controllern aus.

   - Dadurch dass die Hälfte der Controller aktiv bleibt, können Benutzer auf die Site zugreifen. Die VDAs können sich bei den anderen Controllern registrieren. Zeitweise wird die Site möglicherweise mit reduzierter Kapazität ausgeführt, da weniger Controller verfügbar sind. Durch das Upgrade wird nur für das Einrichten neuer Clientverbindungen während der letzten Datenbankaktualisierungsschritte eine kurze Unterbrechung verursacht. Die aktualisierten Controller können Anforderungen erst verarbeiten, wenn die gesamte Site aktualisiert wurde.
   - Wenn die Site nur einen Controller hat, ist sie während des Upgrades nicht funktionsfähig.

5. Ist Studio auf einer Maschine installiert, die Sie noch nicht aktualisiert haben, führen Sie das Installationsprogramm auf der Maschine aus, auf der Studio installiert ist.

6. Führen Sie über die neu aktualisierte Studio-Version ein Upgrade der Sitedatenbank aus. Einzelheiten finden Sie unter Upgrade der Sitedatenbanken und der Site.

7. Wählen Sie in der neu aktualisierten Studio-Version im Navigationsbereich **Citrix Studio** *Sitename* aus. Wählen Sie die Registerkarte **Häufige Aufgaben**. Wählen Sie **Upgrade der übrigen Delivery Controller durchführen**.
8. Nachdem Sie das Upgrade auf den übrigen Controllern abgeschlossen und bestätigt haben, schließen Sie Studio und öffnen es neu. Sie werden von Studio ggf. zu einem zusätzlichen Site-Upgrade aufgefordert, um die Controllerservices bei der Site zu registrieren oder eine Zonen-ID zu erstellen, falls noch keine vorhanden ist.
9. Wählen Sie auf der Seite "Häufige Aufgaben"im Abschnitt "Sitekonfiguration"die Option **Registrierung durchführen**. Durch das Registrieren der Controller werden diese für die Site verfügbar.
10. Nach Auswahl von **Fertig stellen** im Anschluss an das Upgrade können Sie sich optional für die Teilnahme am Citrix Telemetrieprogramm registrieren, durch das Informationen zu Ihrer Bereitstellung gesammelt werden. Diese Informationen werden Verbesserung von Qualität, Zuverlässigkeit und Leistung des Produkts verwendet.
11. Nach dem Upgrade von Komponenten, Datenbank und Site testen Sie die neu aktualisierte Site. Wählen Sie in Studio im Navigationsbereich **Citrix Studio** *Sitename*. Wählen Sie die Registerkarte **Häufige Aufgaben** und dann **Site testen**. Diese Tests werden automatisch nach dem Upgrade der Datenbank ausgeführt, Sie können sie jedoch jederzeit wiederholen.

    Der Test der Site kann auf Controllern unter Windows Server 2016 fehlschlagen, wenn eine lokale SQL Server Express-Instanz für die Sitedatenbank verwendet wird und der SQL Server Browser-Dienst nicht gestartet wurde. Führen Sie zur Vermeidung dieses Fehlers die folgenden Schritte aus.

    a) Aktivieren Sie den SQL Server Browser-Dienst (falls erforderlich) und starten Sie ihn.

    b) Starten Sie den SQL Server-Dienst (SQLEXPRESS) neu.
12. Wenn Sie Maschinenerstellungsdienste einsetzen und den aktualisierten VDA verwenden möchten, führen Sie nach dem Upgrade und Testen der Bereitstellung ein Upgrade der Masterimages durch (falls noch nicht erfolgt). Aktualisieren Sie die Masterimages, die diese VDAs verwenden. Siehe Aktualisieren oder Erstellen eines Masterimages. Führen Sie anschließend ein Upgrade der Maschinenkataloge durch, die die Masterimages verwenden und der Bereitstellungsgruppen, die die Kataloge verwenden.

Upgrade der Sitedatenbanken und der Site

Nach dem Upgrade der Kernkomponenten und VDAs verwenden Sie die neu aktualisierte Studio-Version für ein automatisches oder manuelles Upgrade von Datenbank und Site.

Nicht vergessen: Lesen Sie die Informationen zu Berechtigungen unter Vorbereitung weiter oben.

- Für ein automatisches Datenbankupgrade müssen die Berechtigungen des Studio-Benutzers die Berechtigung zum Aktualisieren des SQL Server-Datenbankschemas umfassen.
- Beim manuellen Upgrade führt der Studio-Benutzer einige der erstellten Skripts über Studio aus. Der Datenbankadministrator führt andere Skripts mit dem SQLCMD-Hilfsprogramm oder mit SQL Server Management Studio im SQLCMD-Modus aus. Andernfalls kann es zu Fehlern kommen.

Citrix empfiehlt dringend, vor dem Upgrade ein Backup der Datenbank anzulegen. Siehe CTX135207. Während des Datenbankupgrades sind die Produktdienste deaktiviert. Während dieser Zeit können Controller keine neuen Verbindungen für die Site verhandeln. Planen Sie daher sorgfältig.

Nach dem Upgrade der Datenbank und der Aktivierung der Produktdienste testet Studio Umgebung und Konfiguration und generiert einen HTML-Bericht. Wenn Probleme identifiziert werden, können Sie die Datenbank aus dem Backup wiederherstellen. Wenn die Probleme beseitigt sind, können Sie die Datenbank erneut aktualisieren.

Automatisches Upgrade von Datenbank und Site:

Starten Sie die aktualisierte Studio-Version. Sobald Sie das automatische Upgrade der Site gestartet und bestätigt haben, dass Sie bereit sind, beginnt das Upgrade von Datenbank und Site.

Manuelles Aktualisieren von Datenbank und Site:

1. Starten Sie die aktualisierte Studio-Version. Wählen die Option für ein manuelles Upgrade der Site. Der Assistent prüft die Kompatibilität des Lizenzservers und fordert eine Bestätigung an. Wenn Sie bestätigt haben, dass Sie die Datenbank gesichert haben, erstellt der Assistent Skripts und eine Checkliste der Upgradeschritte und zeigt diese an.
2. Führen Sie die folgenden Skripts in der angegebenen Reihenfolge aus:

    - **DisableServices.ps1:** PowerShell-Skript, das vom Studio-Benutzer auf einem Controller ausgeführt werden muss und die Produktdienste deaktiviert
    - **UpgradeSiteDatabase.sql:** SQL-Skript, das vom Datenbankadministrator auf dem Server mit der Sitedatenbank ausgeführt werden muss
    - **UpgradeMonitorDatabase.sql:** SQL-Skript, das vom Datenbankadministrator auf dem Server mit der Überwachungsdatenbank ausgeführt werden muss
    - **UpgradeLoggingDatabase.sql:** SQL-Skript, das vom Datenbankadministrator auf dem Server mit der Konfigurationsprotokollierungsdatenbank ausgeführt werden muss Führen Sie dieses Skript nur aus, wenn diese Datenbank geändert wird (z. B. nach dem Anwenden eines Hotfixes).
    - **EnableServices.ps1:** PowerShell-Skript, das vom Studio-Benutzer auf einem Controller ausgeführt werden muss und die Produktdienste aktiviert

3. Nach Abschluss der Checklistenaufgaben klicken Sie auf **Upgrade fertig stellen**.

Upgrade von Datenbankschemas

Wenn Sie ein Upgrade auf ein neues CU durchführen, werden einige Datenbankschemas aktualisiert. Die aktualisierten Datenbankschemas sind in der nachfolgenden Tabelle aufgeführt:

7.15 DBschema upgrade	7.15 CU1	7.15 CU2	7.15 CU3	7.15 CU4	7.15 CU5	7.15 CU6	7.15 CU7	7.15 CU8
7.15 RTM	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU1		Config	Site; Config	Site; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU2			Site; Config	Site; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU3				Site; Config	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU4					Monitor, Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging	Site; Monitor; Config; Logging
7.15 CU5						Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
7.15 CU6							Site; Monitor; Config	Site; Monitor; Config
7.15 CU7								Site; Config

Begriffsdefinitionen:

- Site = Sitedatenspeicher; das Datenbankschema wird im Sitedatenspeicher aktualisiert.
- Monitor = Überwachungsdatenspeicher; das Datenbankschema wird im Überwachungsdatenspeicher aktualisiert
- Config = Konfigurationstabelle; die Desktop Studio-Version, die Lizenzserverversion oder beide werden in der Konfigurationstabelle aktualisiert.
- Logging = Protokollierungsdatenspeicher, Dbschema-Aktualisierung erfolgt auf Protokollierungsdatenspeicher.

Upgrade eines XenApp 6.5-Workers auf einen neuen VDA

November 15, 2022

Nachdem Sie eine XenApp 6.5-Farm migriert haben, können Sie XenApp 6.5-Server, die im ausschließlichen Sitzungshostmodus konfiguriert waren, verwenden, indem Sie die ältere Software entfernen und dann einen neuen VDA für Serverbetriebssysteme installieren.

Hinweis: Sie können zwar einen XenApp 6.5-Workerserver aktualisieren, die Installation des aktuellen VDAs auf einer “sauberen”Maschine bietet jedoch mehr Sicherheit.

Upgrade eines XenApp 6.5-Workers auf einen neuen VDA

1. Entfernen Sie Hotfix Rollup Pack 7 für XenApp 6.5 gemäß den Anweisungen in der Hotfix-Readmedatei. Siehe CTX202095.
2. Deinstallieren Sie XenApp 6.5 gemäß den Anweisungen unter Entfernen von Rollen und Komponenten. Dieser Prozess erfordert mehrere Neustarts. Wenn während der Deinstallation ein Fehler auftritt, prüfen Sie das in der Fehlermeldung angegebene Deinstallationsfehlerprotokoll.

Diese Protokolldatei ist im Ordner "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\".

3. Installieren Sie einen VDA für Serverbetriebssysteme unter Einsatz des in diesem Release bereitgestellten Installationsprogramms. Weitere Informationen finden Sie unter Installieren von VDAs und Installieren über die Befehlszeile.

Erstellen Sie nach der VDA-Installation mit Studio in der neuen XenApp-Site Maschinenkataloge (oder bearbeiten Sie vorhandene Kataloge) für die aktualisierten Worker.

Problembehandlung

Symptome: Fehler beim Entfernen der XenApp 6.5-Software. Das Deinstallationsprotokoll enthält die Meldung:"Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Skript directory. Please make sure that your IIS installation is correct."

Ursache: Das Problem tritt auf Systemen auf, wenn (1) Sie während der XenApp 6.5-Erstinstallation angegeben haben, dass der Citrix XML-Dienst (CtxHttp.exe) keinen Port gemeinsam mit IIS verwenden soll, und (2) .NETFramework 3.5.1 installiert ist.

Lösung:

1. Entfernen Sie die Webserver (IIS)-Rolle mit dem Windows-Assistenten zum Entfernen von Rollen. (Sie können die Webserver (IIS)-Rolle später wieder installieren.)
2. Starten Sie den Server neu.
3. Deinstallieren Sie mit "Programme hinzufügen/entfernen"Citrix XenApp 6.5 und Microsoft Visual C++ 2005 Redistributable (x64), Version 8.0.56336.
4. Starten Sie den Server neu.
5. Installieren Sie den VDA für Windows-Serverbetriebssysteme.

Migrieren von XenApp 6.x

January 21, 2022

Hinweis: Sie können Citrix Smart Migrate nicht mit dieser Version von XenApp und XenDesktop verwenden. Das Migrationstool ist jedoch verfügbar.

Mit dem hier beschriebenen Migrationstool können Sie eine Migration von XenApp 6.x auf XenApp 7.6 durchführen. Anschließend können Sie ein Upgrade von XenApp 7.6 auf ein unterstütztes LTSR oder die aktuelle Citrix Virtual Apps and Desktops-Version durchführen.

XenApp 6.x-Migrationstool

Das XenApp 6.x-Migrationstool ist eine Sammlung von PowerShell-Skripts und Cmdlets, die Richtliniendaten und Farmdaten für XenApp 6.x (6.0 und 6.5) migrieren. Dazu führen Sie auf dem XenApp 6.x-Controllerserver Export-Cmdlets aus, die die Daten in XML-Dateien zusammenfassen. Anschließend führen Sie vom XenApp 7.6-Controller aus die Import-Cmdlets aus, die mit den beim Export gesammelten Daten Objekte erstellen.

Unten ist die Abfolge des Migrationsvorgangs zusammengefasst. Einzelheiten werden später aufgeführt.

1. Auf einem XenApp 6.0- oder 6.5-Controller:
    a) Importieren Sie die PowerShell-Exportmodule.
    b) Exportieren Sie mit den Export-Cmdlets die Richtlinien- und Farmdaten in XML-Dateien.
    c) Kopieren Sie die XML-Dateien (und den Ordner mit den Symbolen, wenn sie für den Export nicht in die XML-Dateien eingebettet werden) auf den XenApp 7.6-Controller.
2. Auf dem XenApp 7.6-Controller:
    a) Importieren Sie die PowerShell-Importmodule.
    b) Importieren Sie mit den Import-Cmdlets die Richtlinien- und Farmdaten (Anwendungen), wobei Sie die XML-Dateien als Eingabe verwenden.
3. Führen Sie die nach der Migration erforderlichen Schritte aus.

Vor der eigentlichen Migration können Sie die XenApp 6.x-Einstellungen exportieren und eine Exportvorschau in der XenApp 7.6-Site ausführen. Die Vorschau lässt mögliche Schwachstellen erkennen, damit Sie die Probleme vor der eigentlichen Migration beheben können. Bei einer Vorschau kann sich beispielsweise herausstellen, dass eine Anwendung mit dem gleichen Namen bereits in der neuen XenApp 7.6-Site vorhanden ist. Sie können die bei der Vorschau erstellten Protokolldateien bei der Migration als Leitfaden verwenden.

Sofern nicht anders angegeben, bezieht sich “6.x”auf XenApp 6.0 oder 6.5.

Neue Features in diesem Release

Dieses Dezember 2014-Release (Version 20141125) enthält die folgenden Updates:

- Wenn mit den Migrationstools in einer XenApp 6.x-Farm Probleme auftreten, melden Sie dies an https://discussions.citrix.com/forum/1411-xenapp-7x/.
- Neues Paketformat: Die Datei `XAMigration.zip` enthält jetzt zwei separate Pakete: `ReadIMA.zip` und `ImportFMA.zip`. Zum Exportieren von einem XenApp 6.x-Server benötigen Sie nur `ReadIMA.zip`. Zum Importieren auf einen XenApp 7.6.x-Server benötigen Sie nur `ImportFMA.zip`.

- Das Cmdlet `Export-XAFarm` unterstützt einen neuen Parameter (`EmbedIconData`), durch den das Kopieren der Symboldaten in verschiedene Dateien nicht mehr nötig ist.
- Das Cmdlet `Import-XAFarm` unterstützt drei neue Parameter:
  - `MatchServer` - Zum Importieren von Anwendungen von Servern, deren Namen mit einem Ausdruck übereinstimmen
  - `NotMatchServer` - Zum Importieren von Anwendungen von Servern, deren Namen nicht mit einem Ausdruck übereinstimmen
  - `IncludeDisabledApps` - Zum Importieren von deaktivierten Anwendungen
- Vorab gestartete Anwendungen werden nicht importiert.
- Das Cmdlet `Export-Policy` ist für XenDesktop 7.x.

Migrationstoolpaket

Das Migrationstool ist auf der Citrix Downloadsite für XenApp 7.6 verfügbar. Die Datei XAMigration.zip enthält zwei separate, unabhängige Pakete:

- `ReadIMA.zip` - Enthält die Dateien zum Exportieren von Daten aus der XenApp 6.x-Farm sowie freigegebene Module.

Modul bzw. Datei	Beschreibung
ExportPolicy.psm1	PowerShell-Skriptmodul zum Exportieren von XenApp 6.x-Richtlinien in eine XML-Datei.
ExportXAFarm.psm1	PowerShell-Skriptmodul zum Exportieren von XenApp 6.x-Farmeinstellungen in eine XML-Datei.
ExportPolicy.psd1	PowerShell-Manifestdatei für Skriptmodul ExportPolicy.psm1
ExportXAFarm.psd1	PowerShell-Manifestdatei für Skriptmodul ExportXAFarm.psm1
LogUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit Protokollierungsfunktionen
XmlUtilities.psd1	PowerShell-Manifestdatei für das Skriptmodul XmlUtilities.psm1.
XmlUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit XML-Funktionen

- `ImportFMA.zip` - Enthält die Dateien zum Importieren von Daten aus der XenApp 7.6-Farm sowie freigegebene Module.

Modul bzw. Datei	Beschreibung
ImportPolicy.psm1	PowerShell-Skriptmodul zum Importieren von Richtlinien nach XenApp 7.6.
ImportXAFarm.psm1	PowerShell-Skriptmodul zum Importieren von Richtlinien nach XenApp 7.6.
ImportPolicy.psd1	PowerShell-Manifestdatei für Skriptmodul ImportPolicy.psm1
ImportXAFarm.psd1	PowerShell-Manifestdatei für Skriptmodul ImportXAFarm.psm1
PolicyData.xsd	XML-Schema für Richtliniendaten.
XAFarmData.xsd	XML-Schema für XenApp-Farmdaten.
LogUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit Protokollierungsfunktionen
XmlUtilities.psd1	PowerShell-Manifestdatei für das Skriptmodul XmlUtilities.psm1.
XmlUtilities.psm1	Freigegebenes PowerShell-Skriptmodul mit XML-Funktionen

Einschränkungen

- Nicht alle Richtlinieneinstellungen werden importiert. Siehe Nicht importierte Richtlinieneinstellungen. Einstellungen, die nicht unterstützt werden, werden ignoriert und in der Protokolldatei angegeben.
- Zwar werden alle Anwendungsdetails während des Exportvorgangs in der XML-Ausgabedatei gesammelt, aber nur auf Servern installierte Anwendungen werden in die XenApp 7.6-Site importiert. Veröffentlichte Desktops, Inhalte und die meisten gestreamten Anwendungen werden nicht unterstützt (Informationen zu Ausnahmen finden Sie unter Schrittweise Anleitungen: Importieren von Daten) im Abschnitt zu den `Import-XAFarm`-Cmdlet-Parametern.
- Anwendungsserver werden nicht importiert.
- Viele Anwendungseigenschaften werden nicht importiert wegen der Unterschiede zwischen der XenApp 6.x Independent Management Architecture (IMA) und der XenApp 7.6 FlexCast Management Architecture (FMA). Siehe Zuordnung von Anwendungseigenschaften.
- Während des Imports wird eine Bereitstellungsgruppe erstellt. Weitere Informationen zum Filtern des importierten Inhalts mit Parametern finden Sie unter Erweiterte Verwendung.
- Nur Citrix-Richtlinieneinstellungen, die mit der AppCenter-Verwaltungskonsole erstellt wurden, werden importiert. Mit Windows-Gruppenrichtlinienobjekten (GPOs) erstellte Citrix-Richtlinieneinstellungen werden nicht importiert.

- Die Migrationsskripts sind nur für die Migrationen von XenApp 6.x auf XenApp 7.6 vorgesehen.
- Mehr als fünffach verschachtelte Ordner werden von Studio nicht unterstützt und werden nicht importiert. Wenn die Ordnerstruktur Ihrer Anwendung Ordner mit mehr als fünf Ebenen von Unterordnern enthält, reduzieren Sie vor dem Importieren die Anzahl der verschachtelten Ordnerebenen.

Sicherheitsüberlegungen

Die durch die Exportskripts erstellten XML-Dateien können vertrauliche Informationen über Ihre Umgebung und Organisation enthalten, z. B. Benutzer- und Servernamen und andere Farm-, Anwendungs- und Richtlinienkonfigurationsdaten. Speichern und verwenden Sie diese Dateien in einer sicheren Umgebung.

Prüfen Sie die XML-Dateien sorgfältig, bevor Sie sie als Eingabe für den Import von Richtlinien und Anwendungen verwenden, um sicherzustellen, dass sie keine unbefugten Änderungen enthalten.

Richtlinienobjektzuweisungen (bisher "Richtlinienfilter") steuern die Anwendung von Richtlinien. Nach dem Importieren von Richtlinien prüfen Sie die Objektzuweisungen für jede Richtlinie sorgfältig, um sicherzustellen, dass durch den Import keine Sicherheitsrisiken entstanden sind. Nach dem Import können auf die Richtlinie verschiedene Gruppen von Benutzern, IP-Adressen oder Clientnamen angewendet werden. Die Einstellungen zum Zulassen und Verweigern haben möglicherweise nach dem Import eine andere Bedeutung.

Protokollierung und Fehlerbehandlung

Die Skripts sorgen für umfangreiche Protokollierung, wobei die Ausführung aller Cmdlets, informative Meldungen, die Ergebnisse der Cmdlet-Ausführung sowie Warnungen und Fehler aufgezeichnet werden.

- Die Verwendung der Citrix PowerShell-Cmdlets wird größtenteils protokolliert. Alle PowerShell-Cmdlets in den Importskripts, die neue Siteobjekte erstellen, werden protokolliert.
- Der Skriptausführungsverlauf wird protokolliert, einschließlich der Objekte, die verarbeitet werden.
- Große Aktionen, die sich auf den Flussstatus auswirken, werden protokolliert, einschließlich über die Befehlszeile geleitete Flüsse.
- Alle Meldungen, die auf der Konsole gedruckt werden, einschließlich Warnungen und Fehler werden protokolliert.
- Jede Zeile wird mit einem Zeitstempel versehen, der auf die Millisekunde genau ist.

Citrix empfiehlt, dass Sie beim Ausführen der Export- und Import-Cmdlets jeweils eine Protokolldatei angeben.

Wenn Sie keinen Protokolldateinamen angeben, wird die Protokolldatei im Basisordner des aktuellen Benutzers (in der PowerShell-Variable `$HOME` angegeben) gespeichert. Wenn dieser Ordner nicht vorhanden ist, wird die Protokolldatei im aktuellen Ausführungsordner des Skripts gespeichert. Der Standardname der Protokolldatei ist `XFarmYYYYMMDDHHmmSS-xxxxxx`, wobei die letzten sechs Ziffern eine zufällige Zahl sind.

Standardmäßig werden die gesamten Fortschrittsinformationen angezeigt. Um die Anzeige zu unterdrücken, legen Sie den NoDetails-Parameter in den Export- und Import-Cmdlets fest.

Bei einem Fehler wird die Ausführung eines Skripts im Allgemeinen angehalten. Wenn der Fehler behoben ist, können Sie das Cmdlet noch einmal ausführen.

Bedingungen, die nicht als Fehler gelten, werden protokolliert. Viele werden als Warnungen gemeldet und das Ausführen des Skripts wird fortgesetzt. Beispielsweise werden nicht unterstützte Anwendungstypen als Warnung gemeldet und nicht importiert. Anwendungen, die bereits in der XenApp 7.6-Site vorhanden sind, werden nicht importiert. Richtlinieneinstellungen, die in XenApp 7.6 veraltet sind, werden nicht importiert.

Die Migrationsskripts verwenden viele PowerShell-Cmdlets und nicht alle möglichen Fehler werden protokolliert. Zusätzliche Protokollierungsfunktionen sind mit den PowerShell-Protokollierungsfeatures verfügbar. Beispielsweise wird alles, was auf dem Bildschirm gedruckt wird, in PowerShell-Aufzeichnungen protokolliert. Weitere Informationen finden Sie in der Hilfe zu den Cmdlets `Start-Transcript` und `Stop-Transcript`.

Anforderungen, Vorbereitungen und Best Practices

Zur Migration müssen Sie das Citrix XenApp 6.5-SDK verwenden. Laden Sie das SDK von https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.html herunter.

Lesen Sie den gesamten Artikel, bevor Sie mit der Migration beginnen.

Sie müssen grundlegende PowerShell-Konzepte verstehen. Obwohl umfangreiche Erfahrung mit dem Erstellen von Skripts nicht erforderlich ist, sollten Sie die ausgeführten Cmdlets verstehen. Mit dem Cmdlet `Get-Help` können Sie sich die Hilfe zu jedem Migrations-Cmdlet ansehen, bevor Sie es ausführen. Beispiel: `Get-Help -full Import-XAFarm`.

Geben Sie eine Protokolldatei in der Befehlszeile an und überprüfen Sie die Protokolldatei jedes Mal, nachdem Sie ein Cmdlet ausgeführt haben. Wenn ein Skript fehlschlägt, identifizieren Sie den Fehler mit der Protokolldatei und beheben Sie ihn. Führen Sie dann das Cmdlet noch einmal aus.

Nützliche Info:

- Zur Vereinfachung der Bereitstellung von Anwendungen während der Ausführung beider Bereitstellungen (vorhandene XenApp 6.x-Farm und neue XenApp 7.6-Site) können Sie beide Bereitstellungen in StoreFront oder dem Webinterface aggregieren. Weitere Informationen zu Ihrem

StoreFront- oder Webinterface-Release finden Sie in der Produktdokumentation (**Verwalten > Store erstellen**).

- Für die Handhabung der Anwendungssymboldaten gibt es zwei Möglichkeiten:
- Wenn Sie den Parameter `EmbedIconData` im Cmdlet `Export-XAFarm` angeben, werden exportierte Anwendungssymboldaten in der XML-Ausgabedatei eingebettet.
- Wenn Sie den Parameter `EmbedIconData` im Cmdlet `Export-XAFarm` nicht angeben, werden exportierte Anwendungssymboldaten werden in einem Ordner gespeichert. Der Name des Ordners wird durch Anfügen der Zeichenfolge `-icons` an den Basisnamen der XML-Ausgabedatei erstellt. Wenn der Parameter `XmlOutputFile` beispielsweise `FarmData.xml` ist, wird der Ordner `FarmData-icons` zum Speichern der Anwendungssymbole erstellt.

  Bei den Symboldatendateien in diesem Ordner handelt es sich um `.txt`-Dateien, die mit dem Browsernamen der veröffentlichten Anwendung benannt wurden. Obwohl es `.txt`-Dateien sind, handelt es sich bei den gespeicherten Daten um codierte binäre Symboldaten, die vom Importskript gelesen werden können, um das Anwendungssymbol neu zu erstellen. Wenn der Symbolordner während des Importvorgangs nicht im selben Verzeichnis gefunden wird wie die XML-Importdatei, werden allgemeine Symbole für die importierten Anwendungen verwendet.
- Die Namen der Skriptmodule, Manifestdateien, freigegebenen Module und Cmdlets sind ähnlich. Verwenden Sie die Tabulatortaste vorsichtig, damit es nicht zu Fehlern kommt. Zum Beispiel ist `Export-XAFarm` ein Cmdlet. `ExportXAFarm.psd1` und `ExportXAFarm.psm1` sind Dateien, die nicht ausgeführt werden können.
- In den nachfolgenden Anleitungen sind die meisten Parameterwerte für `<string>` mit Anführungszeichen umschlossen. Diese sind optional für Zeichenfolgen, die nur aus einem Wort bestehen.

Für den Export des XenApp 6.x-Servers gilt Folgendes:

- Der Export muss auf einem XenApp 6.x-Server ausgeführt werden, der mit dem Servermodus "Controller- und Sitzungshostmodus"(üblicherweise "Controller") konfiguriert wurde.
- Zum Ausführen der Export-Cmdlets müssen Sie XenApp-Administrator mit der Berechtigung zum Lesen von Objekten sein. Sie müssen auch über die erforderlichen Berechtigungen zum Ausführen von Windows-PowerShell-Skripts verfügen. Die schrittweisen Verfahren enthalten Anweisungen.
- Stellen Sie sicher, dass die XenApp 6.x-Farm funktionsfähig ist, bevor Sie mit dem Export beginnen. Erstellen Sie ein Backup der Farmdatenbank. Überprüfen Sie die Integrität der Farm mit dem Hilfsprogramm "Citrix IMA Helper"(CTX133983): Führen Sie von der Registerkarte für den IMA Datastore aus einen Master Check aus (und lösen Sie alle ungültigen Einträge mit der

Option `DSCheck` auf). Durch das Reparieren von Problemen vor der Migration werden Fehler beim Export vermieden.

Wenn ein Server beispielsweise nicht richtig aus der Farm entfernt wird, bleiben seine Daten möglicherweise in der Datenbank vorhanden, was zu Fehlern bei den Cmdlets im Exportskript führen kann (z. B. `Get-XAServer -ZoneName`). Wenn die Cmdlets fehlschlagen, schlägt das Skript fehl.

- Sie können die Export-Cmdlets in einer Farm mit aktiven Benutzerverbindungen ausführen. Die Exportskripte lesen nur die statische Farmkonfiguration und die Richtliniendaten.

Für den Import auf den XenApp 7.6-Server gilt Folgendes:

- Sie können Daten in XenApp 7.6-Bereitstellungen (und höhere unterstützte Versionen) importieren. Sie müssen einen XenApp 7.6-Controller und Studio installieren und eine Site erstellen, bevor Sie die aus der XenApp 6.x-Farm exportierten Daten importieren. VDAs sind zwar zum Importieren von Einstellungen nicht erforderlich, sie gestatten jedoch das Verfügbarmachen von Anwendungsdateitypen.
- Zum Ausführen der Import-Cmdlets müssen Sie XenApp-Administrator mit der Berechtigung zum Lesen und Erstellen von Objekten sein. Ein Volladministrator hat diese Berechtigungen. Sie müssen auch über die erforderlichen Berechtigungen zum Ausführen von Windows-PowerShell-Skripts verfügen. Die schrittweisen Verfahren enthalten Anweisungen.
- Während eines Imports dürfen keine anderen Benutzerverbindungen aktiv sein. Die Importskripts erstellen viele neue Objekte und wenn andere Benutzer gleichzeitig Änderungen an der Konfiguration vornehmen, können Unterbrechungen auftreten.

Sie können Daten exportieren und dann den Parameter `-Preview` für das Import-Cmdlet verwenden, um eine Vorschau des Imports zu sehen, ohne dass tatsächliche Importvorgänge stattfinden. Die Protokolle zeigen genau an, was während eines Imports passieren würde. Wenn Fehler auftreten, können Sie sie beheben, bevor Sie den Import starten.

Schrittweise Anleitungen: Exportieren von Daten

Führen Sie die folgenden Schritte aus, um Daten aus einem XenApp 6.x-Controller in XML-Dateien zu exportieren.

1. Laden Sie das Paket mit dem Migrationstool (`XAMigration.zip`) von der Citrix Downloadsite herunter. Speichern Sie es der Einfachheit halber in einer Netzwerkfreigabe, damit von der XenApp 6.x-Farm und der XenApp 7.6-Site darauf zugegriffen werden kann. Entzippen Sie `XAMigration.zip` in der Netzwerkfreigabe. Es gibt zwei ZIP-Dateien: `ReadIMA.zip` und `ImportFMA.zip`.
2. Melden Sie sich am XenApp 6.x-Controller als XenApp-Administrator mit mindestens Lesezugriff und Windows-Berechtigung zum Ausführen von PowerShell-Skripts an.

3. Kopieren Sie die Datei `ReadIMA.zip` von der Netzwerkfreigabe auf den XenApp 6.x-Controller. Entzippen und extrahieren Sie ReadIMA.zip auf dem Controller in einen Ordner (z. B. `C:\XAMigration`).
4. Öffnen Sie eine PowerShell-Konsole und legen Sie das aktuelle Verzeichnis als Skriptspeicherort fest (z. B. `cd C:\XAMigration`).
5. Überprüfen Sie die Skriptausführungsrichtlinie durch Ausführen von `Get-ExecutionPolicy` .
6. Legen Sie die Skriptausführungsrichtlinie mindestens auf `RemoteSigned` fest, damit die Skripts ausgeführt werden können (z. B. `Set-ExecutionPolicy RemoteSigned`).
7. Importieren Sie die Moduldefinitionsdateien `ExportPolicy.psd1` und `ExportXAFarm.psd1`:

   ```
   Import-Module .\ExportPolicy.psd1
   ```

   ```
   Import-Module .\ExportXAFarm.psd1
   ```

   Nützliche Info:

   - Wenn Sie nur Richtliniendaten exportieren möchten, können Sie nur die Moduldefinitionsdatei `ExportPolicy.psd1` importieren. Genauso gilt, wenn Sie nur Farmdaten importieren möchten, importieren Sie nur `ExportXAFarm.psd1`.
   - Beim Importieren der Moduldefinitionsdateien werden auch die erforderlichen PowerShell-Snap-Ins hinzugefügt.
   - Importieren Sie nicht die Skriptdateien mit der Erweiterung `.psm1`.
8. Führen Sie zum Exportieren von Richtliniendaten das Cmdlet `Export-Policy` aus.

Parameter	Beschreibung
-XmlOutputFile “.xml”	XML-Ausgabedateiname. Diese Datei enthält die exportierten Daten. Sie muss die Erweiterung .xml haben. Die Datei darf nicht vorhanden sein, aber wenn Sie den Pfad angeben, muss der übergeordnete Pfad vorhanden sein. Standard: Ohne. Dieser Parameter ist erforderlich.

Parameter	Beschreibung
-LogFile “”	Name der Protokolldatei. Eine Erweiterung ist optional. Die Datei wird erstellt, wenn sie nicht vorhanden ist. Wenn die Datei vorhanden ist und der Parameter “NoClobber”angegeben ist, wird ein Fehler generiert. Andernfalls wird der Inhalt der Datei überschrieben. Standardwert: siehe Protokollierung und Fehlerbehandlung.
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter “LogFile” , wenn er ebenfalls angegeben ist. Standard: False Die Protokollausgabe wird generiert.
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standard: False Eine vorhandene Protokolldatei wird überschrieben.
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standard: False Ausführliche Berichte werden an die Konsole gesendet.
-SuppressLogo	Drucken Sie die Meldung `XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#` nicht zu der Konsole. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein. Citrix empfiehlt daher, diesen Parameter wegzulassen. Standard: False Die Meldung wird zu der Konsole gedruckt.

Beispiel: Das folgende Cmdlet exportiert Richtlinieninformationen in die XML-Datei `MyPolicies`. Der Vorgang wird in der Datei `MyPolicies.log` protokolliert.

```
1 Export-Policy -XmlOutputFile ".\MyPolicies.XML" -LogFile ".\
     MyPolicies.Log"
2 <!--NeedCopy-->
```

9. Führen Sie zum Exportieren von Farmdaten das Cmdlet `Export-XAFarm` aus und geben Sie

dabei eine Protokolldatei und eine XML-Datei an.

Parameter	Beschreibung
-XmlOutputFile “.xml”	XML-Ausgabedateiname. Diese Datei enthält die exportierten Daten. Sie muss die Erweiterung .xml haben. Die Datei darf nicht vorhanden sein, aber wenn Sie den Pfad angeben, muss der übergeordnete Pfad vorhanden sein. Standard: Ohne. Dieser Parameter ist erforderlich.
-LogFile “”	Name der Protokolldatei. Eine Erweiterung ist optional. Die Datei wird erstellt, wenn sie nicht vorhanden ist. Wenn die Datei vorhanden ist und der Parameter “NoClobber”angegeben ist, wird ein Fehler generiert. Andernfalls wird der Inhalt der Datei überschrieben. Standardwert: siehe Protokollierung und Fehlerbehandlung.
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter “LogFile” , wenn er ebenfalls angegeben ist. Standard: False Die Protokollausgabe wird generiert.
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standard: False Eine vorhandene Protokolldatei wird überschrieben.
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standard: False Ausführliche Berichte werden an die Konsole gesendet.
-SuppressLogo	Drucken Sie die Meldung `XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#` nicht zu der Konsole. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein. Citrix empfiehlt daher, diesen Parameter wegzulassen. Standard: False Die Meldung wird zu der Konsole gedruckt.

Parameter	Beschreibung
-IgnoreAdmins	Administratorinformationen nicht exportieren. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standard: False Administratorinformationen werden exportiert.
-IgnoreApps	Anwendungsinformationen nicht exportieren. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standard: False Anwendungsinformationen werden exportiert.
-IgnoreServers	Serverinformationen nicht exportieren. Standard: False Serverinformationen werden exportiert.
-IgnoreZones	Zoneninformationen nicht exportieren. Standard: False Zoneninformationen werden exportiert.
-IgnoreOthers	Daten wie Folgende nicht exportieren: Konfigurationsprotokollierung, Lastauswertungsprogramme, Lastausgleichsrichtlinien, Druckertreiber und Workergruppen. Standard: False Andere Informationen werden exportiert. **Hinweis**: Mit diesem Schalter können Sie mit einem Export fortfahren, wenn ein Fehler auftritt, der sich nicht auf die tatsächlichen Daten auswirkt, die für den Export- oder Importvorgang verwendet werden.
-AppLimit	Anzahl der Anwendungen, die exportiert werden. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Alle Anwendungen werden exportiert.
-EmbedIconData	Anwendungssymboldaten in die gleiche XML-Datei einbetten wie die anderen Objekte. Standard: Symbole werden separat gespeichert. Einzelheiten finden Sie unter Anforderungen, Vorbereitungen und Best Practices.

Parameter	Beschreibung
-SkipApps	Anzahl der Anwendungen, die übersprungen werden. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Anwendungen werden übersprungen.

```
Example: The following cmdlet exports farm information to the XML file
    named MyFarm.xml. The operation is logged to the file MyFarm.log. A
    folder named "MyFarm-icons" is created to store the application icon
     data files. This folder is at the same location as MyFarm.XML.

`Export-XAFarm -XmlOutputFile ".\MyFarm.XML" -LogFile ".\MyFarm.Log"`
```

Nachdem die Ausführung der Exportskripts abgeschlossen ist, enthalten die in den Befehlszeilen angegebenen XML-Dateien die Richtliniendaten und die XenApp-Farmdaten. Die Anwendungssymboldateien enthalten die Symboldatendateien und die Protokolldatei gibt an, was sich beim Export ereignet hat.

Schrittweise Anleitungen: Importieren von Daten

Denken Sie daran, dass Sie einen Vorschauimport ausführen können (indem Sie das Cmdlet `Import-Policy` oder `Import-XAFarm` mit dem Parameter `Preview` ausführen). Sie können dann die Protokolldateien überprüfen, bevor Sie einen tatsächlichen Import durchführen.

Führen Sie die folgenden Schritte aus, um Daten mit den beim Export erstellten XML-Dateien in eine XenApp 7.6-Site zu importieren.

1. Melden Sie sich als Administrator mit Lese- und Schreibrechten und Windows-Berechtigung zum Ausführen von PowerShell-Skripts am XenApp 7.6-Controller an.
2. Wenn Sie das Paket mit dem Migrationstool (`XAMigration`) noch nicht in der Netzwerkfreigabe entzippt haben, führen Sie den Vorgang nun aus. Kopieren Sie die Datei `ImportFMA.zip` von der Netzwerkfreigabe auf den XenApp 7.6-Controller. Entzippen und extrahieren Sie `ImportFMA.zip` auf dem Controller in einen Ordner (z. B. `C:\XAMigration`).
3. Kopieren Sie die XML-Dateien (die während des Exports erstellten Ausgabedateien) vom XenApp 6.x-Controller in den Speicherort auf dem XenApp 7.6-Controller, wo Sie die Dateien aus `ImportFMA.zip` extrahiert haben.

   Wenn Sie die Anwendungssymboldaten beim Ausführen des Cmdlets `Export-XAFarm` nicht in die XML-Ausgabedatei eingebettet haben, kopieren Sie den Ordner mit den Symboldaten in den gleichen Speicherort auf dem XenApp 7.6-Controller, in den Sie die XML-Ausgabedateien kopiert haben und in dem die extrahierten Dateien aus `ImportFMA.zip` sind.

4. Öffnen Sie eine PowerShell-Konsole und legen Sie das aktuelle Verzeichnis als Skriptspeicherort fest (z. B. `cd C:\XAMigration`).
5. Überprüfen Sie die Skriptausführungsrichtlinie durch Ausführen von `Get-ExecutionPolicy`.
6. Legen Sie die Skriptausführungsrichtlinie mindestens auf `RemoteSigned` fest, damit die Skripts ausgeführt werden können (z. B. `Set-ExecutionPolicy RemoteSigned`).
7. Importieren Sie die PowerShell-Moduldefinitionsdateien `ImportPolicy.psd1` und `ImportXAFarm.psd1`:

   ```
   Import-Module .\ImportPolicy.psd1

   Import-Module .\ImportXAFarm.psd1
   ```

   Nützliche Info:

   - Wenn Sie nur Richtliniendaten importieren möchten, können Sie nur die Moduldefinitionsdatei `ImportPolicy.psd1` importieren. Genauso gilt, wenn Sie nur Farmdaten importieren möchten, importieren Sie nur `ImportXAFarm.psd1`.
   - Beim Importieren der Moduldefinitionsdateien werden auch die erforderlichen PowerShell-Snap-Ins hinzugefügt.
   - Importieren Sie nicht die Skriptdateien mit der Erweiterung `.psm1`.
8. Wenn Sie Richtliniendaten importieren, führen Sie das Cmdlet `Import-Policy` aus. Geben Sie dabei die XML-Datei mit den exportierten Richtliniendaten an.

Parameter	Beschreibung
-XmlInputFile “.xml”	XML-Eingabedateiname. Diese Datei enthält Daten, die beim Ausführen des Cmdlets `Export-Policy` gesammelt wurden. Die Erweiterung muss `.xml` sein. Standard: Ohne. Dieser Parameter ist erforderlich.
-XsdFile “”	Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: PolicyData.XSD

Parameter	Beschreibung
-LogFile “”	Name der Protokolldatei. Wenn Sie Exportprotokolldateien auf diesen Server kopiert haben, sollten Sie einen anderen Namen für die Protokolldatei des Import-Cmdlets verwenden. Standardwert: siehe Protokollierung und Fehlerbehandlung.
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter “LogFile” , wenn er ebenfalls angegeben ist. Standard: False Die Protokollausgabe wird generiert.
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standard: False Eine vorhandene Protokolldatei wird überschrieben.
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standard: False Ausführliche Berichte werden an die Konsole gesendet.
-SuppressLogo	Drucken Sie die Meldung `XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#` nicht zu der Konsole. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein. Citrix empfiehlt daher, diesen Parameter wegzulassen. Standard: False Die Meldung wird zu der Konsole gedruckt.

Parameter	Beschreibung
-Preview	Führen Sie eine Importvorschau aus: Daten werden aus der XML-Eingabedatei gelesen, aber es werden keine Objekte in die Site importiert. In der Protokolldatei und Konsole wird protokolliert, was während der Importvorschau vorgegangen ist. Eine Vorschau zeigt Administratoren, was während eines echten Imports passieren würde. Standard: False Es findet ein echter Import statt.

Beispiel: Mit dem folgenden Cmdlet werden Richtliniendaten aus der XML-Datei `MyPolcies.xml` importiert. Der Vorgang wird in der Datei `MyPolicies.log` protokolliert.

```
1 Import-Policy -XmlInputFile ".\MyPolicies.XML"
2 -LogFile ".\MyPolicies.Log"
3 <!--NeedCopy-->
```

9. Wenn Sie Anwendungen importieren, führen Sie das Cmdlet `Import-XAFarm` aus. Geben Sie dabei eine Protokolldatei und die XML-Datei mit den exportierten Farmdaten an.

Parameter	Beschreibung
-XmlInputFile “.xml”	XML-Eingabedateiname. Diese Datei enthält Daten, die mit dem Cmdlet “Export-XAFarm” gesammelt wurden. Sie muss die Erweiterung .xml haben. Standard: Ohne. Dieser Parameter ist erforderlich.
-XsdFile “”	Name der XSD-Datei. Mit dieser Datei überprüfen die Importskripts die Syntax der XML-Eingabedatei. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: XAFarmData.XSD
-LogFile “”	Name der Protokolldatei. Wenn Sie Exportprotokolldateien auf diesen Server kopiert haben, sollten Sie einen anderen Namen für die Protokolldatei des Import-Cmdlets verwenden. Standardwert: siehe Protokollierung und Fehlerbehandlung.

Parameter	Beschreibung
-NoLog	Keine Protokollausgabe erstellen. Dieser Parameter überschreibt den Parameter “LogFile” , wenn er ebenfalls angegeben ist. Standard: False Die Protokollausgabe wird generiert.
-NoClobber	Vorhandene Protokolldatei, die im Parameter “LogFile”angegeben wurde, nicht überschreiben. Wenn die Protokolldatei nicht vorhanden ist, hat dieser Parameter keine Auswirkung. Standard: False Eine vorhandene Protokolldatei wird überschrieben.
-NoDetails	Keine ausführlichen Berichte zur Skriptausführung an die Konsole senden. Standard: False Ausführliche Berichte werden an die Konsole gesendet.
-SuppressLogo	Drucken Sie die Meldung `XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#` nicht zu der Konsole. Diese Meldung, in der die Skriptversion angegeben wird, kann bei der Problembehandlung hilfreich sein. Citrix empfiehlt daher, diesen Parameter wegzulassen. Standard: False Die Meldung wird zu der Konsole gedruckt.
-Preview	Führen Sie eine Importvorschau aus: Daten werden aus der XML-Eingabedatei gelesen, aber es werden keine Objekte in die Site importiert. In der Protokolldatei und Konsole wird protokolliert, was während der Importvorschau vorgegangen ist. Eine Vorschau zeigt Administratoren, was während eines echten Imports passieren würde. Standard: False Es findet ein echter Import statt.
-DeliveryGroupName “”	Bereitstellungsgruppenname für alle importierten Anwendungen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standard: “-Delivery Group”

Parameter	Beschreibung
-MatchFolder “”	Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung.
-NotMatchFolder “”	Import von Anwendungen in Ordnern, deren Namen mit der Zeichenfolge (String) nicht übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung.
-MatchServer “”	Import von Anwendungen auf Servern, deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung.
-NotMatchServer “”	Import von Anwendungen auf Servern, deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung.
-MatchWorkerGroup “”	Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung.
-NotMatchWorkerGroup “”	Import von Anwendungen, die für Workergruppen veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung.

Parameter	Beschreibung
-MatchAccount “”	Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung.
-NotMatchAccount “”	Import von Anwendungen, die für Benutzerkonten veröffentlicht wurden und deren Namen nicht mit der Zeichenfolge (String) übereinstimmen. Informationen zur Verwendung finden Sie unter Erweiterte Verwendung. Standardwert: Keine Übereinstimmung.
-IncludeStreamedApps	Importieren Sie Anwendungen des Typs `StreamedToClientOrServerInstalled`. (Es werden keine anderen gestreamten Anwendungen importiert.) Standardwert: Gestreamte Anwendungen werden nicht importiert.
-IncludeDisabledApps	Import von Anwendungen, die als deaktiviert markiert sind. Standard: Deaktivierte Anwendungen werden nicht importiert.

Beispiel: Das folgende Cmdlet importiert Anwendungen aus der XML-Datei `MyFarm.xml`. Der Vorgang wird in der Datei `MyFarm.log` protokolliert.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"

<!--NeedCopy-->
```

10. Führen Sie nach dem Abschluss des Imports die nach der Migration erforderlichen Aufgaben durch.

Aufgaben nach der Migration

Nach dem erfolgreichen Import von XenApp 6.x-Richtlinien und Farmeinstellungen in eine XenApp 7.6-Site stellen Sie mit den folgenden Richtlinien sicher, dass die Daten richtig importiert wurden.

Richtlinien und Richtlinieneinstellungen

Das Importieren von Richtlinien ist im Prinzip ein Kopiervorgang mit Ausnahme von veralteten Einstellungen und Richtlinien, die nicht importiert werden. Mit der Prüfung nach der Migration werden die beiden Seiten verglichen.

1. In der Protokolldatei werden alle importierten und ignorierten Richtlinien und Einstellungen aufgeführt. Überprüfen Sie zuerst die Protokolldatei und identifizieren Sie die Einstellungen und Richtlinien, die nicht importiert wurden.
2. Vergleichen Sie die XenApp 6.x-Richtlinien mit den nach XenApp 7.6 importierten Richtlinien. Behalten Sie die Werte der Einstellungen bei (außer bei veralteten Richtlinieneinstellungen, siehe nächster Schritt).

    - Bei einer kleinen Anzahl von Richtlinien können Sie einen visuellen Vergleich der Richtlinien im XenApp 6.x AppCenter und in XenApp 7.6 Studio durchführen.
    - Wenn Sie viele Richtlinien haben, ist ein visueller Vergleich eventuell nicht möglich. Verwenden Sie in solchen Fällen das Export-Cmdlet (`Export-Policy`), um die XenApp 7.6-Richtlinien in eine andere XML-Datei zu exportieren. Vergleichen Sie dann mit einem Textvergleichsprogramm (z. B. `windiff`) die Daten der Datei mit den Daten in der XML-Datei, die zum Richtlinienexport aus XenApp 6.x verwendet wurde.

3. Der Abschnitt Nicht importierte Richtlinieneinstellungen enthält Informationen dazu, was sich beim Import geändert haben könnte. Wenn eine XenApp 6.x-Richtlinie nur veralteten Einstellungen enthält, wird die gesamte Richtlinie nicht importiert. Beispiel: Wenn eine XenApp 6.x-Richtlinie nur HMR-Testeinstellungen enthält, wird die Richtlinie ignoriert, da es keine entsprechende Einstellung in XenApp 7.6 gibt.

    Einige XenApp 6.x-Richtlinieneinstellungen werden nicht mehr unterstützt, aber vergleichbare Funktionen wurden in XenApp 7.6 implementiert. In XenApp 7.6 können Sie beispielsweise einen Neustartzeitplan für Serverbetriebssystemmaschinen konfigurieren, indem Sie eine Bereitstellungsgruppe bearbeiten. Diese Funktionalität wurde zuvor über Richtlinieneinstellungen implementiert.

4. Prüfen Sie, wie Filter für die XenApp 7.6-Site im Vergleich zu der XenApp 6.x angewendet werden. Signifikante Unterschiede zwischen der XenApp 6.x-Farm und der XenApp 7.6-Site können die Wirkung von Filtern verändern.

Filter

Überprüfen Sie sorgfältig die Filter für die einzelnen Richtlinien. Damit sie in XenApp 7.6 weiterhin genauso funktionieren wie in XenApp 6.x, sind möglicherweise Änderungen erforderlich.

Filter	Überlegungen
Zugriffssteuerung	Die Zugriffssteuerung enthält in der Regel die gleichen Werte wie die ursprünglichen XenApp 6.x-Filter und funktioniert ohne Änderungen.
Citrix CloudBridge	Ein einfacher boolescher Wert. Funktioniert normalerweise ohne Änderungen. (Dieses Produkt heißt jetzt NetScaler SD-WAN.)
Client-IP-Adresse	Listet Client-IP-Adressbereiche auf. Jeder Bereich ist entweder erlaubt oder gesperrt. Das Importskript behält die Werte bei, aber Änderungen können erforderlich sein, wenn sich andere Clients mit den XenApp 7.6-VDA-Maschinen verbinden.
Clientname	Ähnlich wie beim Client-IP-Adressenfilter behält das Importskript die Werte bei. Es können jedoch Änderungen erforderlich sein, wenn sich andere Clients mit den XenApp 7.6-VDA-Maschinen verbinden.
Organisationseinheit	Die Werte werden beibehalten, wenn die Organisationseinheiten beim Import aufgelöst werden können. Überprüfen Sie diesen Filter sorgfältig, besonders wenn die XenApp 6.x- und XenApp 7.6-Maschinen in unterschiedlichen Domänen sind. Wenn Sie die Filterwerte nicht richtig konfigurieren, wird die Richtlinie möglicherweise auf einen falschen Satz Organisationseinheiten angewendet. Die Organisationseinheiten werden nur durch Namen dargestellt, daher ist es möglich, dass eine Organisationseinheit zu einer Organisationseinheit aufgelöst wird, die andere Mitglieder enthält als die Organisationseinheit in der XenApp 6.x-Domäne. Selbst wenn einige Werte des Organisationseinheitsfilters beibehalten werden, prüfen Sie die Werte sorgfältig.

Filter	Überlegungen
Benutzer oder Gruppe	Die Werte werden beibehalten, wenn die Konten beim Import aufgelöst werden können. Ähnlich wie Organisationseinheiten werden die Konten nur nach Namen aufgelöst. Wenn die XenApp 7.6-Site eine Domäne mit den gleichen Domänen- und Benutzernamen enthält, wobei es sich aber tatsächlich um zwei verschiedene Domänen und Benutzer handelt, entsprechen die aufgelösten Konten möglicherweise nicht den Domänenbenutzern in XenApp 6.x. Wenn Sie die Filterwerte nicht richtig überprüfen und ändern, kann es zur falschen Anwendung von Richtlinien kommen.
Workergruppe	Workergruppen werden in XenApp 7.6 nicht unterstützt. Verwenden Sie die Bereitstellungsgruppe, den Bereitstellungsgruppentyp und die Tagfilter, die in XenApp 7.6 unterstützt werden (nicht in XenApp 6.x). Bereitstellungsgruppe: Ermöglicht das Anwenden von Richtlinien basierend auf Bereitstellungsgruppen. Jeder Filtereintrag gibt eine Bereitstellungsgruppe an und kann zugelassen oder verweigert werden. Bereitstellungsgruppentyp: Ermöglicht das Anwenden von Richtlinien basierend auf den Bereitstellungsgruppentypen. Jeder Filter gibt einen Bereitstellungsgruppentyp an und kann zugelassen oder verweigert werden. Tag: Gibt Richtlinienanwendung basierend auf Tags an, die für die VDA-Maschinen erstellt wurden. Jedes Tag kann zugelassen oder verweigert werden.

Filter, die Domänenbenutzeränderungen umfassen, müssen besonders sorgfältig überprüft werden, wenn die XenApp 6.x-Farm in einer anderen Domäne ist als die XenApp 7.6-Site. Da das Importskript nur die Zeichenfolgen von Domänen- und Benutzernamen verwendet, um Benutzer in der neuen Domäne aufzulösen, werden möglicherweise nur ein Teil der Konten aufgelöst. Obwohl nicht sehr wahrscheinlich ist, dass verschiedene Domänen und Benutzer den gleichen Namen haben, prüfen

Sie die Filter sorgfältig, um sicherzustellen, dass sie korrekte Werte enthalten.

Anwendungen

Die Skripts zum Import von Anwendungen importieren nicht nur Anwendungen. Sie erstellen auch Objekte wie Bereitstellungsgruppen. Wenn der Anwendungsimport mehrere Durchläufe umfasst, können sich die Originalhierarchien der Anwendungsordner erheblich ändern.

1. Lesen Sie als Erstes die Migrationsprotokolldateien, die Informationen dazu enthalten, welche Anwendungen importiert oder ignoriert wurden und welche Cmdlets zum Erstellen der Anwendungen verwendet wurden.
2. Für jede Anwendung gilt Folgendes:
    - Sehen Sie sich das Protokoll an und prüfen Sie, ob die grundlegenden Eigenschaften beim Importieren beibehalten wurden. Bestimmen Sie mit den Informationen unter Zuordnung von Anwendungseigenschaften, welche Eigenschaften ohne Änderungen importiert, nicht importiert oder mit den XenApp 6.x-Anwendungsdaten initialisiert wurden.
    - Überprüfen Sie die Benutzerliste. Das Importskript importiert automatisch die explizite Liste der Benutzer in die Liste "Sichtbarkeit beschränken"der Anwendung in XenApp 7.6. Stellen Sie sicher, dass die Liste unverändert ist.
3. Anwendungsserver werden nicht importiert. Dies bedeutet, dass auf keine der importierten Anwendungen zugegriffen werden kann. Den Bereitstellungsgruppen, die diese Anwendungen enthalten, müssen Maschinenkataloge mit den Maschinen zugewiesen werden, auf denen die ausführbaren Images der veröffentlichten Anwendungen sind. Für jede Anwendung gilt Folgendes:
    - Stellen Sie sicher, dass der Name der ausführbaren Datei und das Arbeitsverzeichnis auf eine ausführbare Datei verweisen, die auf den Maschinen vorhanden ist, die der Bereitstellungsgruppe (über die Maschinenkataloge) zugewiesen sind.
    - Überprüfen Sie einen Befehlszeilenparameter (dies kann ein beliebiges Objekt sein, z. B. Dateiname, Umgebungsvariable oder der Name einer ausführbaren Datei). Stellen Sie sicher, dass der Parameter für alle Maschinen in den Maschinenkatalogen, die der Bereitstellungsgruppe zugewiesen sind, gültig ist.

Protokolldateien

Die Protokolldateien sind die wichtigsten Referenzressourcen beim Import und Export. Aus diesem Grund werden bestehende Protokolldateien standardmäßig nicht überschrieben und Standardprotokolldateien haben eindeutige Namen.

Im Abschnitt Protokollierung und Fehlerbehandlung wurde bereits erwähnt, dass die Ausgabe und die Protokolldatei, die Sie erhalten, wenn Sie die verfügbaren zusätzlichen Protokollierungsfunktionen für die PowerShell-Cmdlets `Start-Transcript` und `Stop-Transcript` verwenden (sie protokollieren alles, was in die Konsole eingegeben und gedruckt wird), eine vollständige Referenz der Import- und Exportaktivitäten bieten.

Mit den Zeitstempeln in den Protokolldateien können Sie bestimmte Probleme diagnostizieren. Wenn beispielsweise ein Export oder Import lange gedauert hat, können Sie feststellen, ob eine fehlerhafte Datenbankverbindung oder das Auflösen von Benutzerkonten viel Zeit in Anspruch genommen haben.

Aus den in den Protokolldateien aufgezeichneten Befehlen lässt sich auch ermitteln, wie manche Objekte gelesen oder erstellt werden. Beispielsweise werden zum Erstellen einer Bereitstellungsgruppe mehrere Befehle ausgeführt, und zwar nicht nur, um das Bereitstellungsgruppenobjekt zu erstellen, sondern auch andere Objekte, wie die Zugriffsrichtlinienregeln, mit denen Anwendungsobjekte Bereitstellungsgruppen zugewiesen werden.

Mit der Protokolldatei kann auch ein fehlgeschlagener Export oder Import diagnostiziert werden. Normalerweise ist in den letzten Zeilen der Protokolldatei angegeben, was den Fehler verursacht hat. Die Fehlermeldung wird auch in der Protokolldatei gespeichert. Mit der Protokolldatei und der XML-Datei zusammen können Sie bestimmen, welches Objekt an dem Fehler beteiligt war.

Nach der Überprüfung und dem Test der Migration haben Sie folgende Möglichkeiten:

1. Upgrade der XenApp 6.5-Workerserver auf aktuelle Virtual Delivery Agents (VDAs) durch Ausführen des Installers für 7.6 auf den Servern. Der Installer entfernt die XenApp 6.5-Software und installiert dann automatisch einen aktuellen VDA. Anweisungen finden Sie unter Upgrade eines XenApp 6.5-Workers auf einen neuen VDA für Windows-Serverbetriebssysteme.

   Bei XenApp 6.0-Workerservern müssen Sie die XenApp 6.0-Software manuell vom Server deinstallieren. Danach können Sie mit dem Installer für 7.6 den aktuellen VDA installieren. Sie können mit dem Installer für 7.6 nicht automatisch die XenApp 6.0-Software entfernen.

2. Erstellen von Maschinenkatalogen (oder Bearbeiten von vorhandenen Katalogen) für die aktualisierten Worker in der neuen XenApp-Site mit Studio.

3. Hinzufügen der aktualisierten Maschinen aus dem Maschinenkatalog zu den Bereitstellungsgruppen, die die auf den VDAs für Windows-Serverbetriebssysteme installierten Anwendungen enthalten.

Erweiterte Verwendung

Standardmäßig exportiert das Cmdlet `Export-Policy` alle Richtliniendaten in eine XML-Datei. Analog exportiert das Cmdlet `Export-XAFarm` alle Farmdaten in eine XML-Datei. Sie können mit Befehlszeilenparametern genauer steuern, was importiert und exportiert wird.

Teilweises Exportieren von Anwendungen

Wenn Sie viele Anwendungen haben und steuern möchten, wie viele in die XML-Datei exportiert werden, verwenden Sie die folgenden Parameter:

- `AppLimit` - Gibt die Anzahl der zu exportierenden Anwendungen an.
- `SkipApps` - Gibt die Anzahl der zu überspringenden Anwendungen an, bevor Anwendungen exportiert werden.

Sie können beide Parameter verwenden, um große Mengen von Anwendungen in praktischen Segmenten zu exportieren. Beispiel: Wenn Sie das erste Mal "Export-XAFarm"ausführen, möchten Sie nur die ersten 200 Anwendungen exportieren und geben daher den Wert im Parameter "AppLimit" an.

```
Export-XAFarm -XmlOutputFile "Apps1-200.xml"
-AppLimit "200"
<!--NeedCopy-->
```

Wenn Sie das nächste Mal `Export-XAFarm` ausführen, möchten Sie die nächsten 100 Anwendungen exportieren. Sie verwenden den Parameter `SkipApps`, um die bereits exportierten Anwendungen (die ersten 200) zu ignorieren, und exportieren mit dem Parameter `AppLimit` die nächsten 100 Anwendungen.

```
Export-XAFarm -XmlOutputFile "Apps201-300.xml"
-AppLimit "100" -SkipApps "200"
<!--NeedCopy-->
```

Ausschließen von Objekten aus dem Export

Einige Objekte brauchen nicht exportiert zu werden, weil sie ignoriert werden können. Dazu zählen besonders Objekte, die nicht importiert werden. Siehe Nicht importierte Richtlinieneinstellungen und Zuordnung von Anwendungseigenschaften. Mit den folgenden Parametern können Sie den Export unnötiger Objekte verhindern:

- `IgnoreAdmins` - Administratorobjekte werden nicht exportiert
- `IgnoreServers` - Serverobjekte werden nicht exportiert
- `IgnoreZones` - Zonenobjekte werden nicht exportiert
- `IgnoreOthers` - Konfigurationsprotokollierungs-, Lastauswertungsprogramm-, Lastausgleichsrichtlinien-, Druckertreiber- und Workergruppenobjekte werden nicht exportiert
- `IgnoreApps` - Anwendungen werden nicht exportiert. Mit diesem Parameter können Sie andere Daten in eine XML-Ausgabedatei exportieren und dann den Export neu ausführen, um die Anwendungen in eine andere XML-Ausgabedatei zu exportieren.

Sie können mit diesen Parametern auch Probleme umgehen, die zum Fehlschlagen des Exports führen können. Wenn Sie beispielsweise einen fehlerhaften Server in einer Zone haben, schlägt der Zonenexport möglicherweise fehl. Wenn Sie den Parameter `IgnoreZones` einschließen, wird der Export mit anderen Objekten fortgesetzt.

Bereitstellungsgruppennamen

Wenn nicht alle Anwendungen in einer Bereitstellungsgruppe platziert werden sollen (z. B. weil verschiedene Benutzergruppen auf sie zugreifen und sie auf verschiedenen Servern veröffentlicht werden), führen Sie `Import-XAFarm` mehrmals aus und geben Sie dabei jedes Mal unterschiedliche Anwendungen und eine andere Bereitstellungsgruppe an. Sie können Anwendungen nach der Migration zwar mit PowerShell-Cmdlets von einer Bereitstellungsgruppe in eine andere verschieben, jedoch kann das Verschieben von Anwendungen durch selektives Importieren in eindeutige Bereitstellungsgruppen reduziert oder eliminiert werden.

- Verwenden Sie den Parameter `DeliveryGroupName` mit dem Cmdlet `Import-XAFarm`. Das Skript erstellt die angegebene Bereitstellungsgruppe, wenn sie nicht vorhanden ist.
- Verwenden Sie die folgenden Parameter mit regulären Ausdrücken, um die Anwendungen, die in die Bereitstellungsgruppe importiert werden sollen, basierend auf Ordner, Workergruppe Benutzerkontonamen und Servernamen zu filtern. Es empfiehlt sich, den regulären Ausdruck in einzelne oder doppelte Anführungszeichen zu setzen. Informationen zu regulären Ausdrücken finden Sie unter https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expressions.

  - `MatchWorkerGroup` und `NotMatchWorkerGroup` - Zum Beispiel bei Anwendungen, die auf Workergruppen veröffentlicht wurden, importiert das folgende Cmdlet Anwendungen in der Workergruppe `Productivity Apps` in eine XenApp 7.6-Bereitstellungsgruppe mit demselben Namen:

    ```
    1  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile
           XAFarmImport.log -MatchWorkerGroup 'Productivity Apps'
           -DeliveryGroupName 'Productivity Apps
    2  <!--NeedCopy-->
    ```

  - `MatchFolder` und `NotMatchFolde`r - Zum Beispiel bei Anwendungen, die in Anwendungsordnern organisiert sind, importiert das folgende Cmdlet Anwendungen im Ordner `Productivity Apps` in eine XenApp 7.6-Bereitstellungsgruppe mit dem gleichen Namen.

    ```
    1  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile
           XAFarmImport.log -MatchFolder 'Productivity Apps' -
           DeliveryGroupName 'Productivity Apps'
    2  <!--NeedCopy-->
    ```


Beispielsweise importiert das folgende Cmdlet Anwendungen in Ordnern, deren Name `MS Office Apps` enthält, in die Standardbereitstellungsgruppe.

```
1  Import-XAFarm -XmlInputFile .\THeFarmApps.XML -MatchFolder "
       .\*/MS Office Apps/.\*"
2  <!--NeedCopy-->
```

- `MatchAccount` und `NotMatchAccount` - Zum Beispiel bei Anwendungen, die für Active Directory-Benutzer oder -Benutzergruppen veröffentlicht wurden, importiert das folgende Cmdlet Anwendungen, die für die Benutzergruppe `Finance Group` veröffentlicht wurden, in eine XenApp 7.6-Bereitstellungsgruppe mit dem Namen `Finance`.

```
1  Import-XAFarm  –XmlInputFile XAFarm.xml  –LogFile
       XAFarmImport.log  –MatchAccount  'DOMAIN\Finance Group'
       –DeliveryGroupName  'Finance'
2  <!--NeedCopy-->
```

- `MatchServer` und `NotMatchServer` - Zum Beispiel bei Anwendungen, die auf Servern organisiert sind, importiert das folgende Cmdlet Anwendungen von Servern, deren Name nicht `Current` ist, in eine Bereitstellungsgruppe mit dem Namen `Legacy`.

```
1  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.
       log -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
2  <!--NeedCopy-->
```

Anpassung

PowerShell-Programmierer können eigene Tools erstellen. Sie können z. B. das Exportskript als Bestandstool verwenden und damit die Änderungen in einer XenApp 6.x-Farm verfolgen. Sie können auch die XSD-Dateien ändern oder Ihre eigenen XSD-Dateien erstellen, um zusätzliche Daten oder Daten in unterschiedlichen Formaten in den XML-Dateien zu speichern. Sie können eine nicht standardmäßige XSD-Datei mit jedem der Import-Cmdlets angeben.

Obwohl Sie Skriptdateien für bestimmte oder höhere Migrationsanforderungen ändern können, ist der Support auf unveränderte Skripts beschränkt. Der technische Support von Citrix empfiehlt, die Skripts in den Originalzustand zurückzuversetzen, um bei Bedarf erwartetes Verhalten ermitteln und Support bereitstellen zu können.

Problembehandlung

- Wenn Sie PowerShell 2.0 verwenden und das PowerShell-Anbieter-Snap-In für Citrix Gruppenrichtlinien oder das Citrix Common Commands Snap-In mit dem Cmdlet `Add-PSSnapIn` hinzugefügt haben, wird möglicherweise die folgende Fehlermeldung angezeigt, wenn Sie

Cmdlets zum Exportieren oder Importieren ausführen: `Object reference not set to an instance of an object` Dieser Fehler wirkt sich nicht auf die Skriptausführung aus und kann bedenkenlos ignoriert werden.

- Vermeiden Sie es, das PowerShell-Anbieter-Snap-In für Citrix Gruppenrichtlinien in der gleichen Konsolensitzung hinzuzufügen oder zu entfernen, in der Sie die Export- und Importskriptmodule verwenden, da diese Skriptmodule das Snap-In automatisch hinzufügen. Wenn Sie das Snap-In separat hinzufügen oder entfernen, wird u. U. einer der folgenden Fehler angezeigt:
  - `A drive with the name 'LocalGpo'already exists.` Dieser Fehler tritt auf, wenn das Snap-In zweimal hinzugefügt wird. Beim Laden versucht das Snap-In, das Laufwerk "LocalGpo"bereitzustellen und meldet dann den Fehler.
  - `A parameter cannot be found that matches parameter name 'Controller'.` Dieser Fehler wird angezeigt, wenn das Snap-In nicht hinzugefügt wurde und das Skript versucht, das Laufwerk bereitzustellen. Das Skript erkennt nicht, dass das Snap-In entfernt wurde. Schließen Sie die Konsole und starten Sie eine neue Sitzung. Importieren Sie in der neuen Sitzung die Skriptmodule. Fügen Sie das Snap-In nicht separat hinzu oder entfernen es.
- Wenn Sie beim Importieren der Module mit der rechten Maustaste auf eine `.psd1`-Datei klicken und **Öffnen** oder **Mit PowerShell öffnen** auswählen, wird das PowerShell-Konsolenfenster schnell geöffnet und geschlossen, bis Sie den Prozess beenden. Sie vermeiden diesen Fehler, indem Sie den vollständigen Namen des PowerShell-Skriptmoduls direkt im PowerShell-Konsolenfenster eingeben (z. B. `Import-Module .\ExportPolicy.psd1`).
- Wenn beim Ausführen eines Exports oder Imports ein Berechtigungsfehler angezeigt wird, stellen Sie sicher, dass Sie ein XenApp-Administrator mit der Berechtigung zum Lesen von Objekten (beim Export) oder zum Lesen und Erstellen von Objekten (beim Import) sind. Sie müssen auch über die erforderlichen Berechtigungen zum Ausführen von Windows-PowerShell-Skripts verfügen.
- Wenn ein Export fehlschlägt, prüfen Sie, ob die XenApp 6.x-Farm funktionsfähig ist, indem Sie die Dienstprogramme DSMAINT und DSCHECK auf dem XenApp 6.x Controller-Server ausführen.
- Wenn Sie mit den Import-Cmdlets eine Importvorschau ausführen und später bei der tatsächlichen Migration nichts importiert wird, prüfen Sie, ob Sie den Parameter "Preview"aus den Import-Cmdlets entfernt haben.

Nicht importierte Richtlinieneinstellungen

Die folgenden Computer- und Benutzerrichtlinieneinstellungen werden nicht importiert, da sie nicht mehr unterstützt werden. Ungefilterte Richtlinien werden nie importiert. Die Features und Kompo-

nenten, die diese Einstellungen unterstützen, wurden entweder durch neue Technologien und Komponenten ersetzt oder sind aufgrund von Änderungen an Architektur oder Plattform nicht relevant.

Nicht importierte Computerrichtlinieneinstellungen

- Verbindungszugriffssteuerung
- CPU-Managementserverstufe
- DNS-Adressauflösung
- Farm name
- Vollständige Symbolzwischenspeicherung
- Systemüberwachung, Systemüberwachungstests
- Hostname des Lizenzservers, den Lizenzserverport
- Limit für Benutzersitzungen, Limits für Administratorsitzungen
- Lastauswertungsprogrammname
- Protokollierung von Anmeldelimitereignissen
- Maximaler Prozentsatz von Servern mit Anmeldesteuerung
- Speicheroptimierung, Speicheroptimierung - Anwendungsausschlussliste, Speicheroptimierung - Intervall, Speicheroptimierung - Tag des Monats, Speicheroptimierung - Wochentag, Speicheroptimierung - Zeit
- Offlineanwendungsclient vertrauen, Ereignisprotokollierung für Offlineanwendungen, Offlineanwendungslizenzzeitraum, Offlineanwendungsbenutzer
- Zur Kennworteingabe auffordern
- Benutzerdefinierte Neustartwarnung, Text für benutzerdefinierte Neustartwarnung, Anmeldungen vor Neustart deaktivieren (Zeit), Neustarthäufigkeit, Willkürliches Neustartintervall, Neustartbeginn, Neustartzeit, Neustartwarnungsintervall, Neustartwarnung - Startzeit, Neustartwarnung an Benutzer, Geplante Neustarts
- Spiegeln von Sitzungen *
- XML-Anfragen vertrauen (Konfiguration in StoreFront)
- Virtuelle IP - Adapteradressenfilterung, Virtuelle IP - Liste kompatibler Programme, Virtuelle IP - Erweiterte Kompatibilität, Virtuelle IP - Adapteradressenprogrammliste
- Arbeitslastname
- XenApp-Produktedition, XenApp-Produktmodell
- Port für XML-Dienst

* Ersetzt durch Windows-Remoteunterstützung

Nicht importierte Benutzerrichtlinieneinstellungen

- Client-COM-Ports automatisch verbinden, Client-LPT-Ports automatisch verbinden
- Client-COM-Portumleitung, Client-LPT-Portumleitung

- Clientdruckernamen
- Limit für gleichzeitige Anmeldungen
- Eingaben in gespiegelten Verbindungen *
- Trennentimerintervall - Fortbestehen, Beendentimerintervall - Fortbestehen
- Spiegelungsversuche protokollieren *
- Benutzer bei ausstehenden Spiegelungsverbindungen benachrichtigen *
- PreLaunch-Trennentimerintervall, PreLaunch-Beendentimerintervall
- Sitzungspriorität
- Single Sign-On, Zentraler Speicher für Single Sign-On
- Benutzer, die andere Benutzer spiegeln können; Benutzer, die andere Benutzer nicht spiegeln können *

* Ersetzt durch Windows-Remoteunterstützung

Nicht importierte Anwendungstypen

Die folgenden Anwendungstypen werden nicht importiert:

- Serverdesktops
- Inhalt
- Gestreamte Anwendungen (App-V ist die neue Methode für das Streaming von Anwendungen)

Zuordnung von Anwendungseigenschaften

Das Importskript für Farmdaten importiert nur Anwendungen. Die folgenden Anwendungseigenschaften werden ohne Änderungen importiert.

IMA-Eigenschaft	FMA-Eigenschaft
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Beschreibung	Beschreibung
DisplayName	PublishedName
Aktiviert	Aktiviert
StartMenuFolder	StartMenuFolder

IMA-Eigenschaft	FMA-Eigenschaft
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

IMA und FMA haben unterschiedliche Beschränkungen bei der Länge der Ordnernamen. In IMA ist die Länge der Ordnernamen auf 256 Zeichen beschränkt. Das FMA-Limit ist 64 Zeichen. Anwendungen, deren Ordnerpfad einen Ordnernamen mit mehr als 64 Zeichen enthält, werden beim Import übersprungen. Das Limit gilt nur für den Ordnernamen im Ordnerpfad. Der gesamte Ordnerpfad kann länger als die angegebenen Grenzwerte sein. Damit Anwendungen beim Importieren nicht übersprungen werden, empfiehlt Citrix, die Länge der Anwendungsordnernamen zu prüfen und bei Bedarf vor dem Export zu kürzen.

Die folgenden Anwendungseigenschaften sind standardmäßig initialisiert oder nicht initialisiert oder auf die in den XenApp 6.x-Daten bereitgestellten Werte festgelegt:

FMA-Eigenschaft	Wert
Name	Initialisiert auf den vollständigen Pfadnamen, der die IMA-Eigenschaften “FolderPath”und “DisplayName”enthält, aber die voranstehende Zeichenfolge “Applications\”wurde gekürzt
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialisiert mit den XenApp 6.x-Befehlszeilenargumenten
IconFromClient	Nicht initialisiert, Standardwert = false
IconUid	Initialisiert auf ein Symbolobjekt, das mit XenApp 6.x-Symboldaten erstellt wurde
SecureCmdLineArgumentsEnabled	Nicht initialisiert, Standardwert = true
UserFilterEnabled	Nicht initialisiert, Standardwert = false
UUID	Schreibgeschützt, vom Controller zugewiesen
Sichtbar	Nicht initialisiert, Standardwert = true

Die folgenden Anwendungseigenschaften werden teilweise migriert:

IMA-Eigenschaft	Anmerkungen
FileTypes	Nur in der neuen XenApp-Site existierende Dateitypen werden migriert. Dateitypen, die in der neuen Site nicht existieren, werden ignoriert. Dateitypen werden erst importiert, wenn die Dateitypen in der neuen Site aktualisiert wurden.
IconData	Neue Symbolobjekte werden erstellt, wenn die Symboldaten für die exportierten Anwendungen angegeben wurden.
Konten	Die Benutzerkonten einer Anwendung werden zwischen der Benutzerliste für die Bereitstellungsgruppe und der Anwendung aufgeteilt. Explizite Benutzer werden zur Initialisierung der Benutzerliste für die Anwendung verwendet. Zudem wird der Benutzerliste für die Bereitstellungsgruppe das Konto “Domänenbenutzer”für die Domäne der Benutzerkonten hinzugefügt.

Die folgenden XenApp 6.x-Eigenschaften werden nicht importiert:

IMA-Eigenschaft	Anmerkungen
ApplicationType	Wird ignoriert.
HideWhenDisabled	Wird ignoriert.
AccessSessionConditions	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
AccessSessionConditionsEnabled	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
ConnectionsThroughAccessGatewayAllowed	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
OtherConnectionsAllowed	Ersetzt durch Bereitstellungsgruppenzugriffsrichtlinien.
AlternateProfiles	FMA unterstützt keine gestreamten Anwendungen.
OfflineAccessAllowed	FMA unterstützt keine gestreamten Anwendungen.

IMA-Eigenschaft	Anmerkungen
ProfileLocation	FMA unterstützt keine gestreamten Anwendungen.
ProfileProgramArguments	FMA unterstützt keine gestreamten Anwendungen.
ProfileProgramName	FMA unterstützt keine gestreamten Anwendungen.
RunAsLeastPrivilegedUser	FMA unterstützt keine gestreamten Anwendungen.
AnonymousConnectionsAllowed	FMA verwendet eine andere Technologie für die Unterstützung nicht authentifizierter (anonymer) Verbindungen.
ApplicationId, SequenceNumber	IMA-eigene Daten.
AudioType	FMA unterstützt keine erweiterten Clientverbindungsoptionen.
EncryptionLevel	SecureICA ist in Bereitstellungsgruppen aktiviert/deaktiviert.
EncryptionRequired	SecureICA ist in Bereitstellungsgruppen aktiviert/deaktiviert.
SslConnectionEnabled	FMA verwendet eine andere TLS-Implementierung.
ContentAddress	FMA unterstützt keinen veröffentlichten Inhalt.
ColorDepth	FMA unterstützt keine erweiterten Fensterformen.
MaximizedOnStartup	FMA unterstützt keine erweiterten Fensterformen.
TitleBarHidden	FMA unterstützt keine erweiterten Fensterformen.
WindowsType	FMA unterstützt keine erweiterten Fensterformen.
InstanceLimit	FMA unterstützt keine Anwendungslimits.
MultipleInstancesPerUserAllowed	FMA unterstützt keine Anwendungslimits.
LoadBalancingApplicationCheckEnabled	FMA verwendet eine andere Technologie für den Lastausgleich.
PreLaunch	FMA verwendet eine andere Technologie für den Sitzungsvorabstart.

IMA-Eigenschaft	Anmerkungen
CachingOption	FMA verwendet eine andere Technologie für den Sitzungsvorabstart.
ServerNames	FMA verwendet eine andere Technologie.
WorkerGroupNames	FMA unterstützt keine Workergruppen.

Sicherheit

November 29, 2018

XenApp und XenDesktop bieten eine auf Sicherheit ausgelegte Lösung, mit der Sie Ihre Umgebung Ihren Sicherheitsanforderungen anpassen können.

Bei mobilen Mitarbeitern steht die IT-Abteilung dem Sicherheitsrisiko durch verlorene oder gestohlene Daten gegenüber. Durch Hosten von Anwendungen und Desktops trennen XenApp und XenDesktop sicher vertrauliche Daten und geistiges Eigentum von Endpunktgeräten, da alle Daten in einem Datencenter gespeichert werden. Wenn Richtlinien für das Zulassen von Datenübertragungen aktiviert sind, werden alle Daten verschlüsselt.

Die XenDesktop- und XenApp-Datencenter vereinfachen auch die Reaktion auf Vorfälle mit einem zentralisierten Überwachungs- und Verwaltungsdienst. Mit Director überwachen und analysieren IT-Mitarbeiter Daten, auf die im Netzwerk zugegriffen wird, und mit Studio kann die IT-Abteilung im Datencenter Patches anwenden und Systemanfälligkeiten verhindern statt Probleme lokal auf jedem Endbenutzergerät zu beheben.

XenApp und XenDesktop vereinfachen auch Audits und die Einhaltung der Richtlinientreue, da Untersuchende mit einer zentralisierten Überwachungsliste ermitteln können, wer auf welche Anwendungen und Daten zugegriffen hat. Director sammelt durch Zugriff auf die Konfigurationsprotokollierung und die OData-API Verlaufsdaten über Updates des Systems und der Benutzerdatennutzung.

Mit der delegierten Administration richten Sie Administratorrollen ein, um den Zugriff auf XenDesktop und XenApp auf granulärer Ebene zu steuern. Dies ermöglicht Flexibilität in Ihrer Organisation, um bestimmten Administratoren vollständigen Zugriff auf Aufgaben, Vorgänge und Geltungsbereiche zugeben, während der Zugriff anderer Administratoren beschränkt ist.

Mit XenApp und XenDesktop wenden Administratoren Richtlinien auf verschiedenen Netzwerkebenen, von der lokalen Ebene bis zur Organisationseinheitsebene, an und steuern damit Benutzer granular. Diese Steuerung der Richtlinien legt fest, ob ein Benutzer, ein Gerät oder eine Gruppe von Benutzern und Geräten eine Verbindung herstellen, Kopieren bzw. Einfügen oder lokale Laufwerke

zuordnen können. Dies verringert Sicherheitsbedenken bei Zeitpersonal von Drittanbietern. Administratoren können auch Desktop Lock verwenden, sodass Benutzer nur den virtuellen Desktop verwenden können und der Zugriff auf das lokale Betriebssystem des Endbenutzergeräts verhindert wird.

Administratoren können die Sicherheit in XenApp oder XenDesktop erhöhen und die Site so konfigurieren, dass sie das TLS-Sicherheitsprotokoll (Transport Layer Security) des Controllers oder zwischen Endbenutzern und VDAs verwendet. Das Protokoll kann auch für eine Site aktiviert werden, um die Serverauthentifizierung, die Verschlüsselung des Datenstroms und die Prüfung der Nachrichtenintegrität für eine TCP/IP-Verbindungen bereitzustellen.

XenApp und XenDesktop unterstützen auch die mehrstufige Authentifizierung für Windows oder eine bestimmte Anwendung. Mit der mehrstufigen Authentifizierung können auch alle Ressourcen, die von XenApp und XenDesktop bereitgestellt werden, verwaltet werden. Diese Methoden sind u. a.:

- Token
- Smartcards
- RADIUS
- Kerberos
- Biometrie

XenDesktop kann mit vielen Sicherheitslösungen von Drittanbietern verwendet werden, von der Identitätsverwaltung bis zu Antivirensoftware. Eine Liste der unterstützten Produkte finden Sie unter https://www.citrix.com/ready.

Bestimmte Releases von XenApp und XenDesktop sind für Common Criteria zertifiziert. Eine Liste dieser Normen finden Sie unter https://www.commoncriteriaportal.org/cc/.

Bewährte Methoden und Überlegungen zur Sicherheit

August 18, 2021

> **Hinweis:**
>
> Möglicherweise muss Ihre Organisation bestimmte Sicherheitsstandards einhalten, um den gesetzlichen Anforderungen zu genügen. In diesem Dokument wird dieses Thema nicht behandelt, da sich Sicherheitsstandards mit der Zeit ändern. Aktuelle Informationen über Sicherheitsstandards und Citrix Produkte finden Sie unter https://www.citrix.com/security/.

Optimale Verfahren zur Sicherheit

Halten Sie stets alle Computer in der Umgebung mit Sicherheitspatches auf dem neuesten Stand. Ein Vorteil besteht darin, dass Thin Clients als Terminals verwendet werden können. Das erleichtert diese Aufgabe.

Schützen Sie alle Maschinen in der Umgebung mit Antivirensoftware.

Erwägen Sie plattformspezifische Antischadsoftware, wie z. B. das Microsoft Enhanced Mitigation Experience Toolkit (EMET) für Windows-Maschinen. Manche Organisationen empfehlen, die neueste von Microsoft unterstützte Version von EMET in ihren regulierten Umgebungen zu verwenden. Beachten Sie, dass gemäß Microsoft EMET mit mancher Software nicht kompatibel ist. Es muss also gründlich mit Ihren Anwendungen getestet werden, bevor es in einer Produktionsumgebung bereitgestellt wird. XenApp und XenDesktop wurden mit EMET 5.5 in der Standardkonfiguration getestet. Derzeit wird EMET nicht für die Verwendung auf einer Maschine empfohlen, auf der ein Virtual Delivery Agent (VDA) installiert ist.

Schützen Sie alle Maschinen in der Umgebung mit Perimeterfirewalls, u. a. bei Bedarf auch an Grenzen von Enklaven.

Wenn Sie eine konventionelle Umgebung zu diesem Release migrieren, müssen Sie ggf. eine vorhandene Perimeterfirewall neu positionieren oder neue Perimeterfirewalls hinzufügen. Beispiel: Zwischen einem konventionellen Client und einem Datenbankserver im Datenzentrum ist eine Perimeterfirewall. Bei diesem Release muss diese Perimeterfirewall so platziert werden, dass der virtuelle Desktop und das Benutzergerät auf der einen Seite sind und die Datenbankserver und Controller im Datencenter auf der anderen Seite. Es empfiehlt sich daher, im Datencenter einen Netzbereich für die verwendeten Datenbankserver und Controller zu erstellen. Außerdem sollten Sie die Installation eines Schutzmechanismus zwischen dem Benutzergerät und dem virtuellen Desktop in Betracht ziehen.

Alle Maschinen in der Umgebung müssen durch eine persönliche Firewall geschützt werden. Wenn Sie Kernkomponenten und VDAs installieren, können Sie die erforderlichen Ports für Komponenten und Features so einrichten, dass sie automatisch geöffnet werden, sobald der Windows-Firewalldienst erkannt wird (auch wenn die Firewall nicht aktiviert ist). Sie können die Firewallports auch manuell konfigurieren. Wenn Sie eine andere Firewall verwenden, muss diese manuell konfiguriert werden.

Hinweis: Da die TCP-Ports 1494 und 2598 für ICA und CGP verwendet werden, sind sie normalerweise an der Firewall geöffnet, damit Benutzer außerhalb des Rechenzentrums auf sie zugreifen können. Citrix empfiehlt, dass diese Ports nicht für etwas Anderes verwendet werden, damit administrative Benutzeroberflächen nicht versehentlich gefährdet werden. Die Ports 1494 und 2598 sind offiziell bei der Internet Assigned Number Authority (https://www.iana.org/) registriert.

Die gesamte Netzwerkkommunikation sollte Ihren Sicherheitsrichtlinien gemäß angemessen gesichert und verschlüsselt werden. Sie können die gesamte Kommunikation zwischen Microsoft Windows-Computern mit IPSec sichern. Weitere Informationen hierzu finden Sie in der Dokumenta-

tion zum Betriebssystem. Die Kommunikation zwischen Benutzergeräten und Desktops ist außerdem mit Citrix SecureICA gesichert, das in der Standardeinstellung 128-Bit-Verschlüsselung verwendet. Sie können beim Erstellen oder Aktualisieren einer Bereitstellungsgruppe SecureICA konfigurieren.

> **Hinweis:**
>
> Citrix SecureICA ist Teil des ICA/HDX-Protokolls, aber es ist kein standardkonformes Netzwerksicherheitsprotokoll wie Transport Layer Security (TLS). Sie können auch die Netzwerkkommunikation zwischen Benutzergeräten und Desktops mit TLS sichern. Informationen zum Konfigurieren von TLS finden Sie unter Transport Layer Security (TLS).

Übernehmen Sie die für Windows empfohlenen bewährten Methoden bei der Benutzerkontenverwaltung. Erstellen Sie kein Konto auf einer Vorlage oder einem Image, bevor dieses durch Maschinenerstellungsdienste (MCS) oder Provisioning Services dupliziert wurde. Planen Sie keine Aufgaben mit gespeicherten privilegierten Domänenkonten. Erstellen manuell Sie keine freigegebenen Active Directory-Computerkonten. Durch diese Vorgehensweise wird verhindert, dass ein lokales permanentes Kontokennwort für einen Angriff unter Anmeldung bei mit MCS bzw. PVS freigegebenen Images Anderer verwendet wird.

Anwendungssicherheit

Um zu verhindern, dass Benutzer ohne Administratorrechte schädliche Aktionen ausführen, empfiehlt es sich, Windows AppLocker-Regeln für Installationsprogramme, Anwendungen, ausführbare Dateien und Skripts auf dem VDA-Host und dem lokalen Windows-Client zu konfigurieren.

Verwalten von Benutzerprivilegien

Geben Sie Benutzern nur die Rechte, die sie benötigen. Microsoft Windows-Privilegien können weiterhin in der üblichen Weise auf Desktops angewendet werden: Konfigurieren Sie Privilegien mit "Zuweisung von Benutzerrechten"und Gruppenmitgliedschaften mit einer Gruppenrichtlinie. Der Vorteil dieses Release besteht darin, dass einem Benutzer Administratorrechte für einen Desktop eingeräumt werden können, ohne ihm auch die physische Kontrolle über den Computer, auf dem der Desktop gespeichert ist, zu gewähren.

Beachten Sie beim Planen von Desktopprivilegien Folgendes:

- Standardmäßig wird nicht berechtigten Benutzern beim Herstellen einer Verbindung mit einem Desktop die Zeitzone des Systems, auf dem der Desktop ausgeführt wird, statt der Zeitzone ihres eigenen Benutzergerätes angezeigt. Weitere Informationen dazu, wie Sie Benutzern erlauben, ihre Ortszeit beim Verwenden von Desktops anzuzeigen, finden Sie unter Ändern von Grundeinstellungen.

- Ein Benutzer mit Administratorrechten auf einem Desktop hat Vollzugriff auf diesen Desktop. Wenn ein Desktop ein gepoolter Desktop und kein dedizierter Desktop ist, muss dem Benutzer von allen anderen Benutzern dieses Desktops, einschließlich zukünftiger Benutzer, vertraut werden. Alle Benutzer des Desktops müssen sich des potenziellen permanenten Risikos für ihre Datensicherheit bewusst sein, die diese Situation mit sich bringt. Diese Überlegung trifft nicht auf dedizierte Desktops zu, die nur einen einzelnen Benutzer haben. Dieser Benutzer sollte kein Administrator auf einem anderen Desktop sein.
- Ein Benutzer mit Administratorrechten auf einem Desktop kann auf diesem Desktop generell Software installieren, einschließlich potenziell schädlicher Software. Zudem kann der Benutzer u. U. den Datenverkehr in allen mit dem Desktop verbundenen Netzwerken überwachen und steuern.

Einige Anwendungen erfordern Desktopprivilegien, obwohl sie für Benutzer und nicht für Administratoren konzipiert sind. Die damit verbundenen Sicherheitsrisiken sind Benutzern nicht immer bewusst.

Behandeln Sie diese Anwendungen wie hochsensible Anwendungen, selbst wenn ihre Daten nicht vertraulich sind. Erwägen Sie diese Maßnahmen zur Verringerung des Sicherheitsrisikos:

- Erzwingen Sie die zweistufige Authentifizierung und deaktivieren Single Sign-On für diese Anwendung.
- Erzwingen Sie kontextbezogene Zugriffsrichtlinien.
- Veröffentlichen Sie die Anwendung auf einem dedizierten Desktop. Falls die Anwendung auf einem freigegebenen gehosteten Desktop veröffentlicht werden muss, sollten Sie keine anderen Anwendungen auf diesem Desktop veröffentlichen.
- Stellen Sie sicher, dass die Desktopprivilegien nur für diesen Desktop und nicht für andere Computer gelten.
- Aktivieren Sie die Sitzungsaufzeichnung für die Anwendung. Aktivieren Sie auch weitere Verfahren zur Sicherheitsprotokollierung in der Anwendung und in Windows selbst.
- Beschränken Sie in XenApp und XenDesktop die Nutzung bestimmter Features (z. B. Zwischenablage, Drucker, Clientlaufwerk und USB-Umleitung) mit dieser Anwendung.
- Aktivieren Sie alle Sicherheitsfunktionen der Anwendung. Beschränken Sie die Verwendung nur auf die speziellen Anforderungen der Benutzer.
- Konfigurieren Sie die Sicherheitsfunktionen von Windows so, dass sie den Benutzeranforderungen genau entsprechen. Diese Konfiguration ist einfacher, wenn nur diese einzelne Anwendung auf dem Desktop veröffentlicht wird. Beispielsweise kann eine restriktive AppLocker-Konfiguration verwendet werden. Kontrollieren Sie den Zugriff auf das Dateisystem.
- Überlegen Sie, ob Sie die Anwendung neu konfigurieren, aktualisieren oder austauschen können, damit Desktopprivilegien in Zukunft nicht mehr erforderlich sind.

Durch diese Maßnahmen werden nicht alle Sicherheitsrisiken ausgeräumt, die für Anwendungen mit

erforderlichen Desktopprivilegien gelten.

Verwalten von Anmelderechten

Anmelderechte sind für Benutzerkonten und Computerkonten erforderlich. Wie Microsoft Windows-Privilegien werden Anmelderechte weiterhin in der üblichen Weise auf Desktops angewendet: Konfigurieren Sie Anmelderechte mit "Zuweisung von Benutzerrechten"und Gruppenmitgliedschaften mit einer Gruppenrichtlinie.

Es gibt folgende Windows-Anmelderechte: Lokal anmelden, Anmelden über Remotedesktopdienste, über das Netzwerk ("Auf diesen Computer vom Netzwerk aus zugreifen"), Anmelden als Stapelverarbeitungsauftrag und Anmelden als Dienst.

Erteilen Sie Computerkonten nur die Anmelderechte, die diese benötigen. Die Berechtigung "Auf diesen Computer vom Netzwerk aus zugreifen"ist erforderlich:

- Auf VDAs für die Computerkonten der Delivery Controller
- Auf Delivery Controllern für die Computerkonten der VDAs. Siehe hierzu den Artikel Auf Organisationseinheiten von Active Directory-basierte Controller-Discovery.
- Auf StoreFront-Servern für die Computerkonten der anderen Server in der gleichen StoreFront-Servergruppe

Erteilen Sie Benutzerkonten nur die Anmelderechte, die diese benötigen.

Laut Microsoft wird der Gruppe Remotedesktopbenutzer standardmäßig das Anmelderecht "Anmelden über Remotedesktopdienste"gewährt (außer für Domänencontroller).

Die Sicherheitsrichtlinie Ihres Unternehmens legt möglicherweise explizit fest, dass diese Gruppe aus dem Anmelderecht entfernt werden sollte. Erwägen Sie folgenden Ansatz:

- Der Virtual Delivery Agent (VDA) für Serverbetriebssysteme verwendet Microsoft-Remotedesktopdienste. Sie können die Gruppe der Remotedesktopbenutzer als eine eingeschränkte Gruppe konfigurieren und die Gruppenmitgliedschaft durch Active Directory-Gruppenrichtlinien steuern. Weitere Informationen finden Sie in der Dokumentation von Microsoft.
- Für andere XenApp- und XenDesktop-Komponenten, einschließlich dem VDA für Desktopbetriebssysteme, ist die Gruppe der Remotedesktopbenutzer nicht erforderlich. Für diese Komponenten benötigt die Gruppe der Remotedesktopbenutzer das Recht "Anmelden über Remotedesktopdienste"also nicht und Sie können es entfernen. Beachten Sie außerdem Folgendes:
  - Wenn Sie diese Computer mit Remotedesktopdienste verwalten, stellen Sie sicher, dass alle Administratoren Mitglieder der Administratorgruppe sind.
  - Wenn Sie diese Computer nicht mit Remotedesktopdienste verwalten, könnten Sie Remotedesktopdienste auf diesen Computern deaktivieren.

Es ist zwar möglich, dem Anmelderecht "Anmelden über Remotedesktopdienste verweigern"Benutzer und Gruppen hinzuzufügen, jedoch wird von der Verwendung von verweigernden Rechten allgemein abgeraten. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Konfigurieren von Benutzerrechten

Bei der Installation des Delivery Controllers werden die folgenden Windows-Dienste erstellt:

- Citrix AD-Identitätsdienst (NT SERVICE\CitrixADIdentityService): Verwaltet Microsoft Active Directory-Computerkonten für VMs.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Sammelt Sitekonfigurations- und Nutzungsinformationen zur Verwendung von Citrix, wenn das Sammeln vom Siteadministrator genehmigt wurde. Diese Informationen werden dann an Citrix gesendet, damit das Produkt verbessert werden kann.
- Citrix App-Bibliothek (NT SERVICE\CitrixAppLibrary): Unterstützt die Verwaltung und das Provisioning von AppDisks, AppDNA-Integration und die Verwaltung von App-V.
- Citrix Brokerdienst (NT SERVICE\CitrixBrokerService): Wählt die virtuellen Desktops oder Anwendungen aus, die den Benutzern zur Verfügung stehen.
- Citrix Konfigurationsprotokollierungsdienst (NT SERVICE\CitrixConfigurationLogging): Erfasst alle Konfigurationsänderungen und andere Zustandsänderungen, die von den Administratoren an der Site vorgenommen werden.
- Citrix Konfigurationsdienst (NT SERVICE\CitrixConfigurationService): Repository der Site für freigegebene Konfigurationen.
- Citrix Dienst für die delegierte Administration (NT SERVICE\CitrixDelegatedAdmin): Verwaltet die Berechtigungen, die Administratoren gewährt werden.
- Citrix Umgebungstestdienst (NT SERVICE\CitrixEnvTest): Verwaltet Selbsttests der anderen Delivery Controller-Dienste.
- Citrix Hostdienst (NT SERVICE\CitrixHostService): Speichert Informationen zu den Hypervisorinfrastrukturen, die in einer XenApp- oder XenDesktop-Bereitstellung verwendet werden, und bietet der Konsole die Funktionalität zum Enumerieren von Ressourcen in einem Hypervisorpool.
- Citrix Maschinenerstellungsdienste (NT SERVICE\CitrixMachineCreationService): Orchestriert das Erstellen von Desktop-VMs.
- Citrix Überwachungsdienst (NT SERVICE\CitrixMonitor): Sammelt Metrik für XenApp oder XenDesktop, speichert historische Informationen und bietet eine Abfrageschnittstelle für Problembehandlungs- und Berichterstattungstools.
- Citrix StoreFront-Dienst (NT SERVICE\CitrixStorefront): Unterstützt die Verwaltung von StoreFront. (Der Dienst selbst gehört nicht zur StoreFront-Komponente.)
- Citrix StoreFront-Dienst für die privilegierte Administration (NT SERVICE\CitrixPrivilegedService): Unterstützt privilegierte Verwaltungsvorgänge von StoreFront. (Der Dienst selbst gehört nicht

zur StoreFront-Komponente.)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): überträgt Konfigurationsdaten aus der Hauptsitedatenbank an den lokalen Hostcache.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): wählt den virtuellen Desktop bzw. die Anwendungen, die Benutzern zur Verfügung stehen, wenn die Sitedatenbank nicht zur Verfügung steht.

Bei der Installation des Delivery Controllers werden zudem die folgenden Windows-Dienste erstellt: Diese werden auch erstellt, wenn sie mit anderen Citrix Komponenten installiert werden:

- Citrix Diagnostic Facility COM-Server (NT SERVICE\CdfSvc): Unterstützt das Sammeln von Diagnoseinformationen für den Citrix Support.
- Citrix Telemetriedienst (NT SERVICE\CitrixTelemetryService): Sammelt Diagnoseinformationen zur Analyse durch Citrix. Die Analyseergebnisse und Empfehlungen können von Administratoren angezeigt werden, um die Diagnose von Problemen mit der Site zu erleichtern.

Bei der Installation des Delivery Controllers wird zudem der folgende Windows-Dienst erstellt. Dieser wird derzeit nicht verwendet. Wenn er aktiviert wurde, deaktivieren Sie ihn.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

Bei der Installation des Delivery Controllers werden zudem die folgenden Windows-Dienste erstellt. Diese werden zurzeit nicht verwendet, müssen aber aktiviert sein. Deaktivieren Sie sie nicht.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

Abgesehen vom Citrix StoreFront-Dienst für die privilegierte Administration werden diesen Diensten die Anmeldeberechtigung "Anmelden als Dienst"und die Privilegien "Anpassen von Speicherkontingenten für einen Prozess", "Generieren von Sicherheitsüberwachungen"und "Ersetzen eines Tokens auf Prozessebene"zugewiesen. Sie brauchen die Benutzerrechte nicht zu ändern. Diese Privilegien werden vom Delivery Controller nicht verwendet und werden automatisch deaktiviert.

Konfigurieren von Diensteinstellungen

Mit Ausnahme des Citrix StoreFront-Diensts für die privilegierte Administration und des Citrix Telemetriediensts werden die oben im Abschnitt Konfigurieren von Benutzerrechten aufgeführten Windows-Dienste des Delivery Controllers als NETWORK SERVICE angemeldet. Ändern Sie diese Diensteinstellungen nicht.

Der Citrix StoreFront-Dienst für die privilegierte Administration meldet sich als lokales System an (NT AUTHORITY\SYSTEM). Dies ist für StoreFront-Vorgänge des Delivery Controllers erforderlich, die normalerweise nicht für Dienste verfügbar sind (einschließlich Erstellen von Microsoft IIS-Sites). Ändern Sie die Diensteinstellungen nicht.

Der Citrix Telemetriedienst meldet sich als seine eigene dienstspezifische Identität an.

Sie können den Citrix Telemetriedienst deaktivieren. Abgesehen von diesem Dienst und Diensten, die bereits deaktiviert sind, deaktivieren Sie keine der anderen Windows-Dienste für Delivery Controller.

Konfigurieren von Registrierungseinstellungen

Es ist nicht mehr erforderlich, die Erstellung von 8.3-Dateinamen und -Ordnern auf dem VDA-Dateisystem zu aktivieren. Der Registrierungsschlüssel **NtfsDisable8dot3NameCreation** kann zum Deaktivieren der Erstellung von 8.3-Dateinamen und -Ordnern konfiguriert werden. Sie können diese Funktion auch mit dem Befehl **fsutil.exe behavior set disable8dot3** konfigurieren.

Auswirkungen von Bereitstellungsszenarios auf die Sicherheit

Ihre Benutzerumgebung kann Benutzergeräte enthalten, die von Ihrer Organisation nicht verwaltet werden und dem Vollzugriff der jeweiligen Benutzer unterliegen oder solche, die von Ihrer Organisation verwaltet werden. Die Sicherheitsüberlegungen für diese beiden Umgebungen sind generell unterschiedlich.

Verwaltete Benutzergeräte

Verwaltete Benutzergeräte unterliegen einer administrativen Steuerung. Sie werden entweder von Ihnen gesteuert oder von einer anderen Organisation, der Sie vertrauen. Sie können Benutzergeräte konfigurieren und Benutzern direkt bereitstellen. Alternativ können Sie Terminals bereitstellen, auf denen ein einzelner Desktop im Vollbildmodus ausgeführt wird. Befolgen Sie die oben beschriebenen Sicherheitsanweisungen bei allen verwalteten Benutzergeräten. Dieses Release bietet den Vorteil, dass nur ganz wenig Software auf einem Benutzergerät erforderlich ist.

Ein verwaltetes Benutzergerät kann für die Verwendung im Vollbildmodus oder im Fenstermodus konfiguriert werden.

- Im Vollbildmodus können Benutzer sich über den normalen Anmeldebildschirm für Windows anmelden. Dieselben Anmeldeinformationen des Benutzers werden dann zum automatischen Anmelden für dieses Release verwendet.
- Im Fenstermodus melden sich die Benutzer zunächst beim Benutzergerät an. Anschließend melden sie sich über die in diesem Release bereitgestellte Website bei diesem Release an.

Nicht verwaltete Benutzergeräte

Wenn Benutzergeräte nicht von einer vertrauenswürdigen Organisation verwaltet werden, kann nicht von einer administrativen Steuerung ausgegangen werden. Beispiel: Sie erlauben Benutzern, sich ihre eigenen Geräte zu besorgen und sie zu konfigurieren, doch die Benutzer halten sich u. U. nicht an die oben beschriebenen generellen optimalen Sicherheitsverfahren. Dieses Release hat den Vorteil, nicht verwalteten Benutzergeräten Desktops sicher bereitstellen zu können. Diese Geräte sollten jedoch einen grundlegenden Antivirenschutz haben, um Keylogger und ähnliche Angriffe auf Benutzereingaben abzuwehren.

Überlegungen zum Datenspeicher

Mit diesem Release können Sie verhindern, dass Benutzer Daten auf Benutzergeräten speichern, die sie selbst physisch steuern können. Sie müssen dennoch bedenken, welche Auswirkungen es haben kann, wenn Benutzer Daten auf Desktops speichern. Im Allgemeinen sollten Benutzer keine Daten auf Desktops speichern. Daten sollten an einem Ort gespeichert werden, an dem sie entsprechend geschützt werden können, wie z. B. auf Dateiservern, Datenbankservern oder in anderen Repositorys.

Möglicherweise enthält Ihre Desktopumgebung verschiedene Desktoptypen, wie gepoolte und dedizierte Desktops. Benutzer sollten zu keiner Zeit Daten auf Desktops speichern, die für andere Benutzer freigegeben sind, wie z. B. gepoolte Desktops. Wenn Benutzer Daten auf dedizierten Desktops speichern, sollten diese Daten entfernt werden, wenn der Desktop zu einem späteren Zeitpunkt anderen Benutzern zugänglich gemacht wird.

Umgebungen mit mehreren Versionen

Umgebungen mit mehreren Versionen sind während einiger Upgrades unvermeidbar. Folgen Sie bewährten Methoden und minimieren Sie die Zeitdauer, während der unterschiedliche Versionen von Citrix Komponenten koexistieren. In Umgebungen mit mehreren Versionen wird beispielsweise die Sicherheitsrichtlinie nicht gleichförmig durchgesetzt.

Hinweis: Dies ist typisch für andere Softwareprodukte. Bei Verwendung einer älteren Version von Active Directory wird die Gruppenrichtlinie bei neueren Windows-Versionen nur teilweise durchgesetzt.

Nachfolgend wird eine spezifische Citrix Umgebung mit mehreren Versionen beschrieben, bei der ein Sicherheitsproblem auftreten kann. Wenn Citrix Receiver 1.7 zum Herstellen einer Verbindung mit einem virtuellen Desktop verwendet wird, auf dem der Virtual Delivery Agent in XenApp und XenDesktop 7.6 Feature Pack 2 ausgeführt wird, ist die Richtlinieneinstellung **Dateiübertragungen zwischen Desktop und Client zulassen** für die Site aktiviert, kann jedoch nicht von einem Delivery Controller

deaktiviert werden, auf dem XenApp und XenDesktop 7.1 ausgeführt wird. Die Richtlinieneinstellung, die erst in der neueren Version des Produkts hinzugefügt wurde, wird nicht erkannt. Die Richtlinieneinstellung ermöglicht Benutzern das Hochladen und Herunterladen von Dateien zum/vom virtuellen Desktop und repräsentiert damit ein Sicherheitsproblem. Zur Problemumgehung aktualisieren Sie den Delivery Controller bzw. die eigenständige Instanz von Studio auf Version 7.6 Feature Pack 2 und deaktivieren Sie die Richtlinieneinstellung dann mit der Gruppenrichtlinie. Alternativ verwenden Sie die lokale Richtlinie auf allen betroffenen virtuellen Desktops.

Sicherheitsüberlegungen für Remote-PC-Zugriff

Mit Remote-PC-Zugriff werden die folgenden Sicherheitsfeatures implementiert:

- Die Verwendung von Smartcards wird unterstützt.
- Bei Verbindung einer Remotesitzung wird der Monitor des Büro-PCs leer angezeigt.
- Remote-PC-Zugriff leitet alle Tastatur- und Mauseingaben in die Remotesitzung um, ausgenommen Strg + Alt + Entf, USB-aktivierte Smartcards und biometrische Geräte.
- SmoothRoaming wird nur für einen einzelnen Benutzer unterstützt.
- Wenn ein Benutzer über eine Remotesitzung mit einem Büro-PC verbunden ist, kann nur dieser Benutzer den lokalen Zugriff auf den Büro-PC wiederaufnehmen. Zum Wiederaufnehmen des lokalen Zugriffs muss der Benutzer Strg-Alt-Entf auf dem lokalen PC drücken und sich dann mit denselben Anmeldeinformationen wie für die Remotesitzung anmelden. Er kann zudem auch über eine Smartcard oder biometrische Geräte wieder lokal zugreifen, wenn das System die entsprechende Anmeldeinformationsanbieter-Integration besitzt. Das Standardverhalten kann über die schnelle Benutzerumschaltung über Gruppenrichtlinienobjekte oder durch Bearbeiten der Registrierung außer Kraft gesetzt werden.

Hinweis: Citrix empfiehlt, dass Sie VDA-Administratorrechte nicht allgemeinen Sitzungsbenutzern zuweisen.

Automatische Zuweisungen

Standardmäßig unterstützt Remote-PC-Zugriff die automatische Zuweisung von mehreren Benutzern zu einem VDA. Unter XenDesktop 5.6 Feature Pack 1 konnten Administratoren dieses Verhalten mit dem PowerShell-Skript RemotePCAccess.ps1 außer Kraft setzen. Dieses Release verwendet einen Registrierungseintrag, mit dem mehrere automatische Remote-PC-Zuweisungen zugelassen oder abgelehnt werden; diese Einstellung gilt für die gesamte Site.

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht

daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Beschränken der automatischen Zuweisung auf einen einzelnen Benutzer:

Legen Sie auf jedem Controller in der Site den folgenden Registrierungsschlüssel fest:

```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG\_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
   multiple user assignment.
```

Liegen bereits Benutzerzuweisungen vor, entfernen Sie diese mit SDK-Befehlen, damit der VDA anschließend für eine einzelne automatische Zuweisung zur Verfügung steht.

- Entfernen Sie alle zugewiesenen Benutzer aus dem VDA:

```
$machine.AssociatedUserNames | %{
 Remove-BrokerUser-Name $_ -Machine $machine
```

- Entfernen Sie den VDA aus der Bereitstellungsgruppe:

```
$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup
```

Starten Sie den physischen Büro-PC neu.

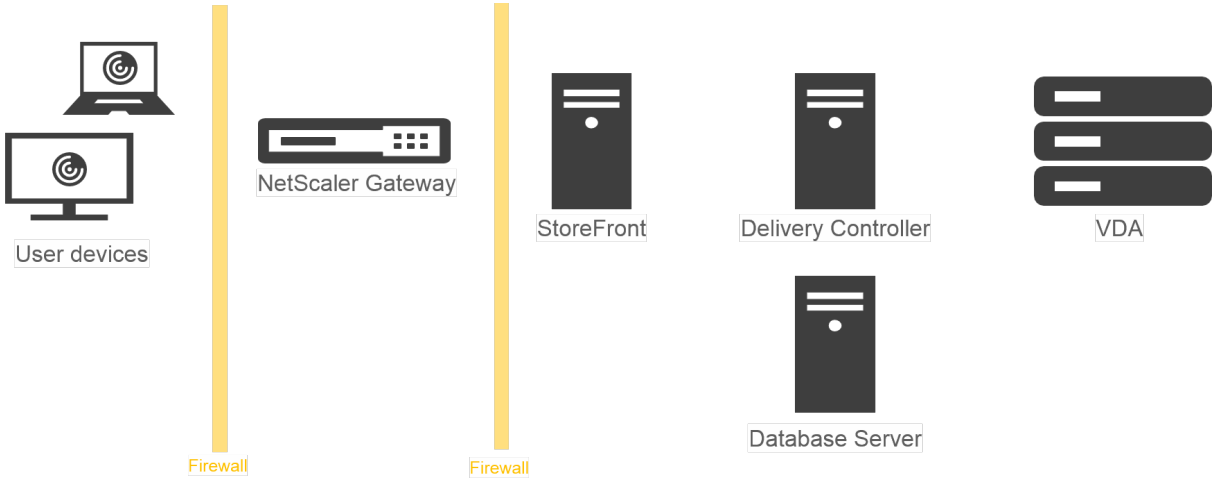
Integrieren von NetScaler Gateway in XenApp und XenDesktop

November 15, 2022

StoreFront-Server werden für die Zugriffsverwaltung auf veröffentlichte Ressourcen und Daten bereitgestellt und konfiguriert. Für den Remotezugriff wird das Hinzufügen von NetScaler Gateway vor StoreFront empfohlen.

> **Hinweis:**
>
> Detaillierte Konfigurationsschritte zur Integration von NetScaler Gateway in XenApp und XenDesktop finden Sie in der StoreFront-Dokumentation.

Die folgende Abbildung zeigt ein Beispiel für eine vereinfachte Citrix Bereitstellung mit NetScaler Gateway. NetScaler Gateway kommuniziert mit StoreFront zum Schutz von Apps und Daten, die mit XenApp und XenDesktop bereitgestellt werden. Die Benutzergeräte führen zum Herstellen einer sicheren Verbindung für den Zugriff auf Apps, Desktops und Dateien Citrix Receiver aus.



Die Anmeldung und Authentifizierung von Benutzern erfolgt über NetScaler Gateway. NetScaler Gateway ist in der DMZ bereitgestellt und geschützt. Die zweistufige Authentifizierung ist konfiguriert. Anhand der Benutzeranmeldeinformationen werden Benutzern die relevanten Ressourcen und Anwendungen bereitgestellt. Die Anwendungen und Daten sind auf geeigneten Servern (nicht abgebildet). Separate Server werden für sicherheitskritische Anwendungen und Daten verwendet.

Delegierte Administration

August 18, 2021

Das Modell der delegierten Administration bietet Flexibilität bei der Delegierung der Administratoraktivitäten mit Rollen und der objektbasierten Steuerung. Die delegierte Administration ist für Bereitstellungen aller Größen geeignet und ermöglicht es Ihnen, mit zunehmender Komplexität der Bereitstellung die Berechtigungsgranularität zu erhöhen. Bei der delegierten Administration werden drei Konzepte eingesetzt: Administratoren, Rollen und Geltungsbereiche.

- **Administratoren** - Ein Administrator ist eine Einzelperson oder eine Gruppe von Personen, die durch ein Active Directory-Konto identifiziert werden. Jeder Administrator ist mit mindestens einem Paar aus Rolle und Geltungsbereich verknüpft.
- **Rollen** - Eine Rolle steht für eine spezielle Jobfunktion, mit der definierte Berechtigungen verknüpft sind. Beispiel: Die Rolle “Bereitstellungsgruppenadministrator”verfügt über Berechtigungen wie etwa “Bereitstellungsgruppe erstellen”und “Desktop aus Bereitstellungsgruppe entfernen”. Ein Administrator kann mehrere Rollen für eine Site haben, d. h. eine Person kann sowohl Bereitstellungsgruppenadministrator als auch Maschinenkatalogadministrator sein. Rollen können integriert oder benutzerdefiniert sein.

  Integrierte Rollen:

Rolle	Berechtigungen
Volladministrator	Kann alle Aufgaben und Vorgänge ausführen. Ein Volladministrator wird immer mit dem Geltungsbereich “Alle”kombiniert.
Lesezugriffadministrator	Kann alle Objekte in den angegebenen Geltungsbereichen sowie globale Informationen anzeigen, aber nicht ändern. Beispiel: Ein Lesezugriffadministrator mit Geltungsbereich = London kann alle globalen Objekte (z. B. Konfigurationsprotokollierung) und alle London-bezogenen Geltungsbereichsobjekte (z. B. London-Bereitstellungsgruppen) sehen. Dieser Administrator kann jedoch nicht die Objekte im Geltungsbereich “New York”sehen (sofern die Geltungsbereiche “London”und “New York”einander nicht überlappen).
Helpdeskadministrator	Kann Bereitstellungsgruppen anzeigen und die diesen Gruppen zugeordneten Sitzungen und Maschinen verwalten. Kann den Maschinenkatalog und die Hostinformationen der überwachten Bereitstellungsgruppen sehen sowie Sitzungsverwaltungs- und Energieverwaltungsvorgänge für die Maschinen in diesen Bereitstellungsgruppen durchführen.
Maschinenkatalogadministrator	Kann Maschinenkataloge erstellen und verwalten sowie darin Maschinen bereitstellen. Kann Maschinenkataloge aus der Virtualisierungsinfrastruktur, Provisioning Services und von physischen Maschinen anlegen. Mit dieser Rolle können Basisimages verwaltet und Software installiert werden, aber den Benutzern können keine Anwendungen oder Desktops zugewiesen werden.
Bereitstellungsgruppenadministrator	Kann Anwendungen, Desktops und Maschinen bereitstellen sowie die mit ihnen verbundenen Sitzungen verwalten. Kann zudem Anwendungs- und Desktopkonfigurationen wie Richtlinien und die Energieverwaltungseinstellungen verwalten.

Rolle	Berechtigungen
Hostadministrator	Kann Hostverbindungen und ihnen zugeordnete Ressourceneinstellungen verwalten. Kann keine Maschinen, Anwendungen oder Desktops für Benutzer bereitstellen.

Bei bestimmten Produkteditionen können Sie benutzerdefinierte Rollen erstellen, um sie den Anforderungen Ihrer Organisation anzupassen und die Berechtigungen entsprechend delegieren. Sie können benutzerdefinierte Rollen dazu verwenden, Berechtigungen in der Granularität einer Aktion oder Aufgabe in einer Konsole zuzuteilen.

- **Geltungsbereiche**: Ein Geltungsbereich steht für eine Sammlung von Objekten. Geltungsbereiche werden verwendet, um die Objekte in einer für Ihre Organisation angemessenen Weise zu gruppieren (z. B. die Bereitstellungsgruppen der Vertriebsabteilung). Objekte können in mehreren Geltungsbereichen vertreten sein, d. h. Objekte können durch einen oder mehrere Geltungsbereiche bezeichnet sein. Der einzige integrierte Geltungsbereich "Alle"enthält alle Objekte. Die Volladministratorrolle bildet immer ein Paar mit dem Geltungsbereich "Alle".

Beispiel

Firma XYZ entscheidet sich zum Verwalten von Anwendungen und Desktops basierend auf ihrer Abteilungsstruktur (Buchhaltung, Vertrieb und Lager) und ihren Desktopbetriebssystemen (Windows 7 oder Windows 8). Der Administrator erstellt fünf Geltungsbereiche und erfasst jede Bereitstellungsgruppe in zwei Geltungsbereichen: einem Geltungsbereich für die Abteilung, in der sie verwendet werden und einem Geltungsbereich für das verwendete Betriebssystem.

Die folgenden Administratoren wurden erstellt:

Administrator	Rollen	Geltungsbereiche
domain/fred	Volladministrator	Alle (Volladministratorrolle wird immer mit "Alle" ausgestattet)
domain/rob	Lesezugriffadministrator	Alle
domain/heidi	Lesezugriffadministrator, Helpdeskadministrator	Vertrieb
domain/warehouseadmin	Helpdeskadministrator	Lager

Administrator	Rollen	Geltungsbereiche
domain/peter	Bereitstellungsgruppenadministrator, Maschinenkatalogadministrator	Win7

- Fred ist Volladministrator und kann alle Elemente im System anzeigen, bearbeiten und löschen.
- Rob kann alle Objekte der Site anzeigen jedoch nicht bearbeiten oder löschen.
- Heidi kann alle Objekte anzeigen und Helpdeskaufgaben an Bereitstellungsgruppen des Geltungsbereichs "Vertrieb" durchführen. Somit kann sie die diesen Gruppen zugeordneten Sitzungen und Maschinen verwalten; sie kann allerdings keine Änderungen an der Bereitstellungsgruppe durchführen, wie Hinzufügen oder Entfernen von Maschinen.
- Jedes Mitglied der Active Directory-Sicherheitsgruppe "warehouseadmin" kann Helpdeskaufgaben für Maschinen des Geltungsbereichs "Lager" ausführen.
- Peter ist Spezialist für Windows 7 und kann alle Windows 7-Maschinenkataloge verwalten und Windows 7-Anwendungen, -Desktops und -Maschinen bereitstellen, unabhängig davon, in welchem Abteilungsgeltungsbereich sie sich befinden. Der Administrator erwägt, Peter zum Volladministrator für den Geltungsbereich "Win7" zu machen; entscheidet sich jedoch dagegen, da ein Volladministrator ebenfalls über vollständige Administratorrechte für alle Objekte verfügt, die nicht in einen Geltungsbereich fallen, z. B. "Site" und "Administrator".

Verwenden der delegierten Administration

Im Allgemeinen hängt die Anzahl der Administratoren und die Granularität der Berechtigungen von der Größe und Komplexität der Bereitstellung ab.

- In kleinen Bereitstellungen oder Machbarkeitsstudien übernehmen ein oder wenige Administratoren alle Aufgaben und es findet keine Delegierung statt. Erstellen Sie in diesem Fall einen einzelnen Administrator mit der integrierten Rolle "Volladministrator", die den Geltungsbereich "Alle" hat.
- In größeren Bereitstellungen mit mehr Maschinen, Anwendungen und Desktops ist mehr Delegierung erforderlich. Mehrere Administratoren haben möglicherweise bestimmte funktionale Zuständigkeiten (Rollen). Beispiel: Es gibt zwei Volladministratoren, andere sind Helpdeskadministratoren. Weiterhin werden von einem Administrator ggf. nur bestimmte Objektgruppen (Geltungsbereiche) wie Maschinenkataloge verwaltet. Erstellen Sie in diesem Fall neue Geltungsbereiche und Administratoren mit einer der integrierten Rollen und den entsprechenden Geltungsbereichen.
- Noch größere Bereitstellungen erfordern möglicherweise weitere (oder differenziertere) Geltungsbereiche sowie andere Administratoren mit ungewöhnlichen Rollen. Bearbeiten oder erstellen Sie in diesem Fall weitere Geltungsbereiche, erstellen Sie benutzerdefinierte Rollen und

erstellen Sie jeden Administrator mit einer integrierten oder benutzerdefinierten Rolle sowie vorhandenen und neuen Geltungsbereichen.

Für mehr Flexibilität und zur Vereinfachung der Konfiguration können Sie neue Geltungsbereiche erstellen, wenn Sie einen Administrator erstellen. Sie können auch beim Erstellen oder Bearbeiten von Maschinenkatalogen oder Verbindungen Geltungsbereiche festlegen.

Erstellen und Verwalten von Administratoren

Beim Erstellen einer Site als lokaler Administrator wird dieses Benutzerkonto automatisch zum Volladministrator mit Vollzugriff auf alle Objekte. Nachdem die Site erstellt wurde, verfügen lokale Administratoren über keine besonderen Rechte.

Die Volladministratorrolle hat immer den Geltungsbereich "Alle"; dies kann nicht geändert werden.

Standardmäßig wird ein Administrator aktiviert. Beim Erstellen des neuen Administrators kann das Deaktivieren eines Administrators erforderlich sein, die betroffene Person übernimmt jedoch erst zu einem späteren Zeitpunkt Verwaltungsaufgaben. Bei vorhandenen aktivierten Administratoren kann es vorkommen, dass Sie einige deaktivieren müssen, während Sie Objekte/Geltungsbereiche neu strukturieren und sie dann wieder aktivieren, wenn Sie die Aktualisierung der Konfiguration abgeschlossen haben. Der Volladministrator kann nicht deaktiviert werden, wenn dies dazu führen würde, dass kein aktivierter Volladministrator mehr vorhanden ist. Das Kontrollkästchen zum Aktivieren/Deaktivieren steht zur Verfügung, wenn Sie einen Administrator erstellen, kopieren oder bearbeiten.

Wenn Sie ein Rollen-/Geltungsbereichspaar beim Kopieren, Bearbeiten oder Löschen eines Administrators löschen, wird nur die Beziehung zwischen Rolle und Geltungsbereich für diesen Administrator gelöscht, jedoch nicht die Rolle oder der Geltungsbereich selbst. Außerdem hat dies keine Auswirkungen auf andere Administratoren, die mit diesem Rollen-/Geltungsbereichspaar konfiguriert sind.

Klicken Sie zum Verwalten von Administratoren im Studio-Navigationsbereich auf "Konfiguration > Administratoren"und dann im mittleren Bereich oben auf die Registerkarte "Administratoren".

- Zum Erstellen eines Administrators klicken Sie im Aktionsbereich auf Administrator erstellen. Geben Sie den Namen eines Benutzerkontos ein oder navigieren zu einem Benutzerkonto, wählen oder erstellen Sie einen Geltungsbereich und wählen Sie eine Rolle. Der neue Administrator ist standardmäßig aktiviert. Sie können dies ändern.
- Zum Kopieren eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator kopieren. Geben Sie den Namen des Benutzerkontos ein oder navigieren zu dem Benutzerkonto. Sie können die Rollen-/Geltungsbereichspaare auswählen und dann bearbeiten oder löschen und neue hinzufügen. Der neue Administrator ist standardmäßig aktiviert. Sie können dies ändern.

- Zum Bearbeiten eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator bearbeiten. Sie können die Rollen-/Geltungsbereichspaare bearbeiten oder löschen und neue hinzufügen.
- Zum Löschen eines Administrators wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Administrator löschen. Der Volladministrator kann nicht gelöscht werden, wenn dies dazu führen würde, dass kein aktivierter Volladministrator mehr vorhanden ist.

Erstellen und Verwalten von Rollen

Rollennamen können bis zu 64 Unicode-Zeichen haben. Sie dürfen keines der folgenden Zeichen enthalten: umgekehrter Schrägstrich (\), Schrägstrich, Semikolon (;), Doppelpunkt (:), Nummernzeichen (#), Komma (,), Sternchen (*), Fragezeichen (?), Gleichheitszeichen (=), Größer-Als-Zeichen (>) oder Kleiner-Als-Zeichen (<), senkrechter Strich (|), eckige Klammern ([und]), runde Klammern ((und)), Anführungszeichen (“) und Apostroph (‘). Beschreibungen können bis zu 256 Unicode-Zeichen enthalten.

Sie können eine integrierte Rolle nicht bearbeiten oder löschen. Benutzerdefinierte Rollen können nicht gelöscht werden, wenn sie von einem Administrator verwendet werden.

Hinweis: Nur bestimmte Produkteditionen unterstützen benutzerdefinierte Rollen. Editionen, die keine benutzerdefinierten Rollen unterstützen, verfügen nicht über verwandte Einträge im Aktionsbereich.

Klicken Sie zum Verwalten von Rollen im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im oberen mittleren Bereich auf die Registerkarte Rollen.

- Zum Anzeigen von Rollendetails wählen Sie die Rolle im mittleren Bereich aus. Im unteren Teil des mittleren Bereichs werden die Objekttypen und die zugehörigen Berechtigungen für die Rolle angezeigt. Klicken Sie auf die Registerkarte Administratoren im unteren Bereich, um eine Liste der Administratoren anzuzeigen, die derzeit diese Rolle haben.
- Zum Erstellen einer benutzerdefinierten Rolle klicken Sie im Aktionsbereich auf Rolle erstellen. Geben Sie einen Namen und eine Beschreibung ein. Wählen Sie die Objekttypen und Berechtigungen aus.
- Zum Kopieren einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle kopieren. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Bearbeiten einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle bearbeiten. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Berechtigungen nach Bedarf.
- Zum Löschen einer Rolle wählen Sie diese im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Rolle löschen. Bestätigen Sie die Löschung.

Erstellen und Verwalten von Geltungsbereichen

Beim Erstellen einer Site steht nur der Geltungsbereich "Alle"zur Verfügung. Dieser kann nicht gelöscht werden.

Sie können Geltungsbereiche mit der unten aufgeführten Vorgehensweise erstellen. Sie können auch die Geltungsbereiche erstellen, wenn Sie einen Administrator erstellen. Jeder Administrator muss mindestens einem Rollen-/Geltungsbereichspaar zugeordnet werden. Beim Erstellen oder Bearbeiten von Desktops, Maschinenkatalogen, Anwendungen oder Hosts können Sie diese einem bestehenden Geltungsbereich hinzufügen. Wenn Sie sie keinem Geltungsbereich hinzufügen, bleiben sie Teil des Geltungsbereichs "Alle".

Die Geltungsbereichszuordnung ist beim Erstellen von Sites und für Objekte der delegierten Administration (Geltungsbereiche und Rollen) nicht möglich. Objekte, die nicht zugeordnet werden können, gehören zum Geltungsbereich "Alle". (Volladministratoren ist immer der Geltungsbereich "Alle"zugeordnet.) Maschinen, Energieaktionen, Desktops und Sitzungen werden nicht direkt einem Geltungsbereich zugeordnet. Administratoren können Berechtigungen für diese Objekte über die zugehörigen Maschinenkataloge oder Bereitstellungsgruppen zugewiesen werden.

Bereichsnamen können bis zu 64 Unicode-Zeichen haben. Sie dürfen keines der folgenden Zeichen enthalten: umgekehrter Schrägstrich (\), Schrägstrich, Semikolon (;), Doppelpunkt (:), Nummernzeichen (#), Komma (,), Sternchen (*), Fragezeichen (?), Gleichheitszeichen (=), Größer-Als-Zeichen (>) oder Kleiner-Als-Zeichen (<), senkrechter Strich (|), eckige Klammern ([und]), runde Klammern ((und)), Anführungszeichen (") und Apostroph (‘). Beschreibungen können bis zu 256 Unicode-Zeichen enthalten.

Wenn Sie einen Geltungsbereich kopieren oder bearbeiten, dürfen Sie nicht vergessen, dass Objekte, die aus dem Geltungsbereich entfernt werden, für den Administrator ggf. nicht mehr zugänglich sind. Ist der bearbeitete Geltungsbereich mit einer oder mehreren Rollen gepaart, stellen Sie sicher, dass durch Änderungen an dem Bereich kein Rollen-/Geltungsbereichspaar unbrauchbar wird.

Klicken Sie zum Verwalten von Geltungsbereichen im Studio-Navigationsbereich auf Konfiguration > Administratoren und dann im mittleren Bereich oben auf die Registerkarte Geltungsbereiche.

- Zum Erstellen eines Geltungsbereichs klicken Sie im Aktionsbereich auf Geltungsbereich erstellen. Geben Sie einen Namen und eine Beschreibung ein. Zum Einschließen aller Objekte eines bestimmten Typs (z. B. Bereitstellungsgruppen), wählen Sie den Objekttyp aus. Zum Einschließen bestimmter Objekte erweitern Sie den Typ und wählen Sie die einzelnen Objekte (z. B. einzelne Bereitstellungsgruppen des Vertriebs) aus.
- Zum Kopieren eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich kopieren. Geben Sie einen Namen und eine Beschreibung ein. Ändern Sie bei Bedarf die Objekttypen und Berechtigungen.
- Zum Bearbeiten eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken

Sie im Aktionsbereich auf Geltungsbereich bearbeiten. Ändern Sie den Namen und die Beschreibung sowie die Objekttypen und Objekte nach Bedarf.

- Zum Löschen eines Geltungsbereichs wählen Sie diesen im mittleren Bereich aus und klicken Sie im Aktionsbereich auf Geltungsbereich löschen. Bestätigen Sie die Löschung.

Erstellen von Berichten

Sie können zwei Arten delegierter Administrationsberichte erstellen:

- Einen HTML-Bericht, der die Rollen-/Geltungsbereichspaare, die einem Administrator zugeordnet sind, sowie die einzelnen Berechtigungen für jeden Objekttyp (z. B. Bereitstellungsgruppen, und Maschinenkataloge) enthält. Sie generieren diesen Bericht in Studio.

  Zum Erstellen dieses Berichts klicken Sie im Navigationsbereich auf Konfiguration > Administratoren. Wählen Sie im mittleren Bereich einen Administrator aus, und klicken Sie dann im Aktionsbereich auf Bericht erstellen.

  Sie können diesen Bericht auch beim Erstellen, Kopieren oder Bearbeiten eines Administrators anfordern.

- HTML- oder CSV Bericht, in dem alle integrierten benutzerdefinierten Rollen und Berechtigungen zugeordnet sind. Sie generieren diesen Bericht durch Ausführen des PowerShell-Skripts "OutputPermissionMapping.ps1".

  Um dieses Skript auszuführen, müssen Sie ein Volladministrator, ein Lesezugriffadministrator oder ein benutzerdefinierter Administrator mit der Berechtigung zum Lesen von Rollen sein. Das Skript befindet sich in: Programme\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Sc

  Syntax:

  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

Parameter	Beschreibung
-Help	Zeigt Skripthilfe an.
-Csv	Gibt CSV-Ausgabe an. Standard = HTML
-Path	Zielspeicherort für die Ausgabe. Standard = stdout
-AdminAddress	IP-Adresse oder Hostname des Delivery Controllers, mit dem eine Verbindung hergestellt wird. Standard = localhost

Parameter	Beschreibung
-Show	Gilt nur, wenn der Parameter “-Path”ebenfalls angegeben wird. Wenn die Ausgabe in eine Datei geschrieben wird, wird sie mit -Show in einem geeigneten Programm, z. B. einem Webbrowser, geöffnet. Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer und OutVariable. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Mit dem Befehl im folgenden Beispiel wird eine HTML-Tabelle in eine Datei namens Roles.html geschrieben und die Tabelle in einem Webbrowser geöffnet.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html  – Show
<!--NeedCopy-->
```

Mit dem Befehl im folgenden Beispiel wird eine CSV-Tabelle in eine Datei namens Roles.csv geschrieben. Die Tabelle wird nicht angezeigt.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
 – CSV -Path Roles.csv
<!--NeedCopy-->
```

An einer Windows-Eingabeaufforderung wird der Befehl aus dem vorherigen Beispiel folgendermaßen eingegeben:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
<!--NeedCopy-->
```

Smartcards

August 18, 2021

Smartcards und ähnliche Technologien werden im Rahmen der in diesem Abschnitt beschriebenen Richtlinien unterstützt. Für die Verwendung von Smartcards mit XenApp oder XenDesktop gelten folgende Richtlinien:

- Machen Sie sich mit den Sicherheitsrichtlinien Ihrer Organisation für die Verwendung von Smartcards vertraut. Mit diesen Richtlinien wird z. B. festgelegt, wie Smartcards ausgegeben werden und wie diese von Benutzern gesichert werden sollten. Einige Aspekte dieser Richtlinien müssen ggf. in einer XenApp und XenDesktop-Umgebung neu bewertet werden.
- Legen Sie fest, welche Benutzergerätetypen, Betriebssysteme und veröffentlichten Anwendungen mit Smartcards verwendet werden dürfen.
- Machen Sie sich mit der Smartcard-Technologie und der Hardware und Software des von Ihnen gewählten Smartcardanbieters vertraut.
- Sie sollten wissen, wie Sie digitale Zertifikate in einer verteilten Umgebung bereitstellen.

Smartcardtypen

Smartcards für Unternehmen und Kunden haben die gleiche Größe, elektrischen Verbindungen und passen in die gleichen Smartcardleser.

Smartcards für die Verwendung in Unternehmen enthalten digitale Zertifikate. Solche Smartcards unterstützen die Windows-Anmeldung und können auch in Kombination mit Anwendungen für die digitale Signierung und Verschlüsselung von Dokumenten und E-Mail verwendet werden. XenApp und XenDesktop unterstützt eine derartige Verwendung.

Smartcards für Kunden enthalten anstelle eines digitalen Zertifikats einen gemeinsamen geheimen Schlüssel. Mit solchen Smartcards ist ggf. eine Bezahlung möglich (z. B. Kreditkarte mit Chip und PIN/Unterschrift). Sie unterstützen keine Windows-Anmeldung oder typische Windows-Anwendungen. Zur Verwendung solcher Smartcards sind spezielle Windows-Anwendungen und eine geeignete Softwareinfrastruktur (z. B. eine Verbindung mit einem Zahlsystemnetzwerk) erforderlich. Informationen zur Unterstützung solcher Spezialanwendungen unter XenApp und XenDesktop erhalten Sie bei Ihrem Citrix Repräsentanten.

Für Unternehmenssmartcards gibt es entsprechende kompatible Technologien, die ähnlich funktionieren.

- Ein smartcardäquivalentes USB-Token stellt eine direkte Verbindung mit einem USB-Anschluss her. Diese USB-Token sind normalerweise so groß wie ein USB-Stick, aber sie können auch so klein wie die SIM-Karte eines Mobiltelefons sein. Sie sind eine Kombination aus einer Smartcard und einem USB-Smartcardleser.
- Virtuelle Smartcards mit Windows Trusted Platform Module (TPM) erscheinen als Smartcard. Solche virtuellen Smartcards werden für Windows 8 und Windows 10 unter Citrix Receiver ab Version 4.3 unterstützt.
  - XenApp und XenDesktop-Versionen vor Version 7.6 FP3 unterstützen keine virtuellen Smartcards.
  - Weitere Informationen finden Sie unter Virtual Smart Card Overview.

Hinweis: Der Begriff "virtuelle Smartcard"wird auch für ein digitales Zertifikat verwendet, das auf dem Computer des Benutzers gespeichert wird. Diese digitalen Zertifikate sind nicht unbedingt gleichbedeutend mit Smartcards.

Die Smartcard-Unterstützung in XenApp und XenDesktop basiert auf dem PC/SC-Standard (Personal Computer/Smart Card) von Microsoft. Als Mindestanforderung müssen Smartcards und Smartcardleser vom zugrunde liegenden Windows-Betriebssystem unterstützt werden und vom Microsoft Windows Hardware Quality Labs (WHQL) für die Verwendung auf Computern mit einem qualifizierenden Windows-Betriebssystem zugelassen sein. Weitere Informationen zur Hardware-PC/SC-Kompatibilität finden Sie in der Microsoft-Dokumentation. Weitere Benutzergeräte können PS/SC-konform sein. Weitere Informationen finden Sie im Citrix Ready-Programm unter https://www.citrix.com/ready/.

Normalerweise wird für jede Smartcard bzw. ähnliche Geräte ein eigener Gerätetreiber benötigt. Entsprechen Smartcards jedoch einem Standard wie NIST PIV (Personal Identity Verification), kann evtl. ein Treiber für mehrere Smartcardtypen verwendet werden. Der Gerätetreiber muss auf dem Benutzergerät und dem Virtual Delivery Agent installiert werden. Der Gerätetreiber ist häufig im Smartcard-Middlewarepaket eines Citrix Partners enthalten, welches zudem erweiterte Features bietet. Der Gerätetreiber wird u. U. auch als Kryptografiedienstanbieter (CSP), Schlüsselspeicheranbieter (KSP) oder Minitreiber bezeichnet.

Die folgenden Kombinationen aus Smartcard und Middleware für Windows-Systeme wurden von Citrix als repräsentatives Beispiel ihres Typs getestet. Es können jedoch auch andere Smartcards und Middleware verwendet werden. Weitere Informationen über Citrix-kompatible Smartcards und Middleware finden Sie unter https://www.citrix.com/ready.

Middleware	Geeignete Karten
ActivClient 7.0 (DoD-Modus aktiviert)	DoD CAC-Karte
ActivClient 7.0 im Modus PIV	NIST PIV-Karte
Microsoft-Minitreiber	NIST PIV-Karte
GemAlto Mini Driver for .NET-Karte	GemAlto .NET v2+
nativer Microsoft-Treiber	virtuelle Smartcards (TPM)

Informationen zur Verwendung von Smartcards mit anderen Gerätetypen finden Sie in der Citrix Receiver-Dokumentation für das jeweilige Gerät.

Informationen zur Verwendung von Smartcards mit anderen Gerätetypen finden Sie in der Citrix Receiver-Dokumentation für das jeweilige Gerät.

Remote-PC-Zugriff

Smartcards werden nur für den Remotezugriff auf physische Büro-PCs mit Windows 10, Windows 8 oder Windows 7 unterstützt; Smartcards werden nicht für Büro-PCs mit Windows XP unterstützt.

Die folgenden Smartcards wurden mit Remote-PC-Zugriff getestet:

Middleware	Geeignete Karten
Gemalto .NET-Minitreiber	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Microsoft-Minitreiber	NIST PIV
nativer Microsoft-Treiber	Virtuelle Smartcards

Smartcardleser

Ein Smartcardleser kann im Benutzergerät eingebaut sein oder an dieses angeschlossen werden (normalerweise über USB oder Bluetooth). Kontaktkartenleser, die dem USB-Protokoll CCID (Chip Card Interface Device) entsprechen, werden unterstützt. Diese enthalten einen Schlitz, in den die Smartcard eingeführt wird. In der DK-Norm (Deutsche Kreditwirtschaft) sind vier Kontaktkartenleserklassen festgelegt.

- Smartcardleser der Klasse 1 sind die häufigsten Geräte und haben normalerweise nur einen Steckplatz. Smartcardleser der Klasse 1 werden in der Regel durch einen CCID-Standardgerätetreiber unterstützt, der mit dem Betriebssystem geliefert wurde.
- Smartcardleser der Klasse 2 enthalten eine sichere Tastatur, auf die über das Benutzergerät nicht zugegriffen werden kann. Smartcardleser der Klasse 2 können in eine Tastatur mit integrierter sicherer Tastatur integriert werden. Wenn Sie Smartcardleser der Klasse 2 verwenden, wenden Sie sich an einen Citrix Mitarbeiter, da u. U. ein spezifischer Gerätetreiber erforderlich ist, damit die sichere Tastatur funktioniert.
- Smartcardleser der Klasse 3 haben ein sicheres Display. Smartcardleser der Klasse 3 werden nicht unterstützt.
- Smartcardleser der Klasse 4 haben ein sicheres Übertragungsmodul. Smartcardleser der Klasse 4 werden nicht unterstützt.

Hinweis: Die Klasse der Smartcardleser hat nichts mit der USB-Geräteklasse zu tun.

Smartcardleser müssen mit einem entsprechenden Gerätetreiber auf dem Benutzergerät installiert sein.

Informationen zu unterstützten Smartcardlesern finden Sie in der Dokumentation zu Ihrer Citrix Receiver-Version. Die unterstützten Versionen werden in der Dokumentation zu Citrix Receiver normalerweise in einem Smartcard-Artikel oder im Artikel zu den Systemanforderungen aufgeführt.

Benutzererfahrung

Smartcardunterstützung ist in XenApp und XenDesktop durch einen virtuellen ICA/HDX-Smartcardkanal integriert, der standardmäßig aktiviert ist.

Wichtig: Verwenden Sie für Smartcardleser keine generische USB-Umleitung. Diese ist für Smartcardleser standardmäßig deaktiviert und wird bei Aktivierung nicht unterstützt.

Mehrere Smartcards und mehrere Leser können an dem gleichen Benutzergerät verwendet werden, wenn jedoch Passthrough-Authentifizierung verwendet wird, kann nur eine Smartcard eingesteckt werden, wenn der Benutzer einen virtuellen Desktop oder eine virtuelle Anwendung startet. Wenn eine Smartcard innerhalb einer Anwendung verwendet wird (z. B. zur digitalen Signierung oder für Verschlüsselungsfunktionen), werden Sie möglicherweise mehrmals zum Einlegen einer Smartcard oder zur Eingabe einer PIN-Nummer aufgefordert. Dieser Fall kann eintreten, wenn eine oder mehrere Smartcards gleichzeitig eingelegt wurden.

- Wenn Benutzer zum Einlegen einer Smartcard aufgefordert werden und diese sich bereits im Leser befindet, sollten sie auf "Abbrechen"klicken.
- Wenn Benutzer zur Eingabe der PIN-Nummer aufgefordert werden, sollten sie diese erneut eingeben.

Wenn Sie gehostete Anwendungen unter Windows Server 2008 oder 2008 R2 und mit Smartcards verwenden, die den Microsoft-Kryptografiedienstanbieter für Basissmartcards benötigen, werden im Fall der Ausführung einer Smartcard-Transaktion alle anderen Benutzer, die eine Smartcard bei der Anmeldung verwendet haben, blockiert. Einzelheiten und einen Hotfix zur Behebung dieses Problems finden Sie unter https://support.microsoft.com/kb/949538.

Sie können PINs mit einem Kartenverwaltungsprogramm oder einem Herstellerdienstprogramm zurücksetzen.

> **Wichtig**
>
> In einer XenApp und XenDesktop-Sitzung wird die Verwendung einer Smartcard mit Microsoft Remotedesktopverbindung nicht unterstützt. Dies wird manchmal als "Double-Hop"bezeichnet.

Führen Sie vor dem Bereitstellen von Smartcards folgende Schritte aus

- Installieren Sie für den Smartcardleser einen Gerätetreiber auf dem Benutzergerät. Viele Smartcardleser können mit dem von Microsoft bereitgestellten CCID-Gerätetreiber benutzt werden.

- Beziehen Sie einen Gerätetreiber und Kryptografiedienstanbietersoftware (CSP) vom Smartcard-Hersteller und installieren Sie beides auf Benutzergeräten und auf virtuellen Desktops. Der Treiber und die CSP-Software müssen mit XenApp und XenDesktop kompatibel sein (Informationen zur Kompatibilität enthält die Dokumentation). Für virtuelle Desktops mit Smartcards, die das Minitreibermodell unterstützen und verwenden, werden die Smartcard-Minitreiber automatisch heruntergeladen. Die Treiber können auch über https://catalog.update.microsoft.com oder den Hersteller bezogen werden. Wird PKCS#11-Middleware benötigt, wenden Sie sich an den Smartcardhersteller.
- Wichtig: Citrix empfiehlt, dass Sie die Treiber und CSP-Software vor der Installation von Citrix Software auf einem physischen Computer installieren und testen.
- Fügen Sie die Citrix Receiver für Web-URL der Liste der vertrauenswürdigen Sites für Benutzer hinzu, die mit Smartcards im Internet Explorer unter Windows 10 arbeiten. In Windows 10 wird Internet Explorer für vertrauenswürdige Sites nicht standardmäßig im geschützten Modus ausgeführt.
- Stellen Sie sicher, dass die Public Key-Infrastruktur entsprechend konfiguriert ist. Hierzu gehört, dass die Zertifikat-zu-Konto-Zuordnung richtig für die Active Directory-Umgebung konfiguriert ist, und dass die Validierung des Benutzerzertifikats ausgeführt werden kann.
- Stellen Sie sicher, dass die Bereitstellung die Systemanforderungen der anderen Citrix Komponenten erfüllt, die mit Smartcards verwendet werden, u. a. Citrix Receiver und StoreFront.
- Stellen Sie sicher, dass auf die folgenden Server in der Site Zugriff besteht:
  - Active Directory-Domänencontroller für das Benutzerkonto mit zugeordnetem Anmeldezertifikat auf der Smartcard
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optional für Remotezugriff): Microsoft Exchange Server

Aktivieren der Smartcard-Verwendung

Schritt 1. Geben Sie die Smartcards an die Benutzer aus und berücksichtigen Sie dabei die Kartenausstellungsrichtlinie.

Schritt 2. Optional: Richten Sie Smartcards ein, damit die Benutzer Remote-PC-Zugriff verwenden können.

Schritt 3. Installieren Sie ggf. den Delivery Controller und StoreFront und konfigurieren Sie beides für Smartcard-Remoting.

Schritt 4. Aktivieren Sie StoreFront für die Verwendung von Smartcards. Einzelheiten finden Sie unter "Konfigurieren der Smartcardauthentifizierung"in der StoreFront-Dokumentation.

Step 5. Aktivieren Sie NetScaler Gateway/Access Gateway für die Verwendung von Smartcards. Einzelheiten finden Sie unter "Configuring Authentication and Authorization und Configuring Smart Card Access with the Web Interface"in der NetScaler-Dokumentation.

Schritt 6. Aktivieren Sie VDAs für die Verwendung mit Smartcard.

- Stellen Sie sicher, dass die erforderlichen Anwendungen und Updates auf dem VDA installiert wurden.
- Installieren Sie die Middleware.
- Richten Sie Smartcard-Remoting ein, damit die Kommunikation von Smartcarddaten zwischen Citrix Receiver auf einem Benutzergerät und einer virtuellen Desktopsitzung möglich ist.

Schritt 7. Aktivieren Sie Benutzergeräte (einschließlich der Maschinen innerhalb und außerhalb von Domänen) für die Verwendung von Smartcards. Einzelheiten finden Sie unter "Konfigurieren der Smartcardauthentifizierung"in der StoreFront-Dokumentation.

- Importieren Sie das Zertifizierungsstellen-Stammzertifikat und das Zertifikat der ausstellenden Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
- Installieren Sie die Smartcard-Middleware des Herstellers.
- Installieren und konfigurieren Sie Citrix Receiver für Windows. Importieren Sie icaclient.adm mit der Gruppenrichtlinien-Verwaltungskonsole und aktivieren Sie die Smartcardauthentifizierung.

Schritt 8. Testen Sie die Bereitstellung. Stellen Sie sicher, dass die Bereitstellung richtig konfiguriert ist, indem Sie den virtuellen Desktop mit der Smartcard eines Testbenutzers starten. Testen Sie alle möglichen Zugriffsmechanismen (beispielsweise Zugriff auf den Desktop über Internet Explorer und Citrix Receiver).

Smartcardbereitstellungen

November 29, 2018

Die folgenden Typen von Smartcardbereitstellungen werden von dieser Produktversion und von gemischten Umgebungen, die diese Version enthalten, unterstützt. Weitere Konfigurationen funktionieren eventuell, werden aber nicht unterstützt.

Typ	Verbindung mit StoreFront
Lokale in Domänen eingebundene Computer	Direkte Verbindung
Remotezugriff von in Domänen eingebundenen Computern	Verbindung über NetScaler Gateway

Typ	Verbindung mit StoreFront
Nicht in Domänen eingebundene Computer	Direkte Verbindung
Remotezugriff von nicht in Domänen eingebundenen Computern	Verbindung über NetScaler Gateway
Nicht in Domänen eingebundene Computer und Thin Clients mit Zugriff auf die Desktopgerätesite	Verbindung über Desktopgerätesites
In Domänen eingebundene Computer und Thin Clients mit Zugriff auf StoreFront über die XenApp Services-URL	Verbindung über XenApp Services-URLs

Die Bereitstellungstypen werden durch die Merkmale des Benutzergeräts definiert, mit dem der Smartcardleser verbunden ist:

- In Domäne eingebundenes Gerät oder nicht in Domäne eingebundenes Gerät
- Art der Verbindung zwischen Gerät und StoreFront
- Zur Anzeige der virtuellen Desktops und Anwendungen verwendete Software

Darüber hinaus können smartcardfähige Anwendungen wie Microsoft Word oder Microsoft Excel in diesen Bereitstellungen verwendet werden. In diesen Anwendungen können Benutzer Dokumente digital signieren und verschlüsseln.

Bimodale Authentifizierung

Soweit in der jeweiligen Bereitstellung möglich, unterstützt Receiver die bimodale Authentifizierung, d. h. der Benutzer hat die Wahl, sich mit einer Smartcard oder mit dem Benutzernamen und Kennwort anzumelden. Dies ist nützlich, wenn die Smartcard nicht verwendet werden kann (z. B. sie wurde vom Benutzer zu Hause vergessen oder das Zertifikat ist abgelaufen).

Da Benutzer nicht domänengebundener Geräte sich direkt an Receiver für Windows anmelden, können Sie für diese Benutzer ein Fallback auf die explizite Authentifizierung aktivieren. Wenn Sie die bimodale Authentifizierung konfigurieren, müssen sich Benutzer zuerst mit den Smartcards und PINs anmelden; sie können aber die explizite Authentifizierung auswählen, wenn sie Probleme mit den Smartcards haben.

Wenn Sie NetScaler Gateway bereitstellen, melden sich Benutzer an den Geräten an und werden von Receiver für Windows zur Authentifizierung bei NetScaler Gateway aufgefordert. Dies gilt sowohl für in Domänen eingebundene Geräte als auch für Geräte, die nicht in Domänen eingebunden sind. Benutzer können sich bei NetScaler Gateway mit Smartcard und PIN oder mit expliziten Anmeldeinformationen anmelden. Sie können dann Benutzern die bimodale Authentifizierung für Anmeldungen an NetScaler Gateway bereitstellen. Konfigurieren Sie die Passthrough-Authentifizierung

von NetScaler Gateway an StoreFront und delegieren Sie die Validierung der Anmeldeinformationen für Smartcardbenutzer an NetScaler Gateway, sodass Benutzer automatisch bei StoreFront authentifiziert werden.

Überlegungen zu mehreren Active Directory-Gesamtstrukturen

In einer Citrix Umgebung werden Smartcards in einer einzelnen Gesamtstruktur unterstützt. Strukturübergreifende Smartcard-Anmeldungen erfordern eine direkte bidirektionale Gesamtstruktur-Vertrauensstellung für alle Benutzerkonten. Komplexere Mehrfachstruktur-Bereitstellungen mit Smartcards (d. h. Vertrauensstellungen sind nur unidirektional oder sonstiger Art) werden nicht unterstützt.

Sie können Smartcards in einer Citrix Umgebung mit Remotedesktops verwenden. Dieses Feature kann lokal installiert werden (auf dem Benutzergerät, mit dem die Smartcard verbunden ist) oder remote (auf dem Remotedesktop, mit dem das Benutzergerät verbunden wird).

Richtlinie zum Entfernen der Smartcard

Die Richtlinie zum Entfernen der Smartcard legt fest, was passiert, wenn die Smartcard während einer Sitzung entfernt wird. Die Richtlinie zum Entfernen der Smartcard wird im Windows-Betriebssystem konfiguriert und verarbeitet.

Richtlinieneinstellung	Desktop-Verhalten
Keine Aktion	Keine Aktion.
Arbeitsstation sperren	Die Desktopsitzung wird getrennt und der virtuelle Desktop gesperrt.
Abmeldung erzwingen	Der Benutzer wird zur Abmeldung gezwungen. Wenn die Netzwerkverbindung unterbrochen ist und diese Einstellung aktiviert wird, wird die Sitzung möglicherweise abgemeldet und der Benutzer verliert Daten.
Trennen bei einer Remotedienstesitzung	Die Sitzung wird getrennt und der virtuelle Desktop gesperrt.

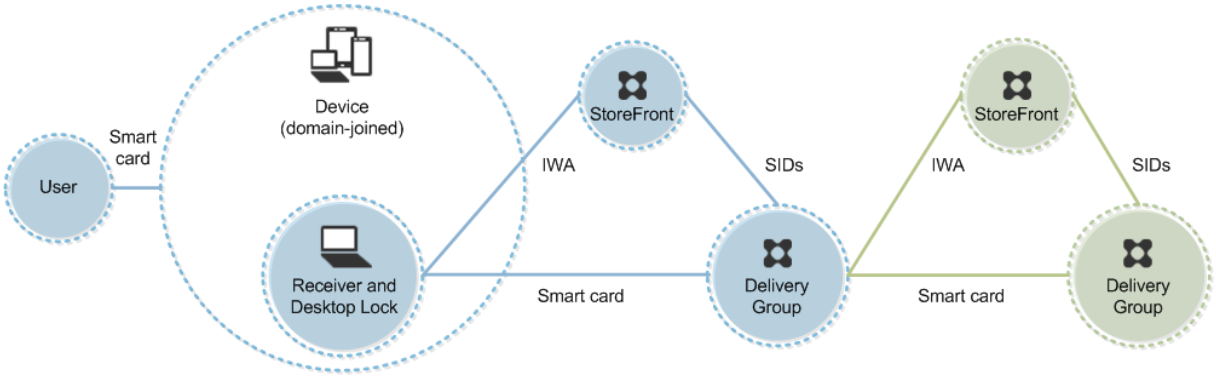
Überprüfen der Zertifikatsperrlisten

Wenn die Überprüfung von Zertifikatsperrlisten aktiviert ist und ein Benutzer führt eine Smartcard mit einem ungültigen Zertifikat in einen Smartcardleser ein, kann der Benutzer nicht authentifiziert werden oder nicht auf den mit dem Zertifikat verbundenen Desktop oder die Anwendung zugreifen. Bei

einem ungültigen Zertifikat für die E-Mail-Entschlüsselung bleibt die E-Mail beispielsweise verschlüsselt. Wenn andere Zertifikate auf der Smartcard, z. B. solche, die für die Authentifizierung verwendet werden, noch gültig sind, bleiben diese Funktionen weiterhin aktiv.

Bereitstellungsbeispiel: in Domänen eingebundene Computer

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.

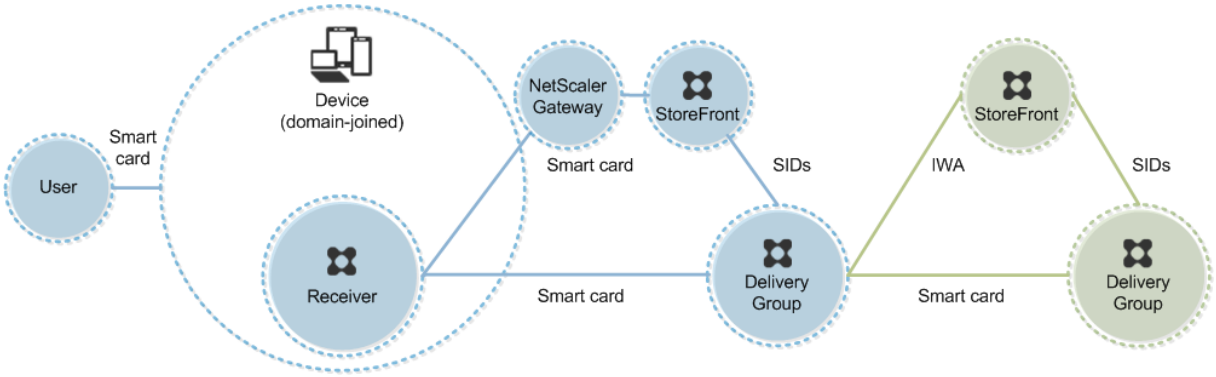


Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Der Benutzer wird dann durch Receiver beim Storefront-Server mittels integrierter Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver das Feature "Single Sign-On"konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: Remotezugriff von in Domänen eingebundenen Computern

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Verbindung mit StoreFront über NetScaler Gateway/Access Gateway.



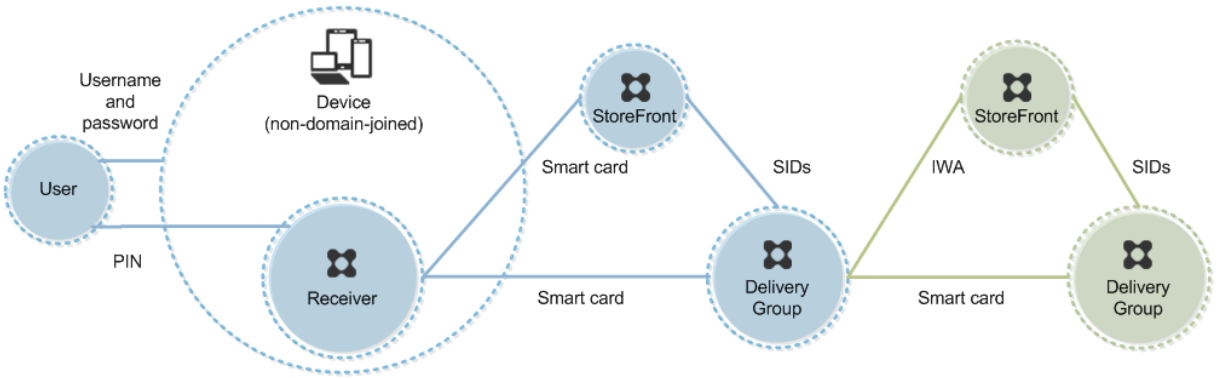
Der Benutzer meldet sich mit Smartcard und PIN beim Gerät und anschließend erneut bei NetScaler Gateway oder Access Gateway an. Die zweite Anmeldung kann entweder mit Smartcard und PIN oder einem Benutzernamen und einem Kennwort erfolgen, da Receiver in dieser Bereitstellung eine bimodale Authentifizierung zulässt.

Der Benutzer wird automatisch bei StoreFront angemeldet; StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver das Feature "Single Sign-On"konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: nicht in Domänen eingebundene Computer

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.



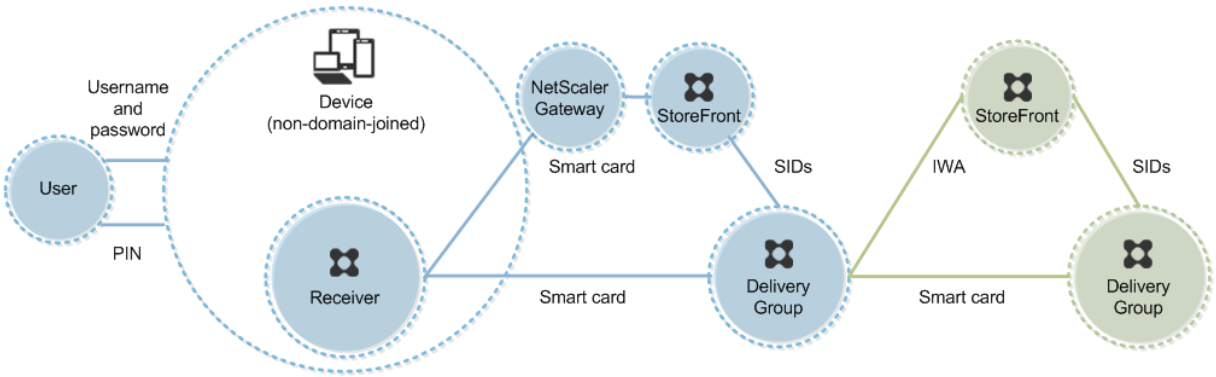
Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver den Benutzer auf, sich entweder mit Smartcard und PIN oder mit Benutzernamen und Kennwort anzumelden. Receiver authentifiziert dann bei StoreFront.

StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er aufgefordert, die PIN neu einzugeben, da Single Sign-On in dieser Bereitstellung nicht verfügbar ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: Remotezugriff von nicht in Domänen eingebundenen Computern

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte mit Desktop Viewer und Direktverbindung mit StoreFront.



Ein Benutzer meldet sich beim Gerät an. Normalerweise muss er seinen Benutzernamen und das Kennwort eingeben, aber da das Gerät nicht Mitglied einer Domäne ist, sind die Anmeldeinformationen für diese Anmeldung optional. Da bimodale Authentifizierung in dieser Bereitstellung möglich ist, fordert Receiver den Benutzer auf, sich entweder mit Smartcard und PIN oder mit Benutzernamen und Kennwort anzumelden. Receiver authentifiziert dann bei StoreFront.

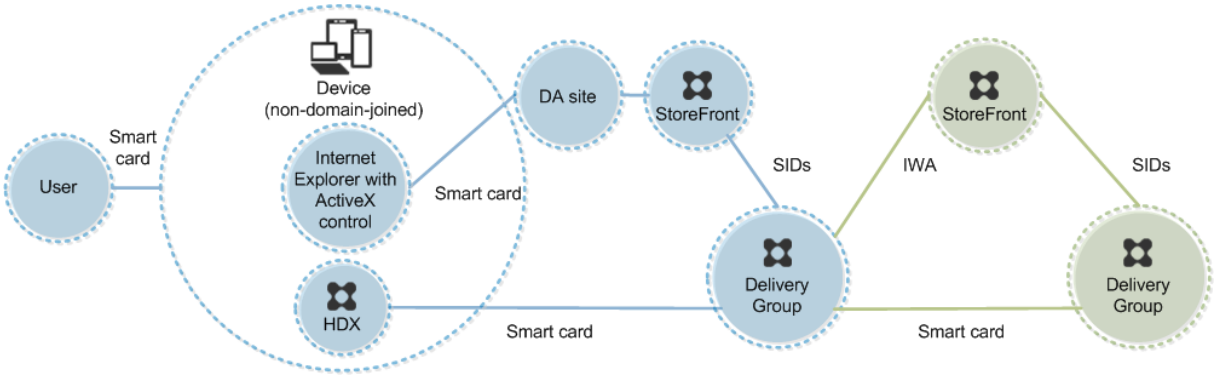
StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop oder eine Anwendung startet, wird er aufgefordert, die PIN neu einzugeben, da Single Sign-On in dieser Bereitstellung nicht verfügbar ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: nicht in Domänen eingebundene Computer und Thin Clients mit Zugriff auf die Desktopgerätesite

Diese Bereitstellung bezieht sich auf nicht in Domänen eingebundene Benutzergeräte, auf denen möglicherweise Desktop Lock ausgeführt wird und die mit StoreFront über Desktopgerätesites verbunden werden.

Desktop Lock ist eine eigenständige Komponente, die mit XenApp, XenDesktop und VDI-in-a-Box auf den Markt gebracht wurde. Das Programm ist eine Alternative zu Desktop Viewer und wird hauptsächlich für umfunktionierte Windows-Computer und Thin Clients verwendet. Desktop Lock ersetzt die Windows-Shell und Task-Manager bei diesen Benutzergeräten, wodurch der Benutzerzugriff auf die zugrunde liegenden Geräte verhindert wird. Mit Desktop Lock können Benutzer auf Desktops von Windows-Servermaschinen und Windows-Desktopmaschinen zugreifen. Die Installation von Desktop Lock ist optional.



Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard. Wenn Desktop Lock auf dem Gerät ausgeführt wird, wird das Gerät so konfiguriert, dass eine Desktopgerätesite über Internet Explorer im Kioskmodus gestartet wird. Der Benutzer wird durch ein ActiveX-Steuerelement der Site aufgefordert, seine PIN einzugeben, die dann an StoreFront gesendet wird. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Der erste verfügbare Desktop in der alphabetischen Liste einer zugewiesenen Desktopgruppe wird gestartet.

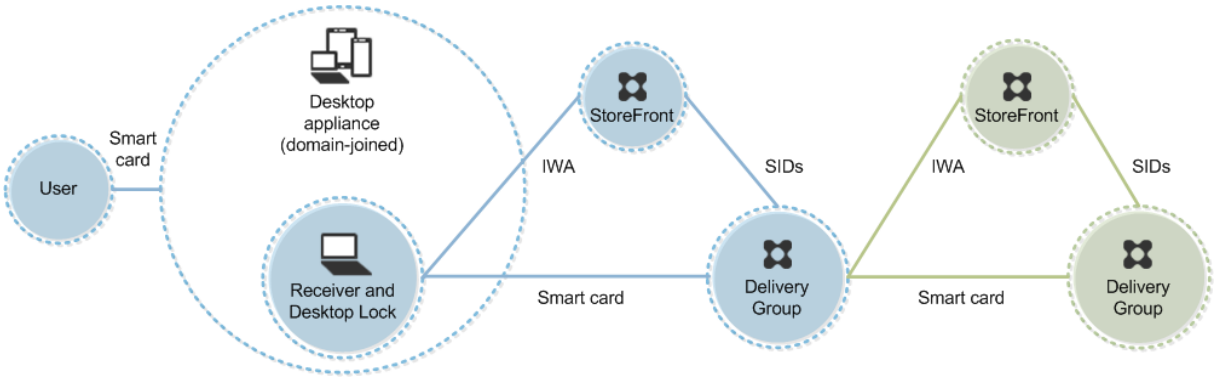
Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann

eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Bereitstellungsbeispiel: in Domänen eingebundene Computer und Thin Clients mit Zugriff auf StoreFront über die XenApp Services-URL

Diese Bereitstellung bezieht sich auf in Domänen eingebundene Benutzergeräte, auf denen Desktop Lock ausgeführt wird und die mit StoreFront über XenApp Services-URLs verbunden werden.

Desktop Lock ist eine eigenständige Komponente, die mit XenApp, XenDesktop und VDI-in-a-Box auf den Markt gebracht wurde. Das Programm ist eine Alternative zu Desktop Viewer und wird hauptsächlich für umfunktionierte Windows-Computer und Thin Clients verwendet. Desktop Lock ersetzt die Windows-Shell und Task-Manager bei diesen Benutzergeräten, wodurch der Benutzerzugriff auf die zugrunde liegenden Geräte verhindert wird. Mit Desktop Lock können Benutzer auf Desktops von Windows-Servermaschinen und Windows-Desktopmaschinen zugreifen. Die Installation von Desktop Lock ist optional.



Zum Anmelden beim Gerät benötigt der Benutzer eine Smartcard und eine PIN. Wenn Desktop Lock auf dem Gerät ausgeführt wird, wird der Benutzer beim Storefront-Server über die integrierte Windows-Authentifizierung (IWA) authentifiziert. StoreFront übergibt die Sicherheits-IDs (SIDs) an XenApp bzw. XenDesktop. Wenn der Benutzer einen virtuellen Desktop startet, wird er nicht aufgefordert, die PIN neu einzugeben, da in Receiver Single Sign-On konfiguriert ist.

Diese Bereitstellung kann um einen zweiten StoreFront-Server und einen Server mit gehosteten Anwendungen auf ein Double-Hop-System erweitert werden. Ein Receiver auf dem virtuellen Desktop übernimmt die Authentifizierung beim zweiten StoreFront-Server. Für diese zweite Verbindung kann eine beliebige Authentifizierungsmethode verwendet werden. Die für den ersten Hop dargestellte Konfiguration kann im zweiten Hop wiederverwendet oder nur für den zweiten Hop verwendet werden.

Passthrough-Authentifizierung und Single Sign-On mit Smartcards

Passthrough-Authentifizierung

Die Passthrough-Authentifizierung mit Smartcards bei virtuellen Desktops wird auf Benutzergeräten unterstützt, auf denen Windows 10, Windows 8 oder Windows 7 SP1 Enterprise und Professional Edition ausgeführt werden.

Die Passthrough-Authentifizierung mit Smartcards für gehosteten Anwendungen wird auf Servern unterstützt, auf denen Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 oder Windows Server 2008 R2 SP1 ausgeführt wird.

Wenn Sie die Passthrough-Authentifizierung mit Smartcards für gehostete Anwendungen verwenden, stellen Sie sicher, dass Sie für Passthrough mit Smartcard als Authentifizierungsmethode für die Site die Verwendung von Kerberos aktivieren.

Hinweis: Die Verfügbarkeit der Passthrough-Authentifizierung mit Smartcards hängt von vielen Faktoren ab, u. a.:

- Sicherheitsrichtlinien für die Passthrough-Authentifizierung der jeweiligen Organisation
- Typ und Konfiguration der Middleware
- Typen der Smartcardleser
- Richtlinie für das Zwischenspeichern von Middleware-PINs

Die Passthrough-Authentifizierung mit Smartcards wird in Citrix StoreFront konfiguriert. Weitere Informationen finden Sie in der Dokumentation zu StoreFront.

Single Sign-On

Single Sign-On ist ein Citrix Feature, mit dem die Passthrough-Authentifizierung in Starts von virtuellen Desktops und Anwendungen implementiert wird. Sie können dieses Feature bei Smartcardbereitstellungen verwenden, die in Domänen eingebunden und direkt mit StoreFront verbunden sind, sowie bei in Domänen eingebundenen und über NetScaler mit StoreFront verbundenen Bereitstellungen. So müssen Benutzer ihre PIN weniger häufig eingeben. Zur die Verwendung von Single Sign-On in diesen Bereitstellungstypen bearbeiten Sie die folgenden Parameter in der Datei default.ica, die sich auf dem StoreFront-Server befindet:

- In Domänen eingebundene, direkt mit StoreFront verbundene Smartcardbereitstellungen: Einstellung für DisableCtrlAltDel auf Off
- In Domänen eingebundene, über NetScaler mit StoreFront verbundene Smartcardbereitstellungen: Einstellung für UseLocalUserAndPassword auf On

Weitere Anweisungen zum Einrichten dieser Parameter finden Sie in der Dokumentation für StoreFront oder NetScaler Gateway.

Die Verfügbarkeit der Single Sign-On-Funktion hängt von vielen Faktoren ab, u. a.:

- Sicherheitsrichtlinien für Single Sign-On der jeweiligen Organisation
- Typ und Konfiguration der Middleware
- Typen der Smartcardleser
- Richtlinie für das Zwischenspeichern von Middleware-PINs

Hinweis: Wenn Benutzer sich beim Virtual Delivery Agent (VDA) mit einer Maschine anmelden, an die ein Smartcardleser angeschlossen ist, wird möglicherweise eine Windows-Kachel angezeigt, die die letzte erfolgreiche Authentifizierungsmethode repräsentiert, z. B. Smartcard oder Kennwort. Daher wird bei aktiviertem Single Sign-On ggf. eine entsprechende Kachel angezeigt. Zum Anmelden müssen die Benutzer die Option
“Benutzer wechseln”auswählen, um eine andere Kachel auszuwählen, da die Single Sign-On-Kachel nicht funktioniert.

Transport Layer Security (TLS)

January 21, 2022

Das Konfigurieren einer XenApp- oder XenDesktop-Site zur Verwendung des TLS-Sicherheitsprotokolls (Transport Layer Security) umfasst folgende Schritte:

- Rufen Sie ein Serverzertifikat ab und installieren und registrieren Sie es auf allen Delivery Controllern. Konfigurieren Sie einen Port mit dem TLS-Zertifikat. Einzelheiten finden Sie unter Installieren von TLS-Serverzertifikaten auf Controllern.

  Sie können die Ports ändern, die der Controller zum Abhören von HTTP- und HTTPS-Datenverkehr verwendet.

- Aktivieren Sie TLS-Verbindungen zwischen Benutzern und Virtual Delivery Agents (VDAs) mit den folgenden Schritten:

  - Konfigurieren Sie TLS auf den Maschinen, auf denen die VDAs installiert sind. (Der Einfachheit halber werden nachfolgend Maschinen, auf denen VDAs installiert sind, als “VDAs” bezeichnet.) Sie können ein PowerShell-Skript von Citrix verwenden oder eine manuelle Konfiguration vornehmen. Allgemeine Informationen finden Sie unter TLS-Einstellungen auf VDAs. Detaillierte Informationen finden Sie unter Konfigurieren von auf einem VDA mit dem PowerShell-Skript und Manuelle Konfiguration von TLS auf einem VDA.
  - Konfigurieren Sie TLS in den Bereitstellungsgruppen, die die VDAs enthalten, indem Sie eine Reihe von PowerShell-Cmdlets in Studio ausführen. Einzelheiten finden Sie unter Konfigurieren von TLS auf Bereitstellungsgruppen.

Anforderungen und Überlegungen:

- Das Aktivieren von TLS-Verbindungen zwischen Benutzern und VDAs gilt nur für XenApp 7.6- und XenDesktop 7.6-Sites sowie für unterstützte höhere Releases.
- Konfigurieren Sie TLS in den Bereitstellungsgruppen und auf den VDAs nach der Installation von Komponenten sowie nach dem Erstellen von Sites, Maschinenkatalogen und Bereitstellungsgruppen.
- Zum Konfigurieren von TLS in den Bereitstellungsgruppen müssen Sie die Berechtigung zum Ändern der Zugriffsregeln für Controller haben; ein Volladministrator hat diese Berechtigung.
- Zum Konfigurieren von TLS auf den VDAs müssen Sie ein Windows-Administrator auf der Maschine sein, auf der der VDA installiert ist.
- Wenn Sie TLS auf VDAs konfigurieren möchten, für die ein Upgrade von einer früheren Version durchgeführt wurde, deinstallieren Sie die SSL-Relay-Software vor dem Upgrade von den Maschinen.
- Das PowerShell-Skript konfiguriert TLS auf statischen VDAs, jedoch nicht auf gepoolten VDAs, die von Maschinenerstellungsdienste oder Provisioning Services bereitgestellt wurden und deren Maschinenimage bei jedem Neustart zurückgesetzt wird.

> **Warnung:**
>
> Vorsicht beim Bearbeiten der Windows-Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Weitere Informationen zur Aktivierung von TLS auf der Sitedatenbank finden Sie unter CTX137556.

> **Hinweis:**
>
> Wenn TLS und UDT am VDA aktiviert sind:
>
> - Für den direkten Zugriff auf den VDA verwendet Citrix Receiver immer TLS über TCP (nicht UDP und UDT).
> - Für den indirekten Zugriff auf den VDA mit NetScaler Gateway verwendet Citrix Receiver DTLS über UDP für die Kommunikation mit NetScaler Gateway. Für die Kommunikation zwischen NetScaler Gateway und VDA wird UDP ohne DTLS verwendet. UDT wird verwendet.

Installieren von TLS-Serverzertifikaten auf Controllern

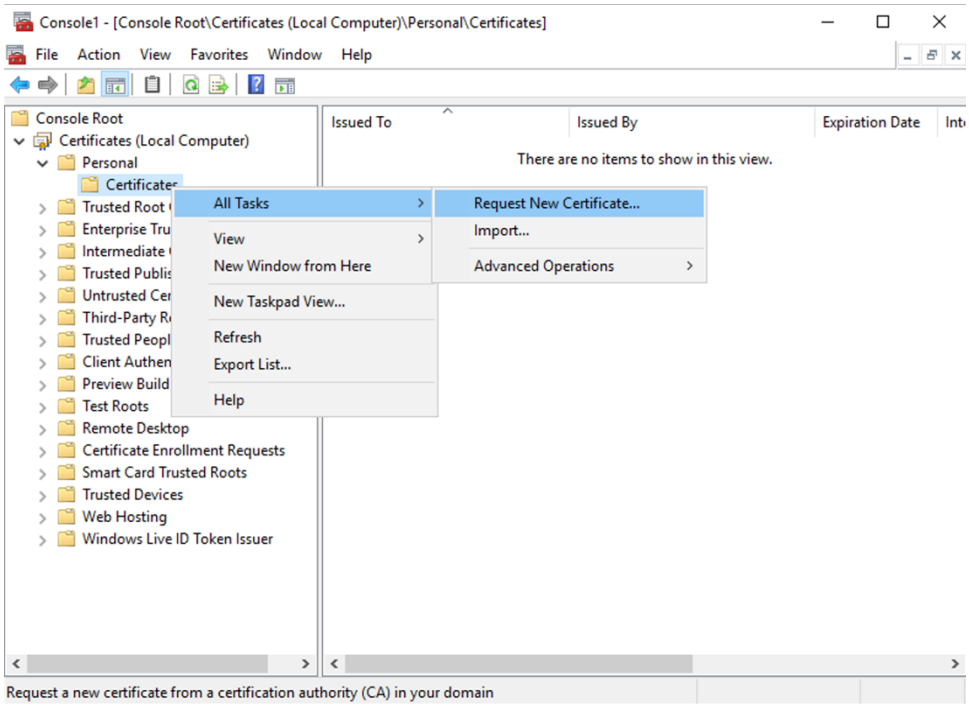
Für HTTPS wird TLS vom XML-Dienst über Serverzertifikate, nicht aber über Clientzertifikate unterstützt. In diesem Abschnitt wird das Beschaffen und Installieren von TLS-Zertifikaten für Delivery Controller beschrieben. Die gleichen Schritte können auf Cloud Connectors zum Verschlüsseln des STA- und XML-Datenverkehrs ausgeführt werden.

Es gibt verschiedene Arten von Zertifizierungsstellen und Methoden zum Anfordern von Zertifikaten. Die Erläuterungen hier basieren auf der Microsoft-Zertifizierungsstelle. Für die Microsoft-Zertifizierungsstelle muss eine Zertifikatvorlage mit dem Zweck "Serverauthentifizierung"veröffentlicht sein.

Wenn die Microsoft-Zertifizierungsstelle in eine Active Directory-Domäne oder die vertrauenswürdige Gesamtstruktur integriert ist, zu der die Delivery Controller gehören, können Sie ein Zertifikat über den Assistenten für die Zertifikatregistrierung des MMC-Snap-Ins Zertifikate beschaffen.

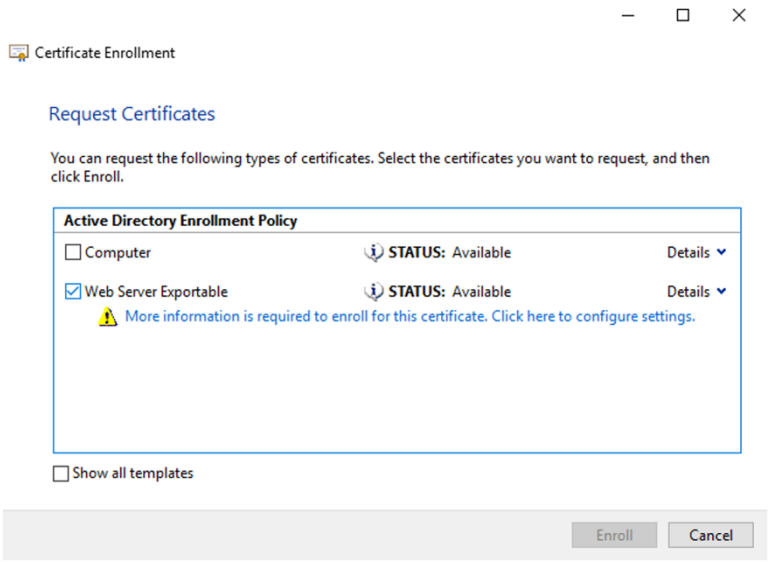
Anfordern und Installieren eines Zertifikats

1. Öffnen Sie auf dem Delivery Controller die MMC-Konsole und fügen Sie das Zertifikat-Snap-In hinzu. Wählen Sie bei Aufforderung "Computerkonto"aus.
2. Erweitern Sie **Persönlich > Zertifikate** und verwenden Sie dann den Kontextmenübefehl **Alle Aufgaben > Neues Zertifikat anfordern**.



3. Klicken Sie auf **Weiter** und erneut auf **Weiter**, um zu bestätigen, dass Sie das Zertifikat von der Active Directory-Registrierung erwerben.

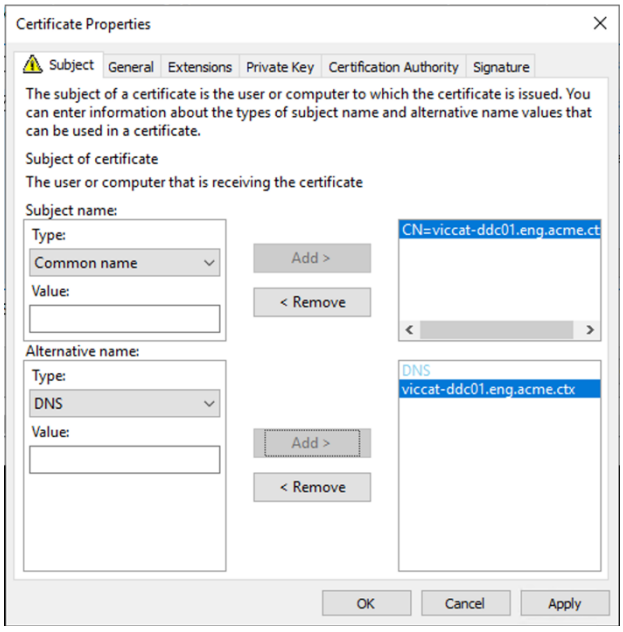
4. Wählen Sie die Vorlage für das Zertifikat “Serverauthentifizierung”aus. Wenn die Vorlage automatisch einen Antragsteller enthält, können Sie auf **Registrieren** klicken, ohne weitere Details anzugeben.



5. Um weitere Details für die Zertifikatvorlage anzugeben, klicken Sie auf die Schaltfläche **Details** und konfigurieren Sie Folgendes:

   Antragstellername: Wählen Sie “Allgemeiner Name”und geben Sie den FQDN des Delivery Controllers an.

   Alternativer Name: Wählen Sie “DNS”und geben Sie den FQDN des Delivery Controllers an.



Konfigurieren des SSL-/TLS-Listener-Ports

1. Öffnen Sie ein PowerShell-Befehlsfenster als Administrator der Maschine.
2. Führen Sie die folgenden Befehle aus, um die Anwendungs-GUID des Brokerdiensts zu erhalten:

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $\_; $\_.GetValueNames() | ForEach-Object {
  $key.GetValue($\_)  }
  | Where-Object {
  $\_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
    ForegroundColor Yellow
<!--NeedCopy-->
```

3. Führen Sie die folgenden Befehle im selben PowerShell-Fenster aus, um den Fingerabdruck des zuvor installierten Zertifikats abzurufen:

```
$HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
    .Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $(
    $Thumbprint)" -Foreground Yellow
<!--NeedCopy-->
```

4. Führen Sie die folgenden Befehle im selben PowerShell-Fenster aus, um den Broker Service SSL/TLS-Port und das Zertifikat für die Verschlüsselung zu konfigurieren:

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
    | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"
```



```
4
5  $SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
       appid={
6   $Formatted_Guid }
7   "
8
9  $SSLxml | netsh
10
11 . netsh http show sslcert
12 <!--NeedCopy-->
```

Bei korrekter Konfiguration zeigt die Ausgabe des letzten Befehls `.netsh http show sslcert`, dass der Listener den richtigen `IP:port` verwendet und dass `Application ID` der Anwendungs-GUID des Brokerdiensts entspricht.

Sofern die Server dem auf den Delivery Controllern installierten Zertifikat vertrauen, können Sie jetzt StoreFront-Delivery Controller und Citrix Gateway STA-Bindungen zur Verwendung von HTTPS anstelle von HTTP konfigurieren.

Die Liste der Verschlüsselungssammlungsreihenfolge sollte die Verschlüsselungssammlung `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` oder `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (oder beide) enthalten. Diese Verschlüsselungssammlungen müssen vor jeglichen `TLS_DHE_`-Verschlüsselungssammlungen stehen.

> **Hinweis:**
>
> Windows Server 2012 unterstützt die GCM-Verschlüsselungssammlungen `TLS_ECDHE_RSA_WITH_AES_256` oder `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` nicht.

1. Navigieren Sie mit dem Microsoft Gruppenrichtlinien-Editor zu **Computerkonfiguration > Administrative Vorlagen > Netzwerk > SSL-Konfigurationseinstellungen**.
2. Bearbeiten Sie die Richtlinie **Reihenfolge der SSL-Verschlüsselungssammlungen**. Standardmäßig ist diese Richtlinie auf **Nicht konfiguriert** festgelegt. Legen Sie diese Richtlinie auf **Aktiviert** fest.
3. Bringen Sie die Verschlüsselungssammlungen in die richtige Reihenfolge und entfernen Sie alle Verschlüsselungssammlungen, die Sie nicht verwenden möchten.

Stellen Sie sicher, dass entweder `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` oder `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` vor `TLS_DHE_`-Verschlüsselungssammlungen steht.

Siehe auch Prioritizing Schannel Cipher Suites auf Microsoft-MSDN.

Ändern von HTTP- oder HTTPS-Ports

Der XML-Dienst auf dem Controller hört standardmäßig Port 80 auf HTTP-Datenverkehr und Port 443 auf HTTPS-Datenverkehr ab. Zwar können auch andere Ports verwendet werden, jedoch wird der Controller dabei nicht vertrauenswürdigen Netzwerken ausgeliefert, und es entsteht ein Sicherheitsrisiko. Das Bereitstellen eines eigenständigen StoreFront-Servers ist dem Ändern der Standardwerte vorzuziehen.

Zum Ändern der vom Controller verwendeten standardmäßigen HTTP- oder HTTPS-Ports führen Sie den folgenden Befehl in Studio aus:

```
BrokerService.exe -WIPORT http-port -WISSLPORT https-port
```

http-port ist die Portnummer für HTTP-Datenverkehr und *https-port* ist die Portnummer für HTTPS-Datenverkehr.

Nachdem Sie einen Port geändert haben, zeigt Studio möglicherweise eine Meldung zur Lizenzkompatibilität und Upgrades an. Sie lösen das Problem, indem Sie Dienstinstanzen mit den folgenden PowerShell-Cmdlets neu registrieren:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS | |
Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq “XML_HTTPS” |
Register-ConfigServiceInstance
```

Erzwingen von HTTPS-Datenverkehr

Wenn der XML-Dienst den HTTP-Datenverkehr ignorieren soll, erstellen Sie die folgende Registrierungseinstellung unter HKLM\Software\Citrix\DesktopServer\ auf dem Controller und starten Sie den Brokerdienst neu.

Um den HTTP-Datenverkehr zu ignorieren, erstellen Sie DWORD XmlServicesEnableNonSsl und legen Sie den Eintrag auf 0 fest.

Es gibt einen entsprechenden DWORD-Registrierungswert, den Sie erstellen können, damit der HTTPS-Datenverkehr ignoriert wird: DWORD XmlServicesEnableSsl. Stellen Sie sicher, dass er nicht auf 0 festgelegt ist.

TLS-Einstellungen auf VDAs

Eine Bereitstellungsgruppe darf nicht eine Mischung von VDAs mit und ohne konfiguriertem TLS enthalten. Wenn Sie TLS für eine Bereitstellungsgruppe konfigurieren, sollten Sie TLS bereits für alle VDAs in dieser Bereitstellungsgruppe konfiguriert haben.

Wenn Sie TLS auf VDAs konfigurieren, werden Berechtigungen auf dem installierten TLS-Zertifikat geändert. Der ICA-Dienst erhält Lesezugriff für den privaten Schlüssel des Zertifikats und wird über Folgendes informiert:

- **Das für TLS zu verwendende Zertifikat im Zertifikatspeicher**
- **Die für TLS-Verbindungen zu verwendende TCP-Portnummer**

Die Windows-Firewall (wenn sie aktiviert ist) muss so konfiguriert sein, dass eingehende Verbindungen auf diesem TCP-Port zugelassen sind. Diese Konfiguration wird für Sie ausgeführt, wenn Sie das PowerShell-Skript verwenden.

- **Welche Versionen des TLS-Protokolls zulässig sind.**

> **Wichtig**
>
> Citrix empfiehlt den Einsatz von SSL Version 3 zu prüfen und die Konfiguration von Bereitstellungen soweit möglich dahingehend zu ändern, dass SSL Version 3 nicht mehr unterstützt wird. Siehe CTX200238.

Die unterstützten SSL-Protokollversionen unterliegen einer Hierarchie (von der niedrigsten zur höchsten Version): TLS 3.0, TLS 1.0, TLS 1.1 und TLS 1.2. Geben Sie die niedrigste zulässige Version an. Alle Protokollverbindungen, die diese Version oder eine höhere Version verwenden, sind dann zulässig.

Wenn Sie beispielsweise TLS 1.1 als Mindestversion angeben, werden auch TLS 1.1- und TLS 1.2-Protokollverbindungen zugelassen. Wenn Sie SSL 3.0 als Mindestversion angeben, sind Verbindungen für alle unterstützten Versionen zulässig. Wenn Sie TLS 1.2 als Mindestversion angeben, werden nur TLS 1.2-Verbindungen zugelassen.

- **Welche TLS-Verschlüsselungssammlungen zugelassen werden sollen.**

Über eine Verschlüsselungssammlung wird die Verschlüsselung für eine Verbindung gewählt. Clients und VDAs können verschiedene Gruppen von Verschlüsselungssammlungen unterstützen. Wenn ein Client (Citrix Receiver oder StoreFront) eine Verbindung herstellt und eine Liste unterstützter TLS-Verschlüsselungssammlungen übermittelt, ordnet der VDA eine Verschlüsselungssammlung des Clients einer Sammlung in seiner eigenen Liste konfigurierter Verschlüsselungssammlungen zu und akzeptiert die Verbindung. Gibt es keine übereinstimmende Verschlüsselungssammlung, lehnt der VDA die Verbindung ab.

Der VDA unterstützt drei Verschlüsselungssammlungen (auch "Konformitätsmodi"): GOV (Government = Behörden), COM (Commercial = Kommerziell) und ALL (Alle). Welche Verschlüsselungssammlungen zulässig sind, hängt auch vom Windows FIPS-Modus ab. Weitere Informationen zum Windows FIPS-Modus finden Sie unter `https://support.microsoft.com/kb/811833`. Die folgende Tabelle enthält die Verschlüsselungssammlungen in jeder Gruppe:

TLS-Verschlüsselungssammlung	GOV	COM	ALLE	GOV	COM	ALLE
FIPS-Modus	Aus	Aus	Aus	Ein	Ein	Ein
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	x		x	x		x
TLS_RSA_WITH_AES_256_GCM_SHA384			x	x		x
TLS_RSA_WITH_AES_128_GCM_SHA256			x	x	x	x
TLS_RSA_WITH_AES_256_CBC_SHA256			x	x		x
TLS_RSA_WITH_AES_256_CBC_SHA			x	x		x
TLS_RSA_WITH_AES_128_CBC_SHA			x		x	x
TLS_RSA_WITH_RC4_128_SHA			x			
TLS_RSA_WITH_RC4_128_MD5			x			
TLS_RSA_WITH_3DES_EDE_CBC_SHA			x	x		x

> **Wichtig:**
>
> Ein zusätzlicher Schritt ist erforderlich, wenn der VDA unter Windows Server 2012 R2, Windows Server 2016, Windows 10 Anniversary Edition oder einer unterstützten Nachfolgeversion ausgeführt wird. Dies betrifft Verbindungen von Citrix Receiver für Windows (Version 4.6 bis 4.9), Citrix Receiver für HTML5 und Citrix Receiver für Chrome. Außerdem sind Verbindungen über NetScaler Gateway betroffen.
>
> Dieser Schritt ist auch für alle Verbindungen mit NetScaler Gateway für alle VDA-Versionen erforderlich, wenn TLS zwischen dem NetScaler Gateway und dem VDA konfiguriert ist. Dies betrifft alle Citrix Receiver-Versionen.

Rufen Sie auf dem VDA (Windows Server 2016/Windows 10 Anniversary Edition oder höher) im Gruppenrichtlinien-Editor **Computerkonfiguration > Administrative Vorlagen > Netzwerk > SSL-Konfigurationseinstellungen > Reihenfolge der SSL-Verschlüsselungssammlungen** auf. Wählen Sie die folgende Reihenfolge:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **Hinweis:**
>
> Die ersten vier Elemente spezifizieren auch die elliptische Kurve (P384 oder P256). Stellen Sie sicher, dass "curve25519"nicht ausgewählt ist. Der FIPS-Modus verhindert die Verwendung von "curve25519"nicht.

Wenn diese Gruppenrichtlinieneinstellung konfiguriert ist, wählt der VDA eine Verschlüsselungssammlung nur, wenn sie in beiden Listen (Liste der Gruppenrichtlinie und Konformitätsmodusliste, d. h. COM, GOV oder ALL) enthalten ist. Die Verschlüsselungssammlung muss auch auf der vom Client (Citrix Receiver oder StoreFront) gesendeten Liste stehen.

Diese Gruppenrichtlinienkonfiguration wirkt sich auch auf andere TLS-Anwendungen und -Dienste auf dem VDA aus. Wenn Ihre Anwendungen bestimmte Verschlüsselungssammlungen erfordern, müssen Sie diese möglicherweise der Gruppenrichtlinienliste hinzufügen.

> **Wichtig:**
>
> Gruppenrichtlinienänderungen werden zwar bei ihrer Anwendung angezeigt, Gruppenrichtlinienänderungen an der TLS-Konfiguration werden jedoch erst nach einem Neustart des Betriebssystems wirksam. Wenden Sie daher für gepoolte Desktops die Gruppenrichtlinienänderungen an der TLS-Konfiguration auf das Basisimage an.

Konfigurieren von TLS auf einem VDA mit dem PowerShell-Skript

Das Skript Enable-VdaSSL.ps1 aktiviert oder deaktiviert den TLS-Listener auf einem VDA. Dieses Skript ist im Ordner Support > Tools > SslSupport auf dem Installationsmedium verfügbar.

Wenn Sie TLS aktivieren, deaktiviert das Skript alle vorhandenen Windows-Firewallregeln für den angegebenen TCP-Port. Dann wird eine Regel hinzugefügt, die dem ICA-Dienst die Annahme eingehender Verbindungen nur auf dem TLS-TCP-Port gewährt. Außerdem werden die Windows-Firewallregeln für Folgendes deaktiviert:

- Citrix ICA (Standard: 1494)
- Citrix CGP (Standard: 2598)
- Citrix WebSocket (Standard: 8008)

Die Folge ist, dass Benutzer nur mit TLS die Verbindung herstellen könne. Sie können ICA/HDX, ICA/HDX mit Sitzungszuverlässigkeit oder HDX über WebSocket nicht ohne TLS .

Siehe Netzwerkports.

> **Hinweis:**
>
> Für zustandslose Maschinen, wie PVS-Ziele oder MCS-Klone, wird standardmäßig ein FQDN-Zertifikat verwendet.

Das Skript enthält die folgenden Syntax-Beschreibungen sowie zusätzliche Beispiele. Sie können diese Informationen mit einem Tool wie Notepad++ lesen.

> **Wichtig:**
>
> Geben Sie den Parameter “Enable”oder “Disable”und den Parameter “CertificateThumbPrint” an. Die übrigen Parameter sind optional.

Syntax

```
Enable-VdaSSL {
 -Enable | -Disable }
  -CertificateThumbPrint "<thumbprint>"
[ – SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-
    SSLCipherSuite"<suite>"]
<!--NeedCopy-->
```

Parameter	Beschreibung
Smartcard	Installiert und aktiviert den TLS-Listener auf dem VDA. Es ist dieser Parameter oder der Parameter “Disable”erforderlich.
Deaktivieren	Deaktiviert den TLS-Listener auf dem VDA. Es ist dieser Parameter oder der Parameter “Enable” erforderlich. Wenn Sie diesen Parameter festlegen, sind keine anderen Parameter gültig.
CertificateThumbPrint “”	Fingerabdruck des TLS-Zertifikats im Zertifikatspeicher in Anführungszeichen. Das Skript verwendet den angegebenen Fingerabdruck zur Auswahl des gewünschten Zertifikats. Wird dieser Parameter ausgelassen, wird ein falsches Zertifikat ausgewählt.
SSLPort	TLS port. Standard: 443.

Parameter	Beschreibung
SSLMinVersion “”	Mindestversion des TLS-Protokolls zwischen Anführungszeichen. Gültige Werte: “SSL_3.0”, “TLS_1.0”(Standardwert), “TLS_1.1”und “TLS_1.2”. **Wichtig:** Citrix empfiehlt seinen Kunden den Einsatz von SSL Version 3 zu prüfen und die Konfiguration von Bereitstellungen möglichst dahingehend zu ändern, dass SSL Version 3 nicht mehr unterstützt wird. Siehe CTX200238.
SSLCipherSuite “”	TLS-Verschlüsselungssammlung zwischen Anführungszeichen. Gültige Werte: “GOV”, “COM”und “ALL”(Standardwert).

Beispiele

Das folgende Skript installiert und aktiviert den TLS 1.2-Versionswert. Der Fingerabdruck (im Beispiel dargestellt als “12345678987654321”) dient zur Auswahl des Zertifikats, das verwendet werden soll.

```
Enable-VdaSSL –Enable -CertificateThumbPrint "12345678987654321"
```

Das folgende Skript installiert und aktiviert den TLS-Listener und gibt den TLS-Port 400 an sowie die Verschlüsselungssammlung GOV (Behörden) und als Mindestprotokollversion “TLS 1.2”. Der Fingerabdruck (im Beispiel dargestellt als “12345678987654321”) dient zur Auswahl des Zertifikats, das verwendet werden soll.

```
Enable-VdaSSL –Enable -CertificateThumbPrint "12345678987654321"–
SSLPort 400 -SSLMinVersion "TLS_1.2"–SSLCipherSuite "All"
```

Das folgende Skript deaktiviert den TLS-Listener auf dem VDA.

```
Enable-VdaSSL –Disable
```

Manuelle Konfiguration von TLS auf einem VDA

Bei der manuellen Konfiguration von TLS auf einem VDA gewähren Sie dem privaten Schlüssel des TLS-Zertifikats allgemeinen Lesezugriff für den entsprechenden Dienst auf jedem VDA: NT SERVICE\PorticaService für einen VDA für Windows-Desktopbetriebssysteme oder NT SERVICE\TermService für einen VDA für Windows-Serverbetriebssysteme. Führen Sie auf der Maschine, auf der der VDA installiert ist, folgende Schritte aus:

1. Starten Sie die Microsoft Management Console (MMC): **Start > Ausführen > mmc.exe**.
2. Fügen Sie dem MMC das Zertifikat-Snap-In hinzu:
    a) Wählen Sie **Datei > Snap-In hinzufügen/entfernen**.
    b) Wählen Sie **Zertifikate** aus, und klicken Sie dann auf **Hinzufügen**.
    c) Wählen Sie unter **Dieses Snap-In verwaltet die Zertifikate für:** die Option **Computerkonto** und klicken Sie dann auf **Weiter**.
    d) Wählen Sie unter **Wählen Sie den Computer aus, den dieses Snap-In verwalten soll** die Option **Lokalen Computer** und klicken Sie dann auf **Fertig stellen**.
3. Klicken Sie unter **Zertifikate (Lokaler Computer) > Persönlich > Zertifikate** mit der rechten Maustaste auf das Zertifikat und wählen Sie dann **Alle Aufgaben > Private Schlüssel verwalten**.
4. Im Zugriffssteuerungslisten-Editor wird "Permissions for (FriendlyName) private keys" angezeigt, wobei (FriendlyName) der Name des TLS-Zertifikats ist. Fügen Sie einen der folgenden Dienste hinzu und geben Sie ihm Lesezugriff:
    - Für einen VDA für Windows-Desktopbetriebssysteme "PORTICASERVICE"
    - Für einen VDA für Windows-Serverbetriebssysteme "TERMSERVICE"
5. Doppelklicken Sie auf das installierte TLS-Zertifikat. Wählen Sie im Dialogfeld "Zertifikat"die Registerkarte **Details** und scrollen Sie dann nach unten. Klicken Sie auf **Fingerabdruck**.
6. Führen Sie regedit aus und navigieren Sie zu HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.
    a) Bearbeiten Sie den SSL-Fingerabdruckschlüssel und kopieren Sie den Fingerabdruckwert des TLS-Zertifikats in den binären Wert. Sie können unbekannte Elemente im Dialogfeld Binärwert bearbeiten ignorieren (z. B. "0000"und Sonderzeichen).
    b) Bearbeiten Sie den Schlüssel "SSLEnabled"und ändern Sie den Wert für DWORD in "1". (Um SSL zu einem späteren Zeitpunkt zu deaktivieren, ändern Sie den Wert für DWORD in "0&".)
    c) Wenn Sie die Standardeinstellungen ändern möchten (optional), verwenden Sie Folgendes im gleichen Registrierungspfad:

        SSLPort DWORD –SSL-Portnummer. Standard: 443.

        SSLMinVersion DWORD –1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Standard: 2 (TLS 1.0).

        SSLCipherSuite DWORD –1 = GOV, 2 = COM, 3 = ALL. Standard: 3 (ALL).
7. Stellen Sie sicher, dass der TLS-TCP-Port in der Windows-Firewall geöffnet ist, wenn Sie nicht den Standardport 443 verwenden. (Wenn Sie die eingehende Regel für die Windows-Firewall

erstellen, wählen Sie in den Eigenschaften die Optionen **Verbindung zulassen** und **Aktiviert** aus.)

8. Stellen Sie sicher, dass keine anderen Anwendungen oder Dienste (z. B. IIS) den TLS-TCP-Port verwenden.
9. Damit die Änderungen auf VDAs für Windows-Serverbetriebssysteme wirksam werden, starten Sie die Maschine neu. (Sie brauchen Maschinen mit VDAs für Windows-Desktopbetriebssysteme nicht neu starten.)

Konfigurieren von TLS auf Bereitstellungsgruppen

Führen Sie diese Schritte für jede Bereitstellungsgruppe aus, die VDAs enthält, die Sie für TLS-Verbindungen konfiguriert haben.

1. Öffnen Sie in Studio die PowerShell-Konsole.
2. Führen Sie `asnp Citrix.*` aus, um die Citrix Produkt-Cmdlets zu laden.
3. Führen Sie `Get-BrokerAccessPolicyRule -DesktopGroupName 'delivery-group-name' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true` aus.
4. Führen Sie `Set-BrokerSite -DnsResolutionEnabled $true` aus.

Problembehandlung

Wenn ein Verbindungsfehler auftritt, überprüfen Sie Systemereignisprotokoll des VDAs.

Tritt bei Verwendung von Citrix Receiver für Windows ein TLS-Verbindungsfehler auf (z. B. 1030), deaktivieren Sie Desktop Viewer und versuchen Sie eine neue Verbindung. Die Verbindung wird zwar dennoch fehlschlagen, es wird jedoch möglicherweise eine Erklärung zu der Ursache angegeben. Beispielsweise könnten Sie beim Anfordern eines Zertifikats von der Zertifizierungsstelle eine falsche Vorlage angegeben haben.

Kommunikation zwischen Controller und VDA

Die Kommunikation zwischen Controller und VDA wird auf Nachrichtenebene durch Windows Communication Framework (WCF) gesichert. Zusätzlicher Schutz auf Übertragungsebene durch TLS ist nicht erforderlich. Die WCF-Konfiguration verwendet Kerberos für die gegenseitige Authentifizierung von Controller und VDA. Die Verschlüsselung verwendet AES im CBC-Modus mit einem 256-Bit-Schlüssel. Für die Nachrichtenintegrität wird SHA-1 verwendet.

Laut Microsoft entsprechen die Sicherheitsprotokolle von WCF den OASIS-Standards (Organization for the Advancement of Structured Information Standards), einschließlich WS-SecurityPolicy 1.2.

Darüber hinaus unterstützt WCF laut Microsoft sämtliche unter SecurityPolicy 1.2 aufgeführten Algorithmussammlungen.

Für die Kommunikation zwischen Controller und VDA wird die Algorithmussammlung basic256 verwendet, deren Algorithmen wie oben angegeben sind.

TLS- und HTML5-Videoumleitung

Sie können die HTML5-Videoumleitung verwenden, um HTTPS-Websites umzuleiten. Das in diese Websites eingefügte JavaScript muss eine TLS-Verbindung mit dem auf dem VDA ausgeführten Citrix Service zur HDX-HTML5-Videoumleitung herstellen. Dazu generiert der HTML5-Videoumleitungsdienst zwei benutzerdefinierte Zertifikate im Zertifikatspeicher auf dem VDA. Durch das Beenden des Diensts werden auch die Zertifikate entfernt.

Die HTML5-Videoumleitungsrichtlinie ist standardmäßig deaktiviert.

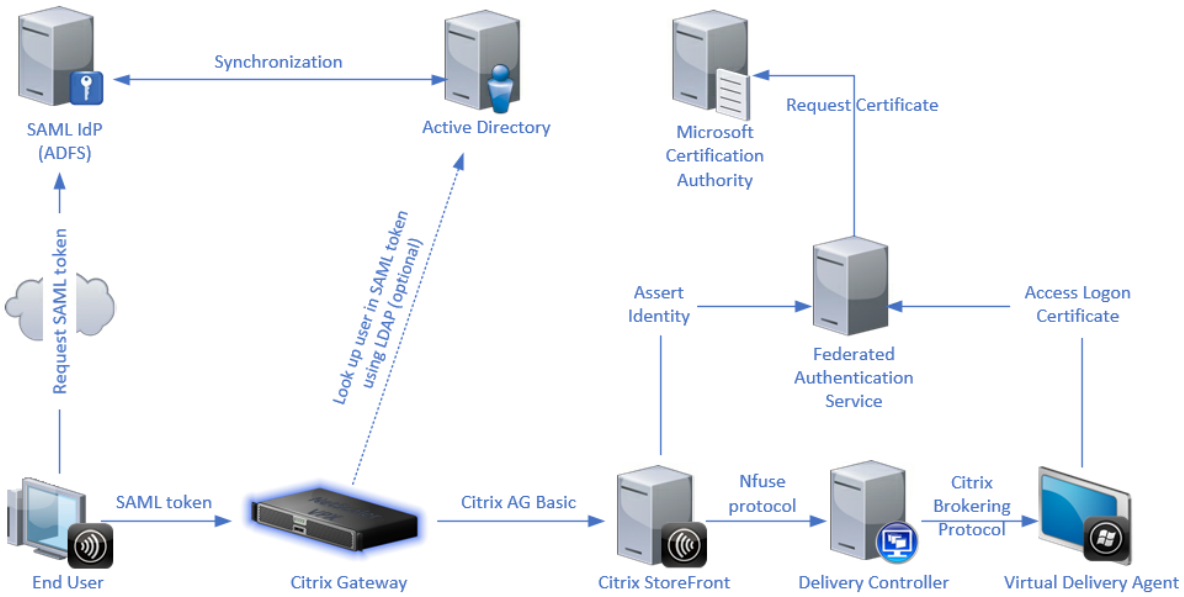
Weitere Informationen zur HTML5-Videoumleitung finden Sie unter Richtlinieneinstellungen für Multimedia.

Verbundauthentifizierungsdienst

February 15, 2024

Der Citrix Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ist eine privilegierte Komponente für die Integration in Active Directory-Zertifikatdienste. Der Dienst stellt dynamisch Zertifikate für Benutzer aus, sodass diese sich bei einer Active Directory-Umgebung so anmelden können, als hätten sie eine Smartcard. Durch FAS kann in StoreFront eine größere Bandbreite an Authentifizierungsoptionen, darunter z. B. SAML-Assertionen (Security Assertion Markup Language), verwendet werden. SAML (Security Assertion Markup Language) wird häufig als Alternative für herkömmliche Windows-Benutzerkonten im Internet verwendet.

Das folgende Diagramm zeigt die Integration von FAS mit einer Zertifizierungsstelle zur Bereitstellung von Diensten für StoreFront und XenApp und XenDesktop Virtual Delivery Agents (VDAs).



Vertrauenswürdige StoreFront-Server kontaktieren den Verbundauthentifizierungsdienst (FAS), wenn Benutzer Zugriff auf die Citrix Umgebung anfordern. Der FAS stellt ein Ticket aus, mit dem eine einzelne XenApp- oder XenDesktop-Sitzung eine Authentifizierung mit einem Zertifikat für die Sitzung durchführen kann. Wenn ein VDA einen Benutzer authentifizieren muss, stellt er eine Verbindung mit dem FAS her und löst das Ticket aus. Nur der FAS hat Zugriff auf den privaten Schlüssel des Benutzerzertifikats. Der VDA sendet jeden erforderlichen Signier- und Entschlüsselungsvorgang zusammen mit dem Zertifikat an FAS.

Anforderungen

Der Verbundauthentifizierungsdienst wird unter Windows Server-Betriebssystemen (Windows Server 2008 R2 oder höher) unterstützt.

- Citrix empfiehlt die Installation des FAS auf einem Server, der keine anderen Citrix-Komponenten enthält.
- Der Windows-Server muss geschützt werden. Er hat Zugriff auf ein Registrierungsstellenzertifikat und den entsprechenden privaten Schlüssel. Der Server verwendet diese Zugriffe, um das Zertifikat für Domänenbenutzer auszustellen. Nach der Ausstellung hat der Server auch Zugriff auf die Benutzerzertifikate und privaten Schlüssel.
- Für das FAS-PowerShell SDK ist Windows PowerShell 64-Bit auf dem FAS-Server erforderlich.
- Für die Ausstellung von Benutzerzertifikaten ist eine Zertifizierungsstelle wie Microsoft Enterprise oder eine andere im Citrix Ready-Programm validierte Zertifizierungsstelle erforderlich.
- Stellen Sie für andere Zertifizierungsstellen als Microsoft Folgendes sicher:

  - Die Zertifizierungsstelle (ZS) ist im Active Directory als Registrierungsdienst registriert.
  - Das Zertifizierungsstellenzertifikat befindet sich im NTAuth-Store auf dem Domänencontroller. Weitere Informationen finden Sie unter Importieren von Zertifizierungsstellenzertifikaten von Drittanbietern in den Enterprise NTAuth-Speicher.

XenApp- bzw. XenDesktop-Site

- Die Delivery Controller müssen mindestens die Version 7.15 haben.
- Die VDAs müssen mindestens die Version 7.15 haben. Stellen Sie sicher, dass Sie die FAS-Gruppenrichtlinienkonfiguration auf die VDAs anwenden, bevor Sie den Maschinenkatalog erstellen. Weitere Informationen finden Sie unter Gruppenrichtlinie konfigurieren.
- Der StoreFront-Server muss mindestens die Version 3.12 haben (XenApp und XenDesktop 7.15 ISO unterstützt die StoreFront-Version 3.12).

Konsultieren Sie bei der Planung der Bereitstellung dieses Diensts den Abschnitt Sicherheitsüberlegungen.

Informationsquellen:

- Active Directory-Zertifikatdienste

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11)?redirectedfrom=MSDN

- Windows für die Zertifikatanmeldung konfigurieren

https://support.citrix.com/article/CTX206156

Reihenfolge der Schritte zur Installation und Einrichtung

1. Verbundauthentifizierungsdienst installieren
2. Plug-In für den Verbundauthentifizierungsdienst auf StoreFront-Servern konfigurieren
3. Gruppenrichtlinie konfigurieren
4. Verwenden Sie die Verwaltungskonsole des Verbundauthentifizierungsdiensts für folgende Aufgaben: (a) Bereitstellen der vorhandenen Vorlagen, (b) Einrichten von Zertifizierungsstellen und (c) Autorisieren des Verbundauthentifizierungsdiensts für die Verwendung der Zertifizierungsstelle.
5. Konfigurieren von Benutzerregeln

Verbundauthentifizierungsdienst installieren

Aus Sicherheitsgründen empfiehlt Citrix die Installation des FAS auf einem dedizierten Server, ähnlich dem Domänencontroller oder der Zertifizierungsstelle. Der FAS kann über die Schaltfläche **Verbun-**

dauthentifizierungsdienst auf dem Begrüßungsbildschirm der automatischen Ausführung beim Einfügen der ISO-Datei installiert werden.

Bei diesem Vorgang werden die folgenden Komponenten installiert:

- Verbundauthentifizierungsdienst
- PowerShell-Snap-In-Cmdlets zur Remotekonfiguration des Verbundauthentifizierungsdiensts
- Verwaltungskonsole des Verbundauthentifizierungsdiensts
- Gruppenrichtlinienvorlagen für den Verbundauthentifizierungsdienst (CitrixFederatedAuthenticationService.admx/adml)
- Zertifikatvorlagendateien zur einfachen Konfiguration einer Zertifizierungsstelle
- Leistungsindikatoren und Ereignisprotokolle

Plug-In für den Verbundauthentifizierungsdienst für einen StoreFront-Store aktivieren

Zum Aktivieren der FAS-Integration auf einem StoreFront-Store führen Sie die folgenden PowerShell-Cmdlets als Administrator aus. Wenn Sie mehrere Stores haben oder der Store einen anderen Namen hat, kann der Pfad von dem unten angegebenen abweichen.

```
1  ```
2  Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
3
4  $StoreVirtualPath = "/Citrix/Store"
5
6  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
7
8  $auth = Get-STFAuthenticationService -StoreService $store
9
10 Set-STFClaimsFactoryNames -AuthenticationService $auth -
       ClaimsFactoryName "FASClaimsFactory"
11
12 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
       FASLogonDataProvider"
13 <!--NeedCopy--> ```
```

Zum Beenden der Verwendung des FAS verwenden Sie folgendes PowerShell-Skript:

```
1  ```
2  Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
3
4  $StoreVirtualPath = "/Citrix/Store"
5
6  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
7
8  $auth = Get-STFAuthenticationService -StoreService $store
9
10 Set-STFClaimsFactoryNames -AuthenticationService $auth -
       ClaimsFactoryName "standardClaimsFactory"
```



```
11
12 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
13 <!--NeedCopy--> ```
```

Delivery Controller konfigurieren

Zur Verwendung des FAS konfigurieren Sie den XenApp- bzw. XenDesktop-Delivery Controller für eine Vertrauensstellung mit den StoreFront-Servern, die mit ihm eine Verbindung herstellen können. Führen Sie hierfür das PowerShell-Cmdlet **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true** aus.

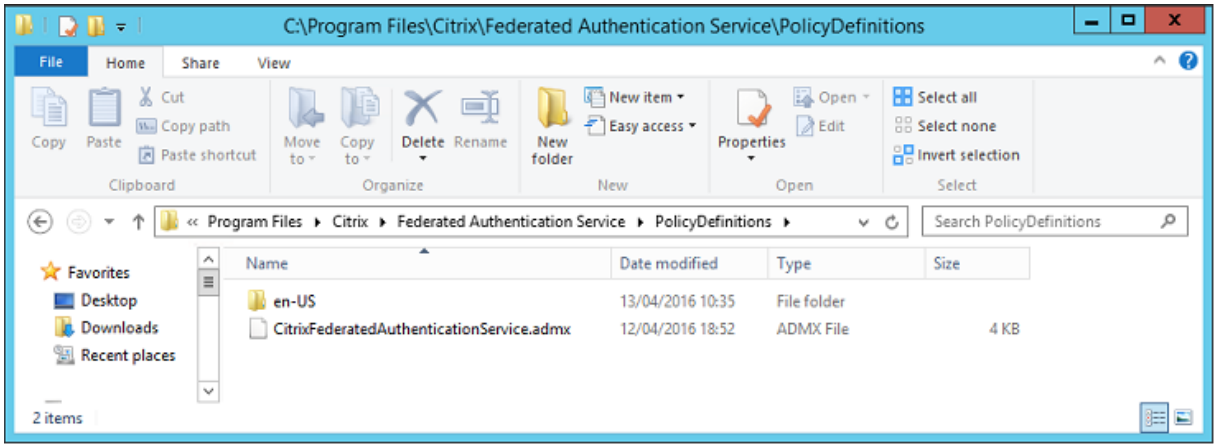
Gruppenrichtlinie konfigurieren

Nach der Installation des FAS müssen Sie die vollständigen DNS-Adressen der FAS-Server in der Gruppenrichtlinie angeben und hierfür die während der Installation bereitgestellten Gruppenrichtlinienvorlagen verwenden.

Wichtig: Die Tickets anfordernden StoreFront-Server und die Tickets auslösenden VDAs müssen die gleiche DNS-Adresskonfiguration haben, einschließlich der automatischen Servernummerierung, die vom Gruppenrichtlinienobjekt angewendet wird.

Die folgenden Beispiele zeigen die Konfiguration einer Richtlinie auf Domänenebene für alle Maschinen. Der FAS funktioniert, wenn die Liste der DNS-Adressen für die StoreFront-Server, die VDAs und die Maschine mit der FAS-Verwaltungskonsole identisch sind. Das Gruppenrichtlinienobjekt fügt jedem Eintrag eine Indexnummer hinzu, die auch übereinstimmen muss, wenn mehr als ein Objekt verwendet wird.

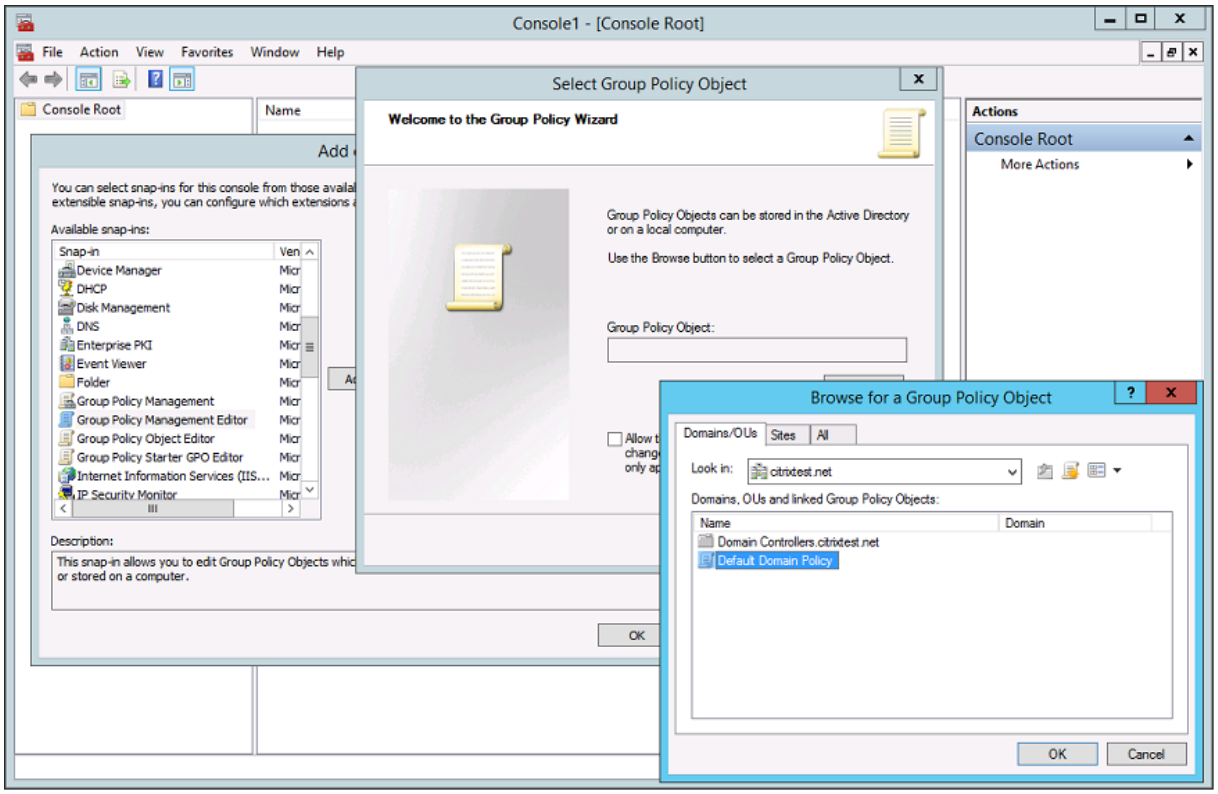
Schritt 1: Suchen Sie auf dem Server, auf dem Sie den FAS installiert haben, die Datei C:\Programme\Citrix\Federat Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx und dann den Ordner “de-DE”.



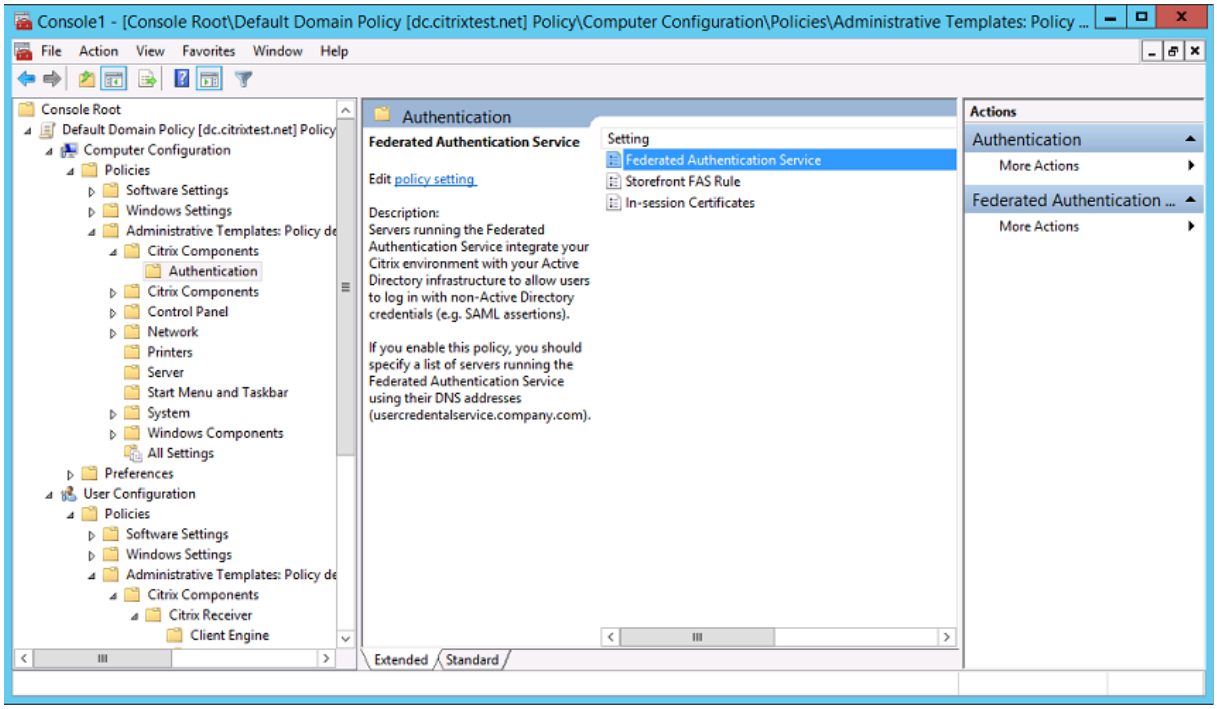
Schritt 2: Kopieren Sie die Dateien und den Ordner auf den Domänencontroller in den Pfad C:\Windows\PolicyDefinitions.

Schritt 3: Führen Sie Microsoft Management Console (Befehlszeile: "mmc.exe") aus. Wählen Sie auf der Menüleiste **Datei > Snap-In hinzufügen/entfernen**. Fügen Sie den **Gruppenrichtlinienverwaltungs-Editor** hinzu.

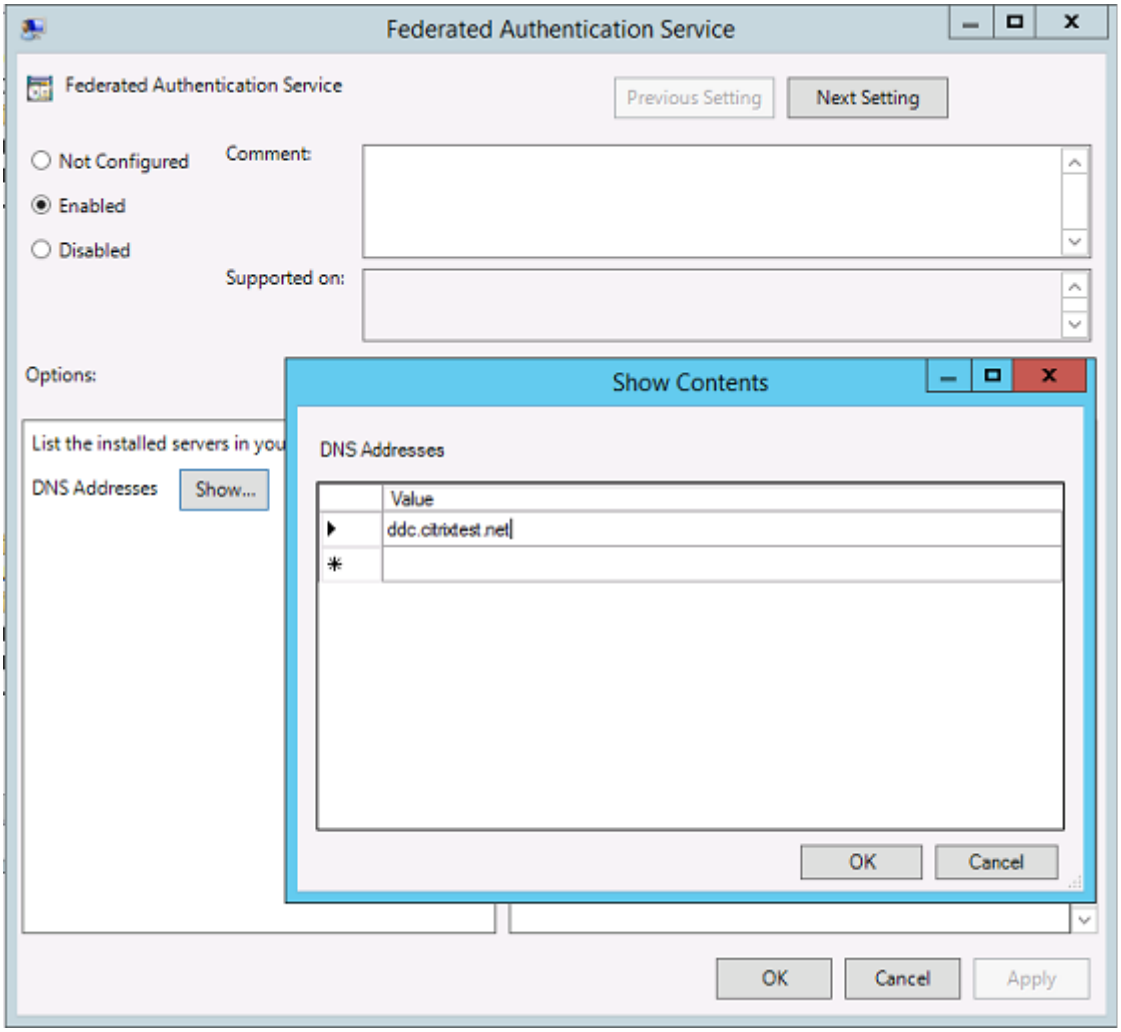
Wenn Sie nach einem Gruppenrichtlinienobjekt gefragt werden, wählen Sie **Durchsuchen** und dann **Standarddomänenrichtlinie**. Sie können auch ein für Ihre Umgebung geeignetes Richtlinienobjekt mit einem Tool Ihrer Wahl erstellen und auswählen. Die Richtlinie muss auf alle Maschinen angewendet werden, auf denen relevante Citrix Software (VDAs, StoreFront-Server, Verwaltungstools) ausgeführt wird.



Schritt 4: Gehen Sie zur Richtlinie Verbundauthentifizierungsdienst (Federated Authentication Service) unter Configuration/Policies/Administrative Templates/Citrix Components/Authentication.



Schritt 5: Öffnen Sie die Verbundauthentifizierungsdienst-Richtlinie und wählen Sie **Aktiviert**. Dadurch wird die Schaltfläche **Anzeigen** wählbar, über die Sie die DNS-Adressen der FAS-Server konfigurieren.

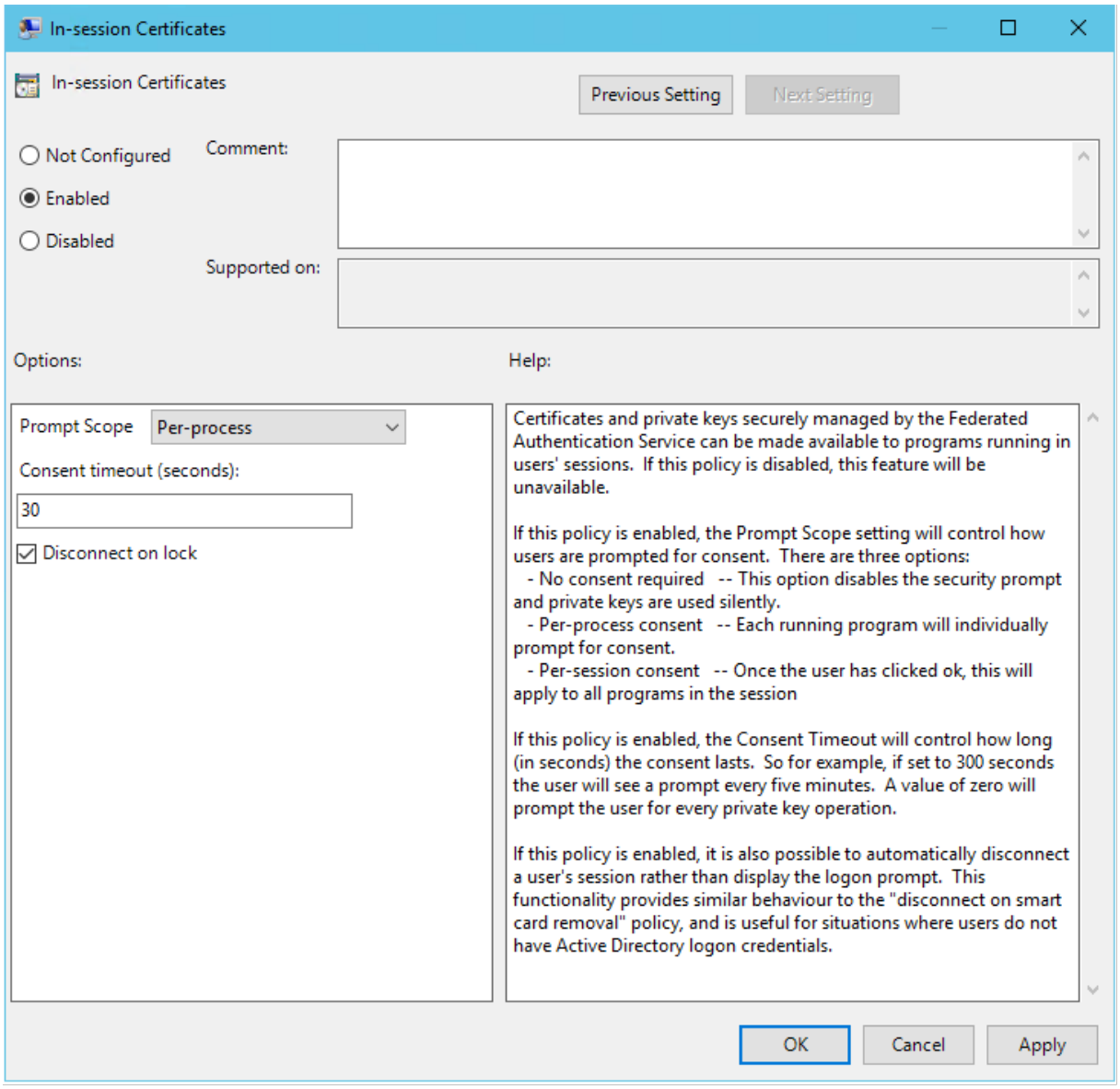


Schritt 6: Geben Sie die DNS-Adressen der Server ein, auf denen der Verbundauthentifizierungsdienst gehostet wird.

Hinweis: Wenn Sie mehrere Adressen eingeben, muss die Reihenfolge der Liste, einschließlich der leeren oder nicht verwendeten Einträge, zwischen StoreFront-Servern und VDAs übereinstimmen.

Schritt 7: Klicken Sie auf **OK**, um den Gruppenrichtlinien-Assistenten zu beenden und die Änderungen der Gruppenrichtlinie anzuwenden. Sie müssen gegebenenfalls die Maschinen neu starten oder **gpupdate /force** an der Befehlszeile ausführen, damit die Änderungen wirksam werden.

Aktivieren der Unterstützung für sitzungsinterne Zertifikate und Trennen der Verbindung beim Sperren



Unterstützung für sitzungsinterne Zertifikate Die Gruppenrichtlinienvorlage umfasst Unterstützung zur Konfiguration des Systems für sitzungsinterne Zertifikate. Damit werden Zertifikate nach der Anmeldung eines Benutzers in dessen persönlichem Zertifikatspeicher abgelegt. Ein Zertifikat kann dann beispielsweise von Internet Explorer verwendet werden, wenn innerhalb der VDA-Sitzung eine TLS-Authentifizierung bei Webservern erforderlich ist. Standardmäßig gestatten VDAs keinen Zugriff auf Zertifikate nach der Anmeldung.

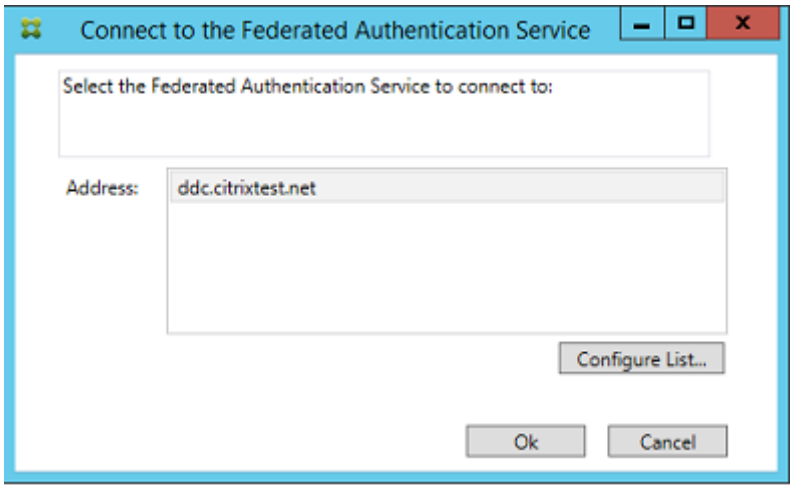
Disconnect on lock Wenn diese Richtlinie aktiviert ist, wird die Sitzung des Benutzers automatisch getrennt, wenn der Bildschirm gesperrt wird. Dieses Verhalten ähnelt der Richtlinie "Trennen beim Entfernen von Smartcards"und ist nützlich, wenn Benutzer keine Active Directory-Anmeldeinformationen haben.

> **Hinweis:**
>
> Die Richtlinie zum Trennen der Verbindung beim Sperren gilt für alle Sitzungen auf dem VDA.

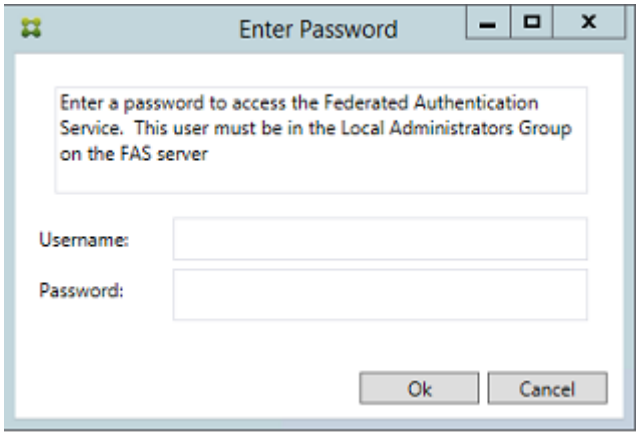
Verwendung der FAS-Verwaltungskonsole

Die FAS-Verwaltungskonsole wird zusammen mit dem Verbundauthentifizierungsdienst installiert. Ein Symbol (Citrix Verbundauthentifizierungsdienst) wird in das Startmenü eingefügt.

Es wird automatisch versucht, die FAS-Server in der Umgebung mithilfe der Gruppenrichtlinie zu lokalisieren. Wenn der Vorgang fehlschlägt, konsultieren Sie den Abschnitt Gruppenrichtlinie konfigurieren.



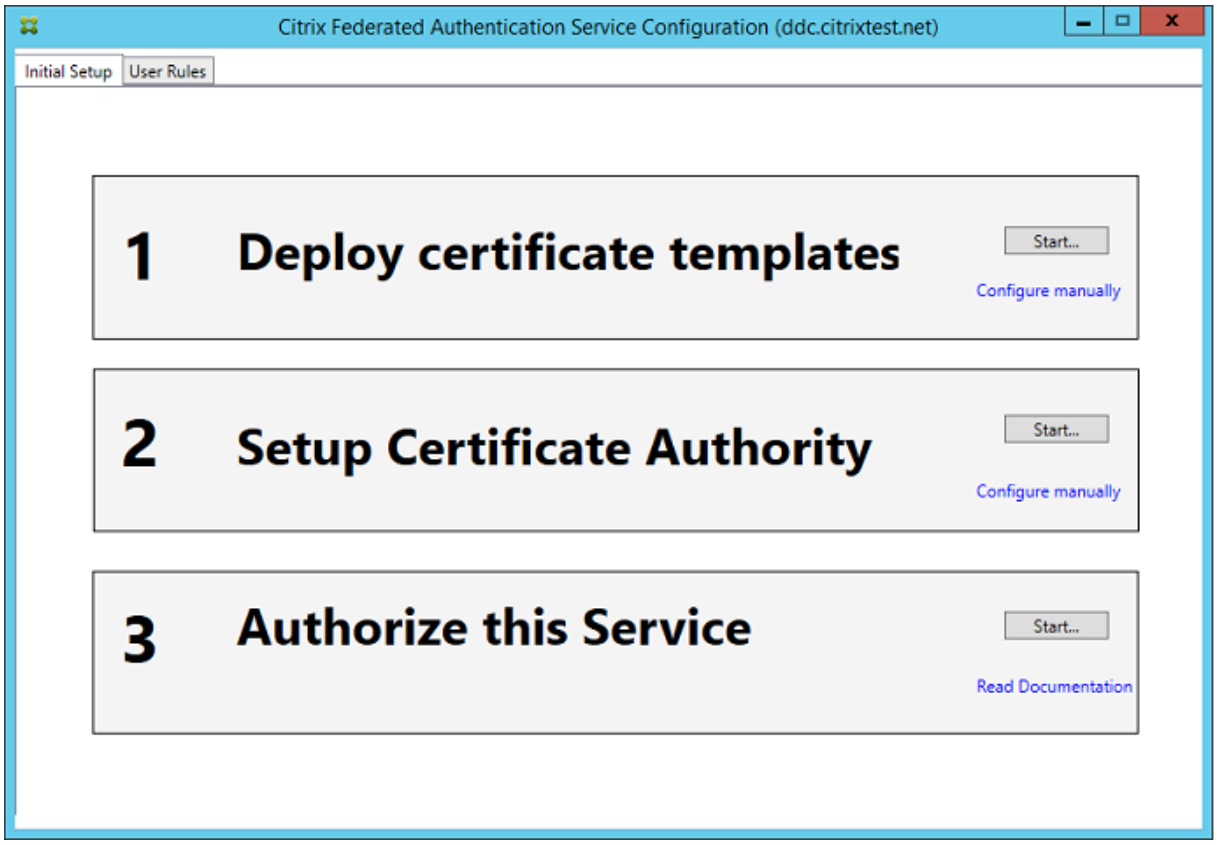
Wenn Ihr Benutzerkonto nicht Mitglied der Administratorengruppe auf dem Computer mit dem Verbundauthentifizierungsdienst ist, werden Sie zur Eingabe von Anmeldeinformationen aufgefordert.



Wenn Sie die Verwaltungskonsole zum ersten Mal verwenden, werden Sie durch einen Prozess mit den drei folgenden Schritten geführt:

- Zertifikatvorlagen bereitstellen.
- Zertifizierungsstelle einrichten.
- Zertifizierungsstelle für den Verbundauthentifizierungsdienst autorisieren.

Sie können die Konfigurationstools des Betriebssystems verwenden, um einige der Schritte manuell auszuführen.

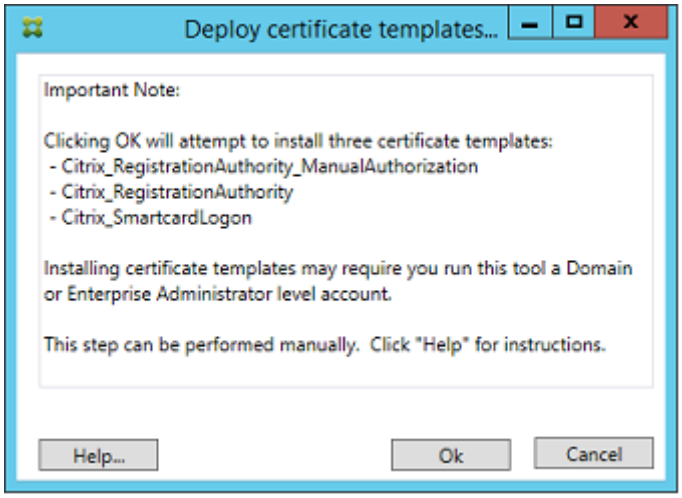


Zertifikatvorlagen bereitstellen

Zur Vermeidung von Interoperabilitätsproblemen mit anderer Software bietet Citrix Verbundauthentifizierungsdienst drei eigene Zertifikatvorlagen.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Diese Vorlagen müssen bei einem Active Directory registriert sein. Wenn sie von der Konsole nicht gefunden werden, können Sie sie mit dem Tool **Deploy certificate templates** installieren. Dieses Tool muss mit einem Konto ausgeführt werden, das Administratorberechtigung für die Gesamtstruktur des Unternehmens hat.



Die Konfiguration der Vorlagen ist in den XML-Dateien mit der Erweiterung “certificatetemplate”. Diese werden mit dem Verbundauthentifizierungsdienst in folgenden Pfad installiert:

C:\Programme\Citrix\Federated Authentication Service\CertificateTemplates

Wenn Sie keine Berechtigung zum Installieren dieser Vorlagendateien haben, geben Sie sie dem Active Directory-Administrator.

Zur manuellen Installation der Vorlagen können Sie die folgenden PowerShell-Befehle verwenden:

```
```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")

 $CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService

 $CertEnrol.InitializeImport($template)

 $comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
```

 
```

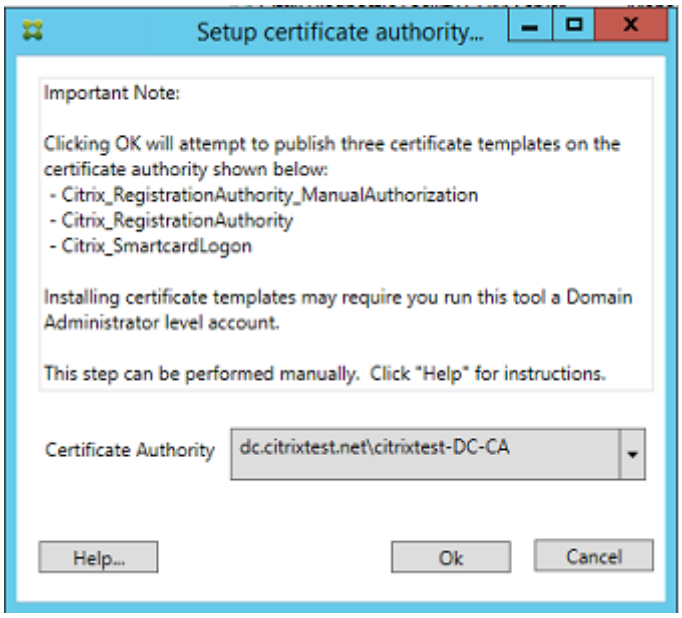
```
9  $writabletemplate = New-Object -ComObject X509Enrollment.
       CX509CertificateTemplateADWritable
10
11  $writabletemplate.Initialize($comtemplate)
12
13  $writabletemplate.Commit(1, $NULL)
14  <!--NeedCopy--> ```
```

Active Directory-Zertifikatdienste einrichten

Nachdem Sie die Citrix Zertifikatsvorlagen installiert haben, müssen Sie sie auf mindestens einem Zertifizierungsstellenserver veröffentlichen. Informationen zur Bereitstellung von Active Directory-Zertifikatdienste finden Sie in der Dokumentation von Microsoft.

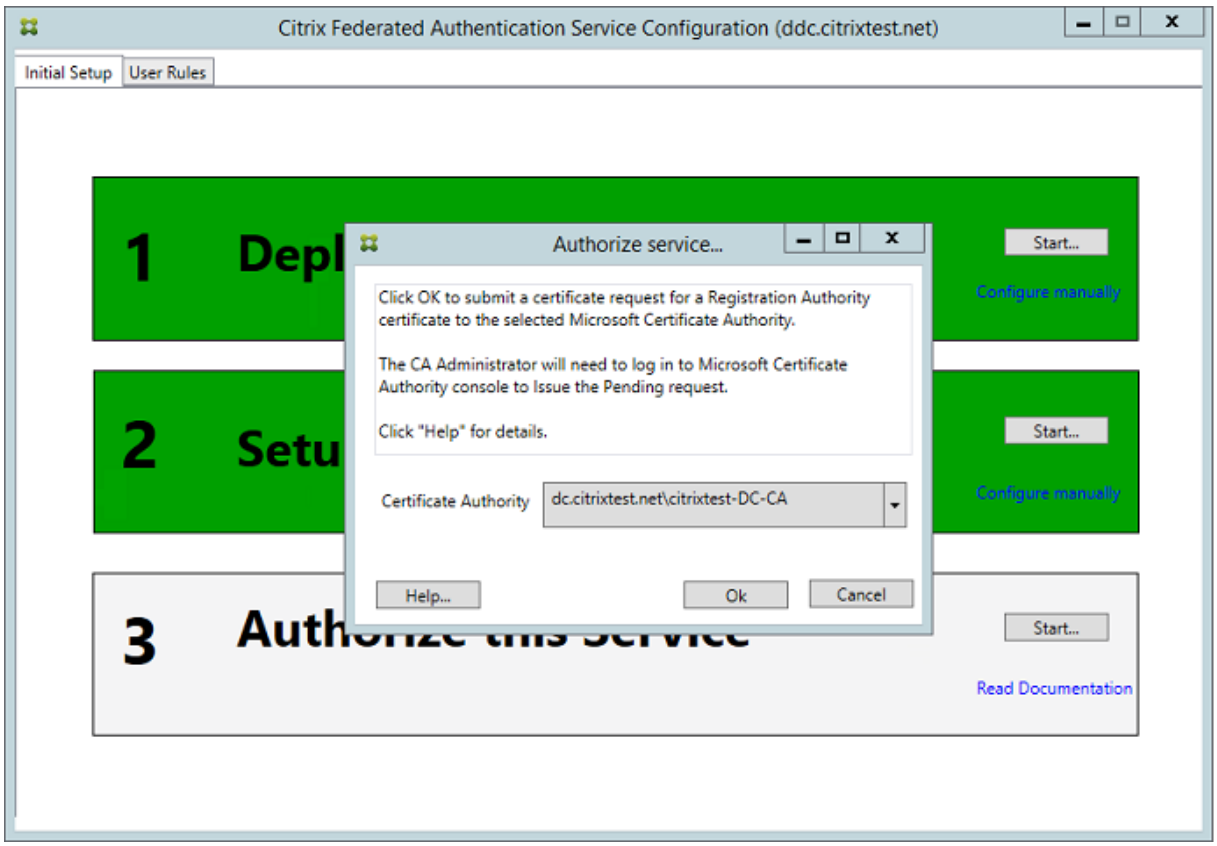
Wenn die Vorlagen nicht auf mindestens einem Server veröffentlicht sind, bietet das **Tool zum Einrichten der Zertifizierungsstelle** an, sie zu veröffentlichen. Sie müssen das Tool als Benutzer mit Berechtigung zum Verwalten der Zertifizierungsstelle ausführen.

(Zertifikatvorlagen können auch mit der Microsoft-Zertifizierungsstellenkonsole veröffentlicht werden.)

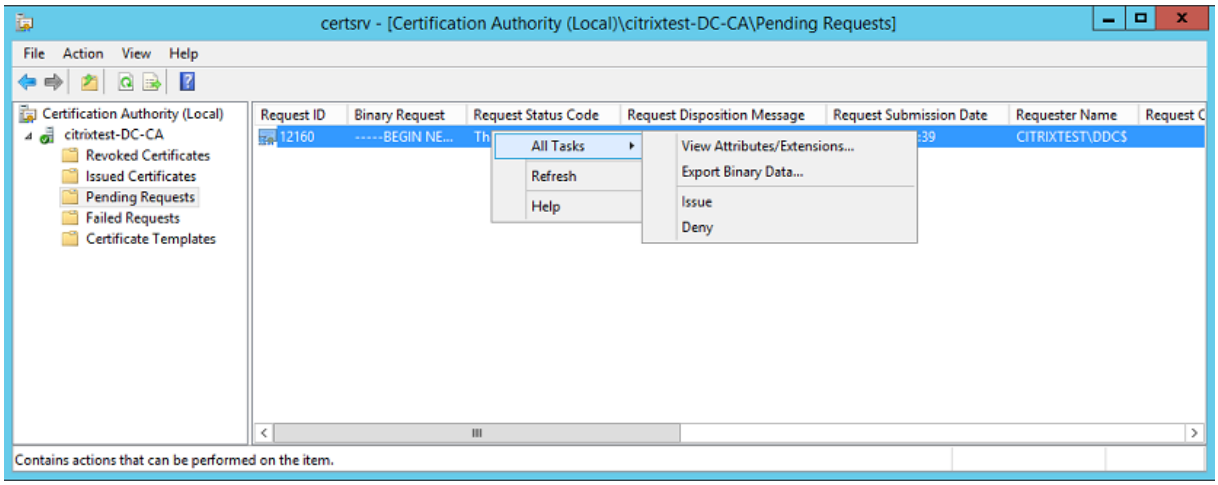


Verbundauthentifizierungsdienst autorisieren

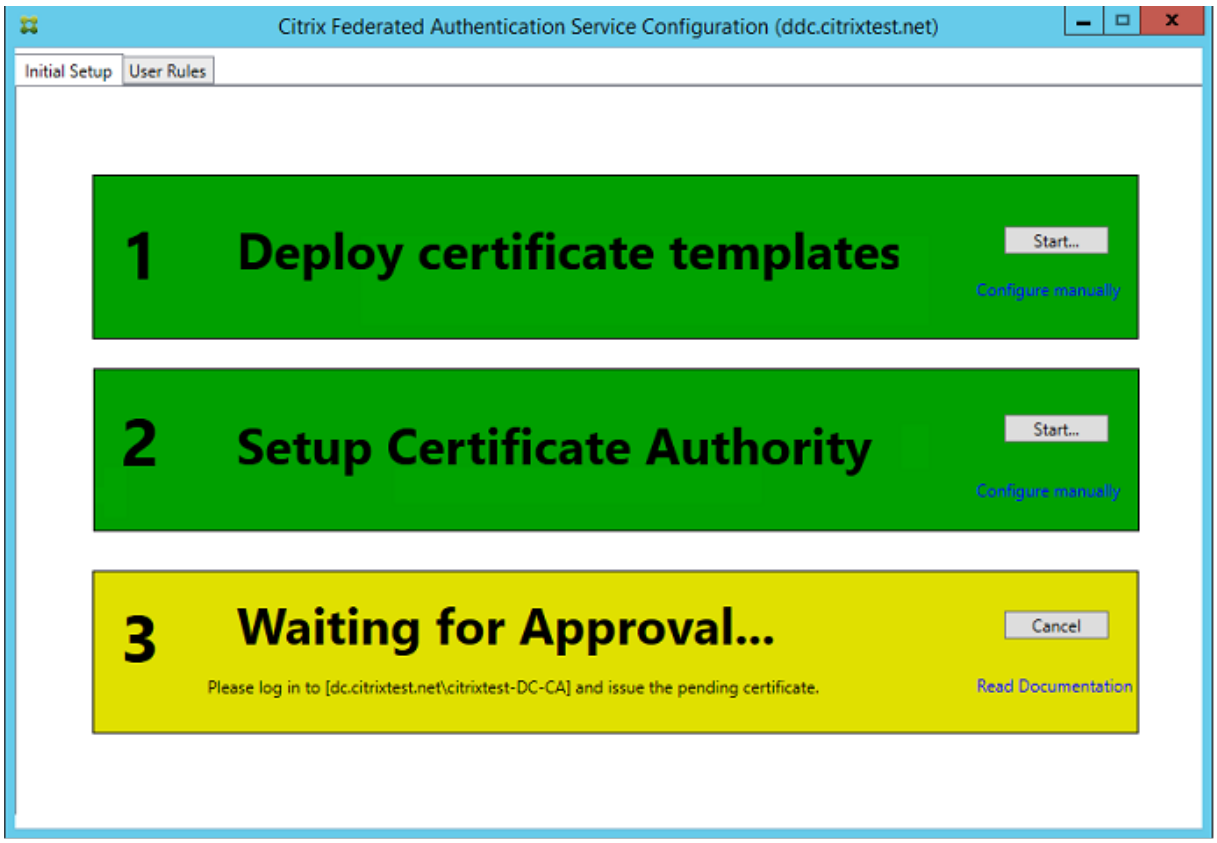
Der letzte Schritt bei der Einrichtung über die Konsole ist die Autorisierung des Verbundauthentifizierungsdiensts. Die Verwaltungskonsole verwendet die Vorlage Citrix_RegistrationAuthority_ManualAuthoriza
um eine Zertifikatanforderung zu generieren. Anschließend wird die Anforderung an eine der Zertifizierungsstellen gesendet, die die Vorlage veröffentlicht.



Nachdem die Anforderung gesendet wurde, wird sie in der Liste **Ausstehende Anforderungen** der Microsoft-Zertifizierungsstellenkonsole angezeigt. Der Administrator der Zertifizierungsstelle muss die Anforderung **ausstellen** oder **ablehnen**, damit die Konfiguration des Verbundauthentifizierungsdiensts fortgesetzt werden kann. Die Autorisierungsanforderung wird als **ausstehende Anforderung** des FAS-Computerkontos angezeigt.



Klicken Sie mit der rechten Maustaste auf **Alle Tasks** und wählen Sie für die Zertifikatanforderung **Ausstellen** oder **Verweigern**. Die FAS-Verwaltungskonsole erkennt automatisch, wenn dieser Prozess abgeschlossen ist. Dieser Schritt kann einige Zeit dauern.

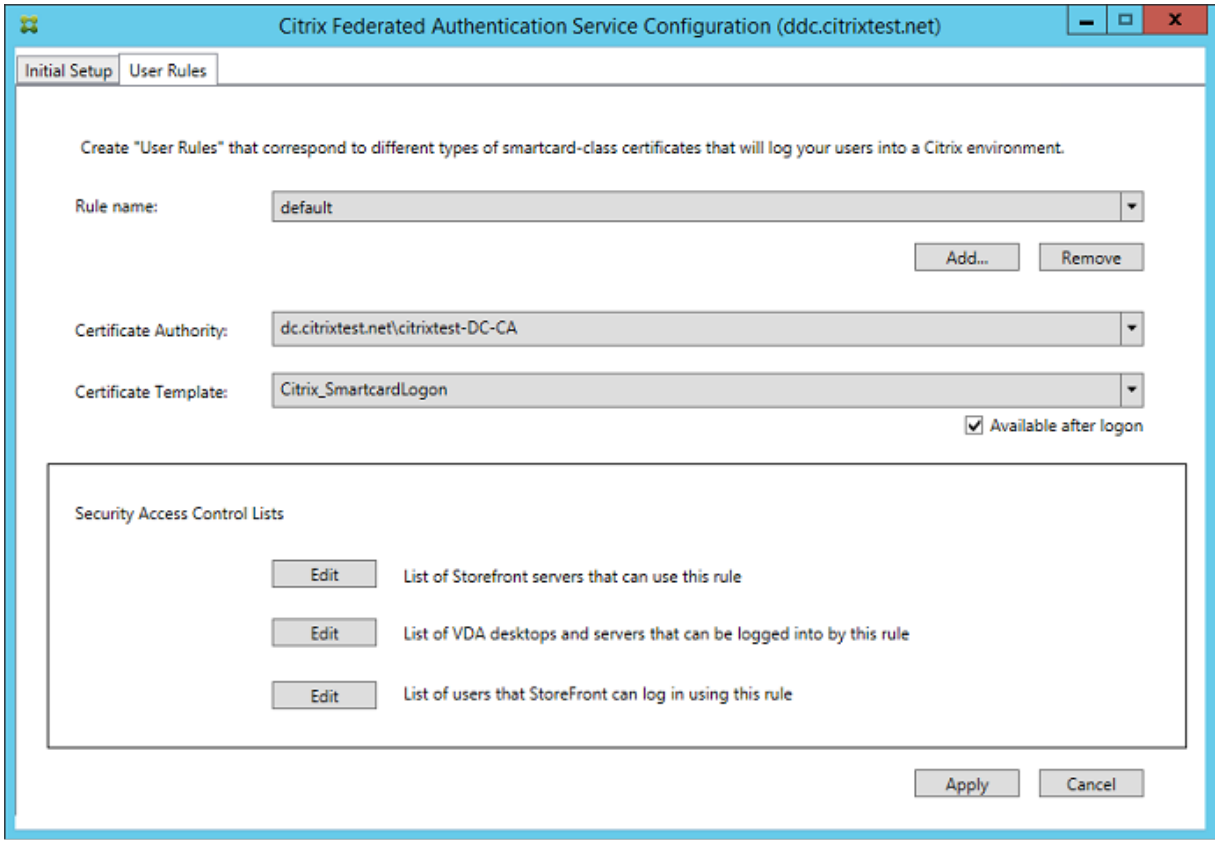


Konfigurieren von Benutzerregeln

Mit Benutzerregeln wird die Ausstellung von Zertifikaten für VDA-Anmeldungen und -Sitzungen nach Vorgabe von StoreFront autorisiert. Jede Regel spezifiziert Folgendes:

- StoreFront-Server, denen das Anfordern von Zertifikaten vertraut wird.
- Gruppe von Benutzern, für die Sie die Zertifikate anfordern können.
- Gruppe von VDA-Maschinen, die die Zertifikate verwenden dürfen.

Der Administrator muss die Standardregel definieren, um die Einrichtung des Verbundauthentifizierungsdienstes abzuschließen.
Um die Standardregel zu definieren, wechseln Sie zur Registerkarte **User Rules** der FAS-Verwaltungskonsole, wählen Sie eine Zertifizierungsstelle aus, in der die Vorlage Citrix_SmartcardLogon veröffentlicht wird, und bearbeiten Sie die Liste der StoreFront-Server. Die Liste der VDAs enthält standardmäßig die Domänencomputer und die Liste der Benutzer die Domänenbenutzer. Die Listen können geändert werden, wenn sie nicht geeignet sind.



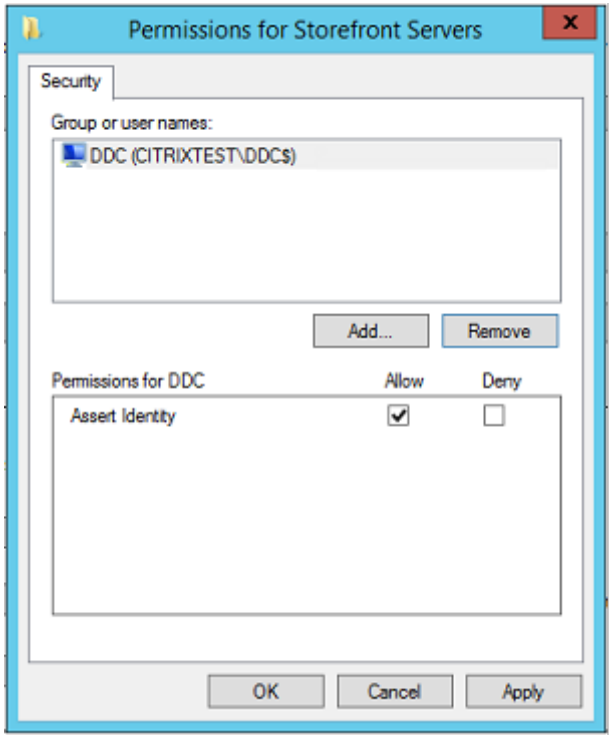
Felder:

Certificate Authority und Certificate Template: Die Zertifizierungsstelle und Zertifikatvorlage, die zum Ausstellen von Benutzerzertifikaten verwendet wird. Die Vorlage muss "Citrix_SmartcardLogon" oder eine geänderte Kopie dieser Vorlage für eine der Zertifizierungsstellen sein, in der die Vorlage veröffentlicht ist.

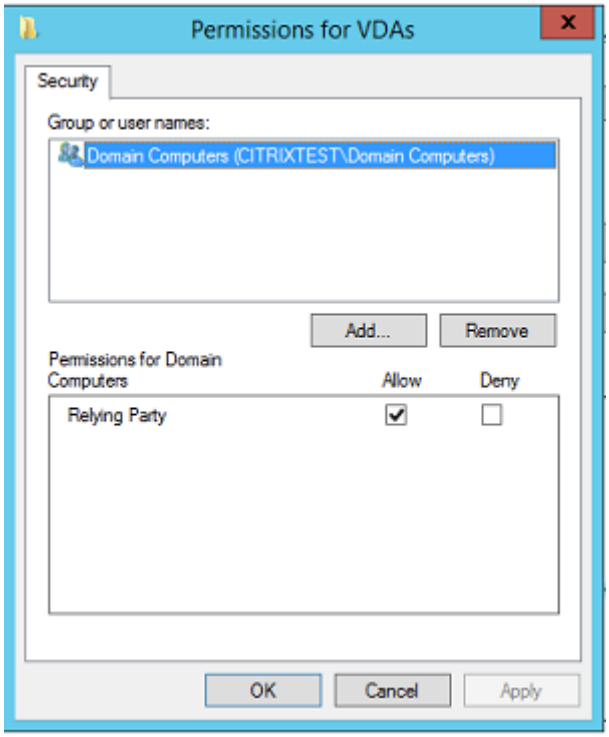
Für Failover und Lastausgleich können mehrere Zertifizierungsstellen mit PowerShell-Befehlen hinzugefügt werden. Erweiterte Optionen für die Zertifikaterstellung können über die Befehlszeile und die Konfigurationsdateien festgelegt werden. Weitere Informationen finden Sie in den Abschnitten PowerShell und Hardwaresicherheitsmodule.

In-Session Certificates: Das Kontrollkästchen **Available after logon** steuert, ob ein Zertifikat auch als sitzungsinternes Zertifikat verwendet werden kann. Wenn das Kontrollkästchen nicht aktiviert ist, wird das Zertifikat nur für Anmeldungen oder Wiederverbindungen verwendet und der Benutzer hat nach der Authentifizierung keinen Zugriff auf das Zertifikat.

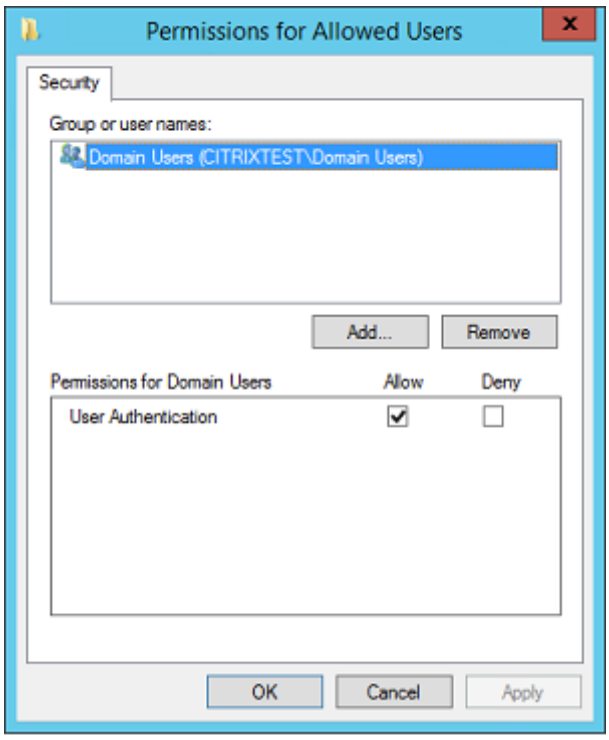
List of StoreFront servers that can use this rule: Liste der vertrauenswürdigen StoreFront-Servermaschinen, die Zertifikate für die Anmeldung oder Wiederverbindung von Benutzern anfordern dürfen. Diese Einstellung ist sicherheitsrelevant und muss mit großer Sorgfalt gewählt werden.



List of VDA desktops and servers that can be logged into by this rule: Liste der VDA-Maschinen, die Benutzer über das FAS-System anmelden dürfen.



List of users that StoreFront can log in using this rule: Liste der Benutzer, denen Zertifikate über den FAS ausgestellt werden dürfen.



Erweiterte Verwendung

Sie können zusätzliche Regeln erstellen, um auf verschiedene Zertifikatvorlagen und Zertifizierungsstellen zu verweisen und für sie unterschiedliche Eigenschaften und Berechtigungen zu konfigurieren. Sie können diese Regeln für die Verwendung durch verschiedene StoreFront-Server konfigurieren. Konfigurieren Sie die StoreFront-Server so, dass die benutzerdefinierte Regel über den Namen angefordert wird. Verwenden Sie dazu die Konfigurationsoptionen für die Gruppenrichtlinien.

Standardmäßig fordert StoreFront-Anforderungen bei der Kontaktaufnahme mit dem Verbundauthentifizierungsdienst **default** an. Dies kann über die Optionen zur Konfiguration der Gruppenrichtlinie geändert werden.

Zum Erstellen einer Zertifikatvorlage kopieren Sie die Vorlage "Citrix_SmartcardLogon"in der Microsoft-Zertifizierungsstellenkonsole, benennen Sie sie um (z. B. in "Citrix_SmartcardLogon2") und bearbeiten Sie sie nach Bedarf. Erstellen Sie eine Benutzerregel, indem Sie auf **Add** klicken, um auf die neue Zertifikatvorlage zu verweisen.

Überlegungen zu Upgrades

- Alle Servereinstellungen des Verbundauthentifizierungsdiensts bleiben erhalten, wenn Sie ein direktes Upgrade durchführen.

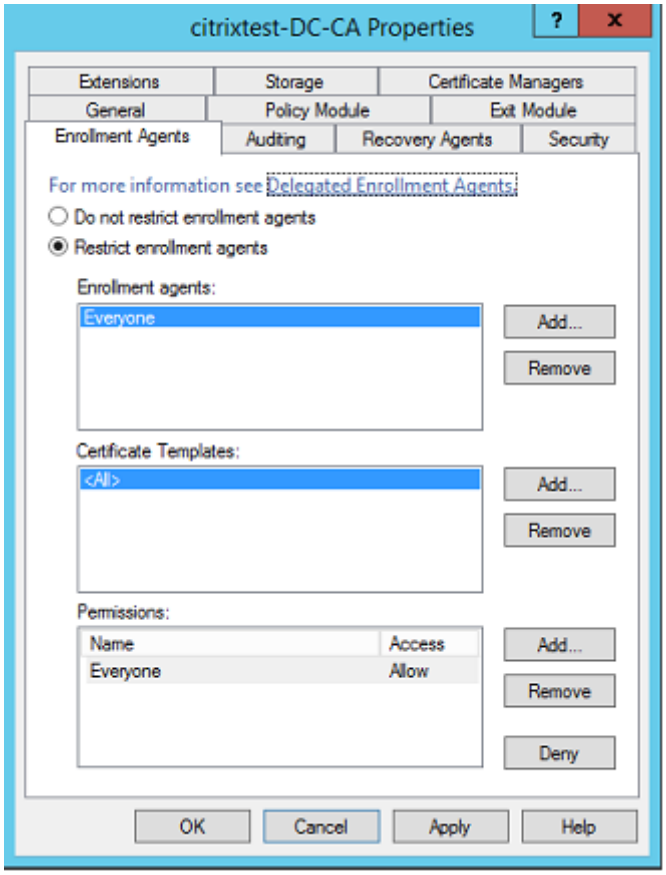
- Führen Sie zum Upgrade des Verbundauthentifizierungsdiensts das Installationsprogramm für XenApp und XenDesktop aus.
- Führen Sie vor dem Upgrade des Verbundauthentifizierungsdiensts von 7.15 LTSR auf 7.15 LTSR CU2 (bzw. ein aktuelleres unterstütztes CU) ein Upgrade des Controllers und der VDAs (sowie anderer Kernkomponenten) auf die erforderliche Version durch.
- Vergewissern Sie sich, dass die Konsole des Verbundauthentifizierungsdiensts geschlossen ist, bevor Sie den Dienst aktualisieren.
- Stellen Sie sicher, dass immer mindestens ein Verbundauthentifizierungsdienst-Server verfügbar ist. Wenn kein Server mit einem für den Verbundauthentifizierungsdienst aktivierten StoreFront-Server erreichbar ist, können die Benutzer sich nicht anmelden und keine Anwendungen starten.

Sicherheitsüberlegungen

Der Verbundauthentifizierungsdienst hat ein Registrierungsstellenzertifikat, mit dem er autonom Zertifikate für die Domänenbenutzer ausstellen kann. Es ist daher wichtig, eine Sicherheitsrichtlinie zum Schutz des FAS-Servers zu entwickeln und zu implementieren und die zugehörigen Berechtigungen einzuschränken.

Delegierte Registrierungsagents

FAS stellt Benutzerzertifikate als Registrierungsagent aus. Die Microsoft-Zertifizierungsstelle steuert die Vorlagen, die der FAS-Server verwenden kann. Sie bestimmt auch die Benutzer, für die der FAS-Server Zertifikate ausstellen kann.



Citrix empfiehlt dringend, diese Optionen zu konfigurieren, damit der Verbundauthentifizierungsdienst nur den beabsichtigten Benutzern Zertifikate ausstellen kann. Es empfiehlt sich beispielsweise, eine Ausstellung von Zertifikaten durch den Verbundauthentifizierungsdienst für Benutzer in der Verwaltungsgruppe oder der Gruppe der geschützten Benutzer zu unterbinden.

Zugriffssteuerungsliste konfigurieren

Wie unter Benutzerrollen konfigurieren beschrieben, müssen Sie eine Liste von StoreFront-Servern konfigurieren, die als vertrauenswürdig gelten und bei der Ausstellung von Zertifikaten dem Verbundauthentifizierungsdienst Benutzeridentitäts-Assertions erstellen dürfen. Sie können außerdem festlegen, welchen Benutzern Zertifikate ausgestellt werden dürfen und bei welchen VDA-Maschinen sie sich authentifizieren können. Dieser Schritt versteht sich zusätzlich zu den von Ihnen konfigurierten Active Directory- bzw. Zertifizierungsstellen-Standardsicherheitsfeatures.

Firewalleinstellungen

Für die gesamte Kommunikation mit FAS-Servern werden gegenseitig authentifizierte Kerberos-Netzwerkverbindungen gemäß Windows Communication Foundation über Port 80 verwendet.

Ereignisprotokollüberwachung

Der Verbundauthentifizierungsdienst und der VDA schreiben Informationen in das Windows-Ereignisprotokoll. Dieses Protokoll kann zur Überwachung und Überprüfung verwendet werden. Der Abschnitt Ereignisprotokolle enthält eine Liste möglicher Ereignisprotokolleinträge.

Hardwaresicherheitsmodule

Alle privaten Schlüssel, einschließlich der Schlüssel der vom Verbundauthentifizierungsdienst ausgestellten Benutzerzertifikate, werden als nicht exportierbare private Schlüssel vom Netzwerkdienstkonto gespeichert. Der Verbundauthentifizierungsdienst unterstützt die Verwendung eines kryptographischen Hardwaresicherheitsmoduls, sollte eine Sicherheitsrichtlinie dies erfordern.

Eine detaillierte Kryptographiekonfiguration ist über die Datei FederatedAuthenticationService.exe.config verfügbar. Diese Einstellungen gelten für die Ersterstellung privater Schlüssel. Daher können verschiedene Einstellungen für private Registrierungsstellenschlüssel (z. B. 4096 Bit, TPM-geschützt) und Laufzeit-Benutzerzertifikate verwendet werden.

Parameter	Beschreibung
ProviderLegacyCsp	Bei der Einstellung “true”verwendet der FAS die Microsoft CryptoAPI (CAPI). Andernfalls verwendet der FAS die Microsoft Cryptography Next Generation-API (CNG).
ProviderName	Name des CAPI- oder CNG-Anbieters, der verwendet werden soll.
ProviderType	Bezieht sich auf Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Muss immer 24 lauten, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Hersteller hat eine andere Spezifikation.
KeyProtection	Steuert das Flag “Exportable”privater Schlüssel. Ermöglicht außerdem die Verwendung eines TPM-Schlüsselspeichers (Trusted Platform Module), wenn die Hardware dies unterstützt.
KeyLength	Schlüssellänge privater RSA-Schlüssel. Zulässige Werte sind 1024, 2048 und 4096 (Standard = 2048).

PowerShell SDK

Die Verwaltungskonsole des Verbundauthentifizierungsdiensts eignet sich für einfache Bereitstellungen, während die PowerShell erweiterte Optionen bietet. Wenn Sie mit Optionen arbeiten, die in der Konsole nicht verfügbar sind, empfiehlt Citrix, ausschließlich PowerShell für die Konfiguration zu verwenden.

Mit dem folgenden Befehl werden die PowerShell-Cmdlets hinzugefügt:

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Verwenden Sie **Get-Help** <*cmdlet name*>, um die Cmdlet-Hilfe anzuzeigen. Die folgende Tabelle enthält einige Befehle, wobei * für das standardmäßige PowerShell-Verb (New, Get, Set, Remove usw.) steht.

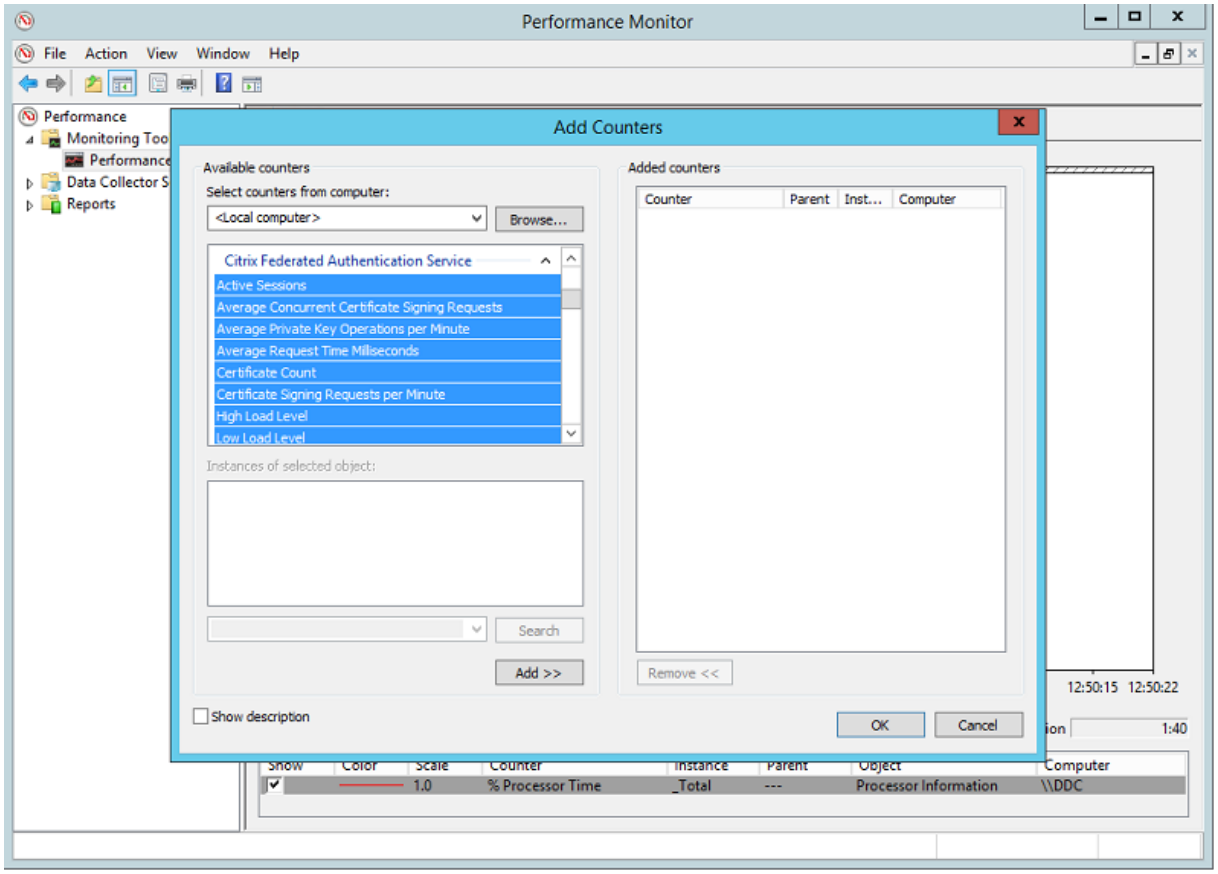
Befehle	Übersicht
*-FasServer	Zum Auflisten und Umkonfigurieren der FAS-Server in der aktuellen Umgebung
*-FasAuthorizationCertificate	Zum Verwalten des Registrierungsstellenzertifikats
*-FasCertificateDefinition	Zum Steuern der Parameter, die vom FAS beim Generieren von Zertifikaten verwendet werden
*-FasRule	Zum Verwalten der für den Verbundauthentifizierungsdienst konfigurierten Benutzerregeln
*-FasUserCertificate	Zum Auflisten und Verwalten der vom Verbundauthentifizierungsdienst zwischengespeicherten Zertifikate

PowerShell-Cmdlets können remote unter Angabe der Adresse eines FAS-Servers verwendet werden.

Sie können auch eine ZIP-Datei mit allen Cmdlet-Hilfedateien des PowerShell SDKs für FAS herunterladen. Weitere Informationen finden Sie im Artikel zum PowerShell SDK.

Leistungsindikatoren

Der Verbundauthentifizierungsdienst enthält eine Reihe von Leistungsindikatoren zur Lastnachverfolgung.



In der folgenden Tabelle werden die Leistungsindikatoren aufgelistet. Die meisten Leistungsindikatoren sind gleitende Mittelwerte über fünf Minuten.

Name	Beschreibung
Aktive Sitzungen	Anzahl der Verbindungen, die vom Verbundauthentifizierungsdienst nachverfolgt werden
Gleichzeitige CSRs	Anzahl der gleichzeitig verarbeiteten Zertifikatanforderungen
Privater-Schlüssel-Vorgänge	Anzahl der pro Minute für private Schlüssel durchgeführten Vorgänge
Request time	Länge der beim Generieren und Signieren eines Zertifikats verstrichenen Zeit
Certificate Count	Anzahl der im Verbundauthentifizierungsdienst zwischengespeicherten Zertifikate
CSR per minute	Anzahl der pro Minute verarbeiteten Zertifikatsignieranforderungen

Name	Beschreibung
Low/Medium/High	Schätzung der Last, die der Verbundauthentifizierungsdienst in Form von Zertifikatsignieranforderungen pro Minute übernehmen kann. Bei Überschreitung des Schwellenwerts für "High Load"können Sitzungsstarts fehlschlagen.

Ereignisprotokolle

Die folgenden Tabellen enthalten die vom Verbundauthentifizierungsdienst generierten Ereignisprotokolleinträge.

Verwaltungsereignisse

[Ereignisquelle: Citrix.Authentication.FederatedAuthenticationService]

FAS protokolliert diese Ereignisse als Reaktion auf die Konfigurationsänderungen auf dem FAS-Server.

Logcodes
[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group
[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]
[S003] Administrator [{0}] setting Maintenance Mode to [{1}]
[S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]
[S012] Administrator [{0}] creating certificate [upn: {0} sid: {1} role: {2}][Certificate Definition: {3}]
[S013] Administrator [{0}] deleting certificates [upn: {0} role: {1} Certificate Definition: {2}]

Logcodes
[S401] Performing configuration upgrade –[From version {0}][to version {1}]
[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]

Erstellen von Identitätsassertions [Verbundauthentifizierungsdienst]

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn von einem vertrauenswürdigen Server eine Assertion für eine Benutzeranmeldung erstellt wird.

Logcodes
[S101] Server [{0}] is not authorized to assert identities in role [{1}]
[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})
[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}
[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])
[S105] Server [{0}] issued identity assertion [upn: {0}, role {1}, Security Context: [{2}]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]
[S121] Issuing certificate to [upn: {0} role: {1}] on behalf of account {2}
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].

Bei Agieren als vertrauende Seite [Verbundauthentifizierungsdienst]

Diese Ereignisse werden zur Laufzeit auf dem FAS-Server protokolliert, wenn von einem VDA ein Benutzer angemeldet wird.

Logcodes
[S201] Relying party [{0}] does not have access to a password.
[S202] Relying party [{0}] does not have access to a certificate.
[S203] Relying party [{0}] does not have access to the Logon CSP
[S204] Relying party [{0}] accessing the Logon CSP [Operation: {1}]

Logcodes
[S205] Calling account [{0}] is not a relying party in role [{1}]
[S206] Calling account [{0}] is not a relying party
[S207] Relying party [{0}] asserting identity [upn: {1}] in role: [{2}]
[S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}].

Server für sitzungsinterne Zertifikate [Verbundauthentifizierungsdienst]

Diese Ereignisse werden auf dem FAS-Server protokolliert, wenn ein Benutzer ein sitzungsinternes Zertifikat verwendet.

Logcodes
[S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card
[S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}]
[S303] User [{0}] does not match Virtual Smart Card [upn: {1}]
[S304] User [{1}] running program [{2}] on computer [{3}] using Virtual Smart Card [upn: {4} role: {5}] for private key operation: [{6}]
[S305] Private Key operation failed [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}].

Anmeldung [VDA]

[Ereignisquelle: Citrix.Authentication.IdentityAssertion]

Diese Ereignisse werden bei der Anmeldung auf dem VDA protokolliert.

Logcodes
[S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}]
[S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}]
[S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2}
[S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}]
[S105] Identity Assertion Logon. Logging in [Username: {0}][Domain: {1}]

Logcodes
[S106] Identity Assertion Logon. Logging in [Certificate: {0}]
[S107] Identity Assertion Logon failed. [Exception: {1}{2}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

Sitzungsinterne Zertifikate [VDA]

Diese Ereignisse werden auf dem VDA protokolliert, wenn ein Benutzer versucht, ein sitzungsinternes Zertifikat zu verwenden.

Logcodes
[S201] Virtual Smart Card Authorized [User: {0}][PID: {1} Name:{2}][Certificate {3}]
[S202] Virtual Smart Card Subsystem. No smart cards available in session {0}
[S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}, expected: {2}]
[S204] Virtual Smart Card Subsystem. Smart card support disabled.

Zertifikatanforderung und Generierungscodes [Verbundauthentifizierungsdienst]

[Event Source: Citrix.TrustFabric]

Diese Detailereignisse werden protokolliert, wenn der FAS-Server kryptographische Vorgänge auf Protokollebene durchführt.

Logcodes
[S0001]TrustArea::TrustArea: Installed certificate chain
[S0002]TrustArea::Join: Callback has authorized an untrusted certificate
[S0003]TrustArea::Join: Joining to a trusted server
[S0004]TrustArea::Maintain: Renewed certificate
[S0005] Trustarea:: Maintain: Abgerufene neue Zertifikatskette
[S0006]TrustArea::Export: Exporting private key
[S0007]TrustArea::Import: Importing Trust Area
[S0008]TrustArea::Leave: Leaving Trust Area

Logcodes

[S0009]TrustArea::SecurityDescriptor: Setting Security Descriptor

[S0010]CertificateVerification: Installing new trusted certificate

[S0011]CertificateVerification: Uninstalling expired trusted certificate

[S0012]TrustFabricHttpClient: Attempting single sign-on to {0}

[S0013]TrustFabricHttpClient: Explicit credentials entered for {0}

[S0014]Pkcs10Request::Create: Created PKCS10 request

[S0015]Pkcs10Request::Renew: Created PKCS10 request

[S0016]PrivateKey::Create

[S0017]PrivateKey::Delete

[S0018]TrustArea::TrustArea: Waiting for Approval

[S0019]TrustArea::Join: Delayed Join

[S0020]TrustArea::Join: Delayed Join

[S0021]TrustArea::Maintain: Installed certificate chain

Logcodes

[S0101]TrustAreaServer::Create root certificate

[S0102]TrustAreaServer::Subordinate: Join succeeded

[S0103]TrustAreaServer::PeerJoin: Join succeeded

[S0104]MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}

[S0104]MicrosoftCertificateAuthority::SubmitCertificateRequest Error {0}

[S0105]MicrosoftCertificateAuthority::SubmitCertificateRequest Issued cert {0}

[S0106]MicrosoftCertificateAuthority::PublishCRL: Published CRL

[S0107]MicrosoftCertificateAuthority::ReissueCertificate Error {0}

[S0108]MicrosoftCertificateAuthority::ReissueCertificate Issued Cert {0}

[S0109]MicrosoftCertificateAuthority::CompleteCertificateRequest - Still waiting for approval

[S0110]MicrosoftCertificateAuthority::CompleteCertificateRequest - Pending certificate refused

[S0111]MicrosoftCertificateAuthority::CompleteCertificateRequest Issued certificate

[S0112]MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval

Logcodes
[S0120]NativeCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0121]NativeCertificateAuthority::SubmitCertificateRequest Error
[S0122]NativeCertificateAuthority::RootCARollover New root certificate
[S0123]NativeCertificateAuthority::ReissueCertificate New certificate
[S0124]NativeCertificateAuthority::RevokeCertificate
[S0125]NativeCertificateAuthority::PublishCRL

Verwandte Informationen

- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.

Übersicht über die Architekturen des Verbundauthentifizierungsdiensts

November 15, 2022

Einführung

Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ist eine Citrix Komponente zur Integration in die Active Directory-Zertifizierungsstelle (ZS), die eine nahtlose Authentifizierung der Benutzer innerhalb einer Citrix Umgebung ermöglicht. In diesem Dokument werden die verschiedenen Authentifizierungsarchitekturen beschrieben, die für diverse Bereitstellungen geeignet sind.

Wenn der FAS aktiviert ist, delegiert er die Entscheidung über die Benutzerauthentifizierung an vertrauenswürdige StoreFront-Server. StoreFront hat umfassende integrierte Authentifizierungsoptionen, die auf modernen Internet-Technologien aufbauen. Es kann problemlos mit dem StoreFront-SDK oder IIS-Plug-Ins anderer Hersteller erweitert werden. Das grundlegende Designziel besteht darin, dass jede Technologie zur Authentifizierung von Benutzern bei einer Website nun auch für die Anmeldung bei einer Citrix XenApp- oder XenDesktop-Bereitstellung verwendet werden kann.

In diesem Dokument werden die Beispiele einiger Bereitstellungsarchitekturen in der Reihenfolge zunehmender Komplexität vorgestellt.

- Interne Bereitstellung
- NetScaler Gateway-Bereitstellung
- ADFS SAML
- B2B-Kontozuordnung
- Einbindung in Azure AD unter Windows 10

Das Dokument enthält außerdem Links zu verwandten FAS-Artikeln. Für alle Architekturen gilt der Artikel Verbundauthentifizierungsdienst als primäre Referenz für das Einrichten des FAS.

Funktionsweise

Der FAS kann für Active Directory-Benutzer, die von StoreFront authentifiziert werden, automatisch Zertifikate der Smartcardklasse ausstellen. Dabei werden ähnliche APIs verwendet, wie bei Tools zum Bereitstellen physischer Smartcards.

Wenn ein Benutzer an einen Citrix XenApp- oder XenDesktop-VDA vermittelt wird, wird das Zertifikat der Maschine angehängt und die Anmeldung von der Windows-Domäne als normale Smartcardauthentifizierung behandelt.

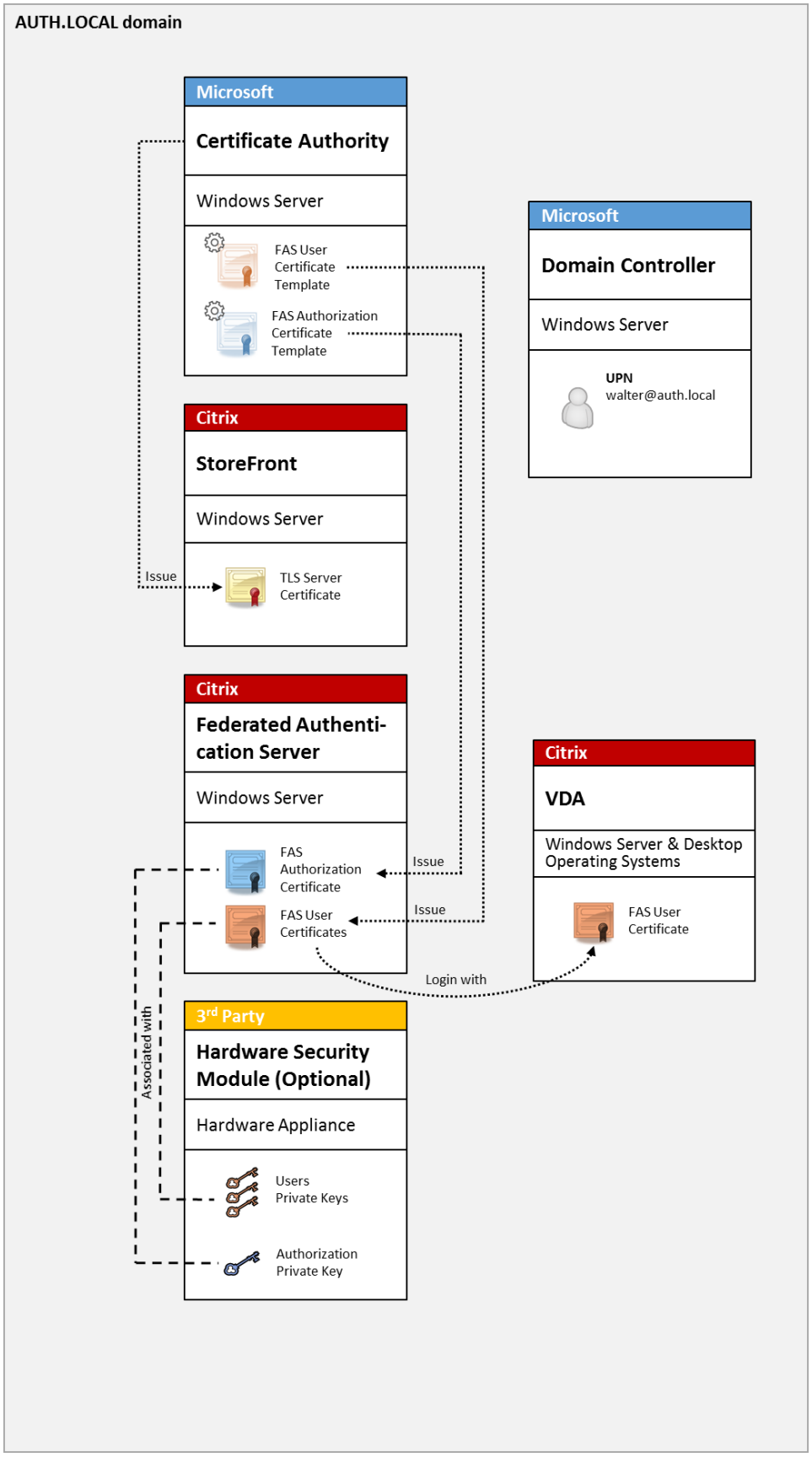
Interne Bereitstellung

Der FAS ermöglicht die sichere Authentifizierung der Benutzer bei StoreFront mit einer Reihe von Authentifizierungsoptionen, einschließlich Kerberos-Single Sign-On (SSO), und die Verbindung mit einer vollauthentifizierten Citrix HDX-Sitzung.

Dies ermöglicht die Windows-Authentifizierung ohne Aufforderungen zur Eingabe von Anmeldeinformationen oder Smartcard-PINs und ohne Verwaltung gespeicherter Kennwörter wie beim Single Sign-On-Dienst. Der Service kann die Anmeldefeatures der eingeschränkten Kerberos-Delegierung älterer Versionen von XenApp ersetzen.

Alle Benutzer haben Zugriff auf PKI-Zertifikate (Public Key-Infrastruktur) in ihrer Sitzung, unabhängig davon, ob sie sich bei Endpunktgeräten mit einer Smartcard angemeldet haben. Dies ermöglicht eine reibungslose Migration zur zweistufigen Authentifizierung, und zwar selbst bei Smartphones, Tablets und ähnlichen Geräten ohne Smartcardleser.

Bei dieser Bereitstellung gibt es einen Server, auf dem der FAS ausgeführt wird und der Zertifikate der Smartcardklasse für Benutzer ausstellen darf. Die Zertifikate werden dann zur Anmeldung bei Benutzersitzungen in einer Citrix HDX-Umgebung verwendet, die wie eine klassische Smartcard-Anmeldung verarbeitet wird.



Die XenApp- oder XenDesktop-Umgebung muss ähnlich konfiguriert werden wie für die Smartcard-Anmeldung (siehe CTX206156).

In einer bestehenden Bereitstellung muss hierfür in der Regel nur sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und den Domänencontrollern Domänencontrollerzertifikate zugewiesen wurden. (Weitere Informationen finden Sie unter CTX206156 im Abschnitt zum Ausstellen von Domänencontrollerzertifikaten .)

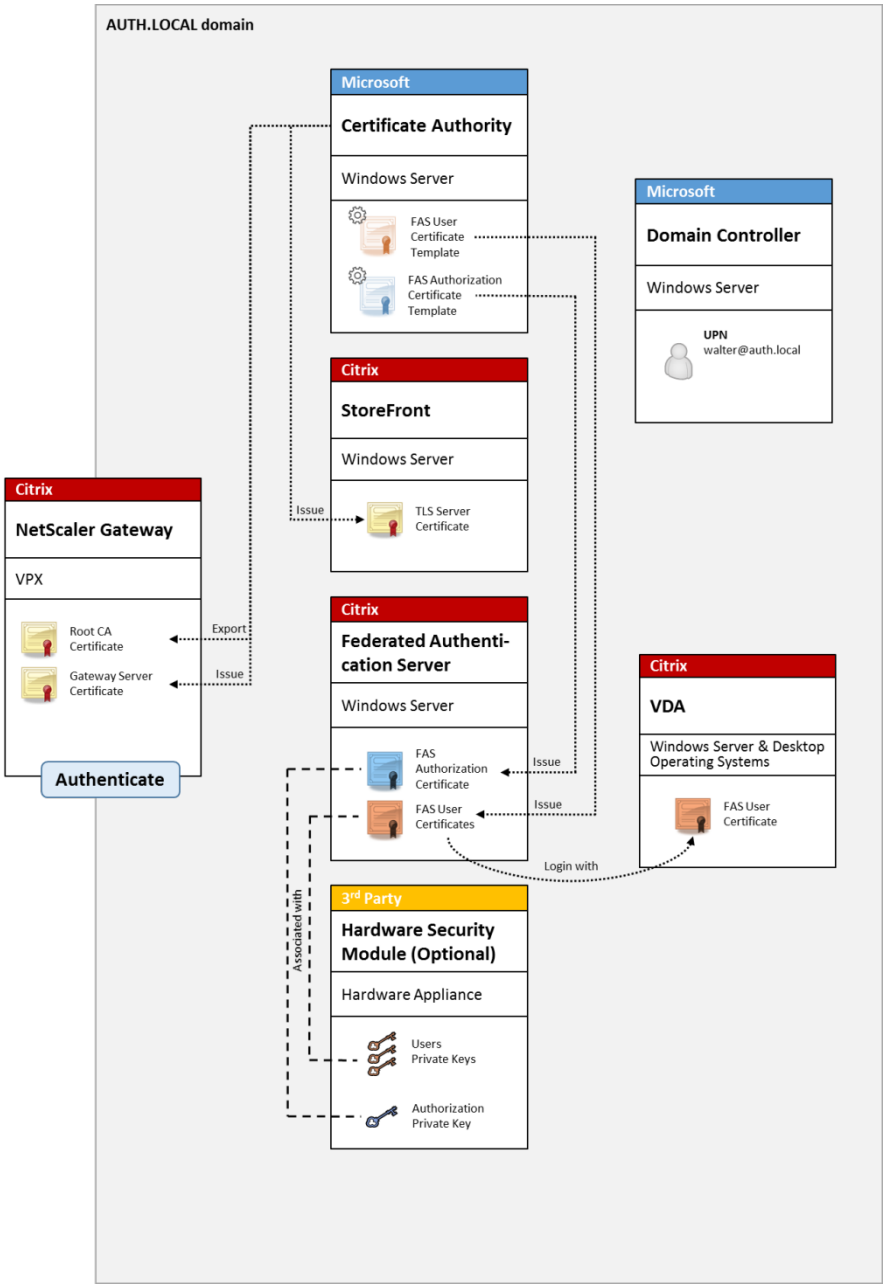
Verwandte Informationen

- Schlüssel können in einem Hardwaresicherheitsmodul (HSM) oder einem integrierten Trusted Platform Module (TPM) gespeichert werden. Weitere Informationen finden Sie unter Schutz durch private Schlüssel beim Verbundauthentifizierungsdienst.
- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.

NetScaler Gateway-Bereitstellung

Die NetScaler-Bereitstellung ähnelt der internen Bereitstellung, wobei zusätzlich ein mit StoreFront gekoppeltes Citrix NetScaler Gateway verwendet wird und die primäre Authentifizierung in NetScaler erfolgt. Citrix NetScaler bietet intelligente Optionen für Authentifizierung und Autorisierung, mit denen der Remotezugriff auf die Websites eines Unternehmens gesichert werden kann.

Diese Bereitstellung kann verwendet werden, um mehrere PIN-Eingabeaufforderungen zu vermeiden, wie sie bei der Authentifizierung bei NetScaler und anschließender Anmeldung bei einer Benutzersitzung auftreten. Außerdem können erweiterte NetScaler-Authentifizierungstechnologien ohne Active Directory-Kennwörter oder Smartcards genutzt werden.

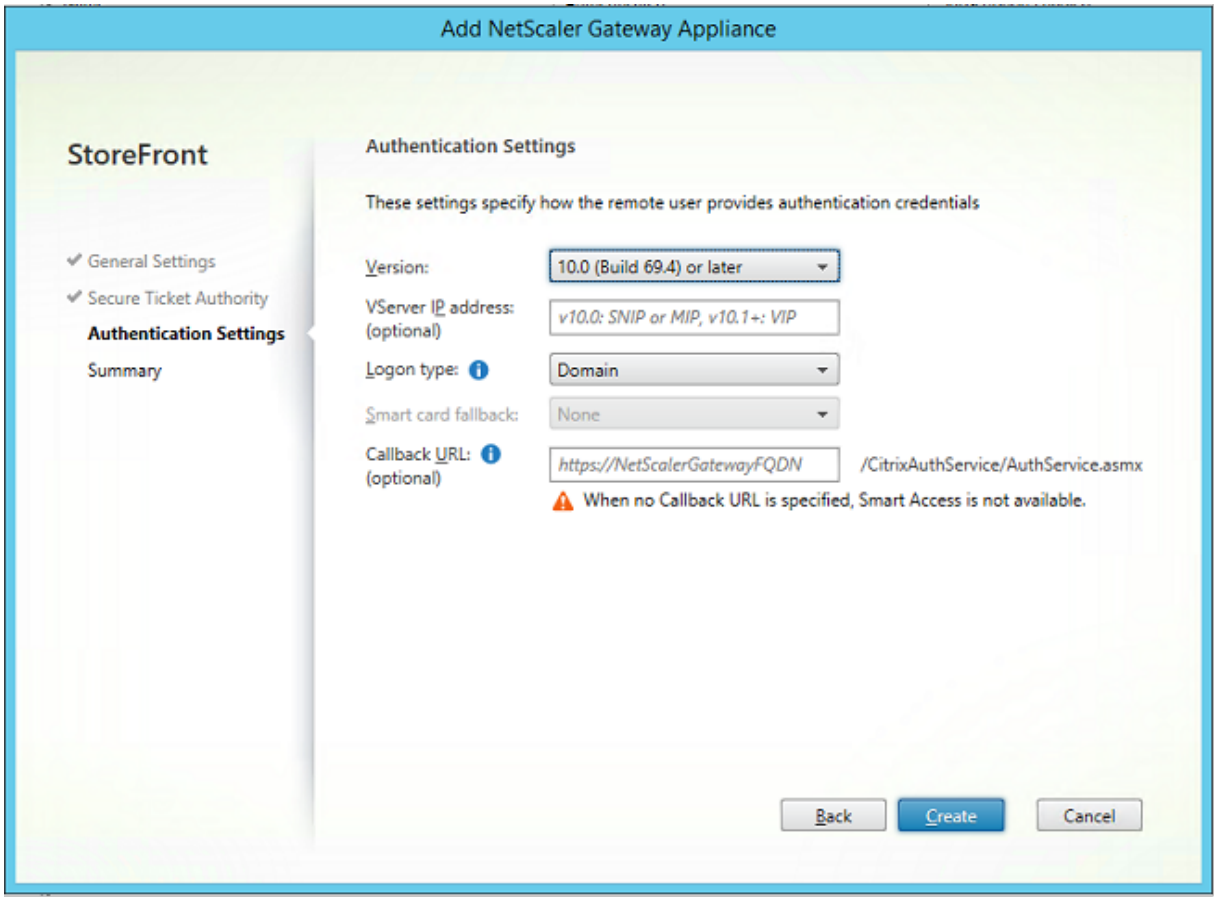


> **Hinweis:**
>
> Es macht keinen Unterschied, ob die Back-End-Ressource Windows VDA oder Linux VDA ist.

Die XenApp- oder XenDesktop-Umgebung muss ähnlich konfiguriert werden wie für die Smartcard-Anmeldung (siehe CTX206156).

In einer bestehenden Bereitstellung muss hierfür in der Regel nur sichergestellt werden, dass eine in die Domäne eingebundene Microsoft-Zertifizierungsstelle verfügbar ist und den Domänencontrollern Domänencontrollerzertifikate zugewiesen wurden. (Weitere Informationen finden Sie in dem Abschnitt zum Ausstellen von Domänencontrollerzertifikaten in CTX206156.)

Bei der Konfiguration von NetScaler als primäres Authentifizierungssystem müssen alle Verbindungen zwischen NetScaler und StoreFront mit TLS geschützt werden. Sorgen Sie vor allem dafür, dass die Callback-URL richtig auf den NetScaler-Server zeigt, denn sie kann zur Authentifizierung des NetScaler-Servers in dieser Bereitstellung verwendet werden.



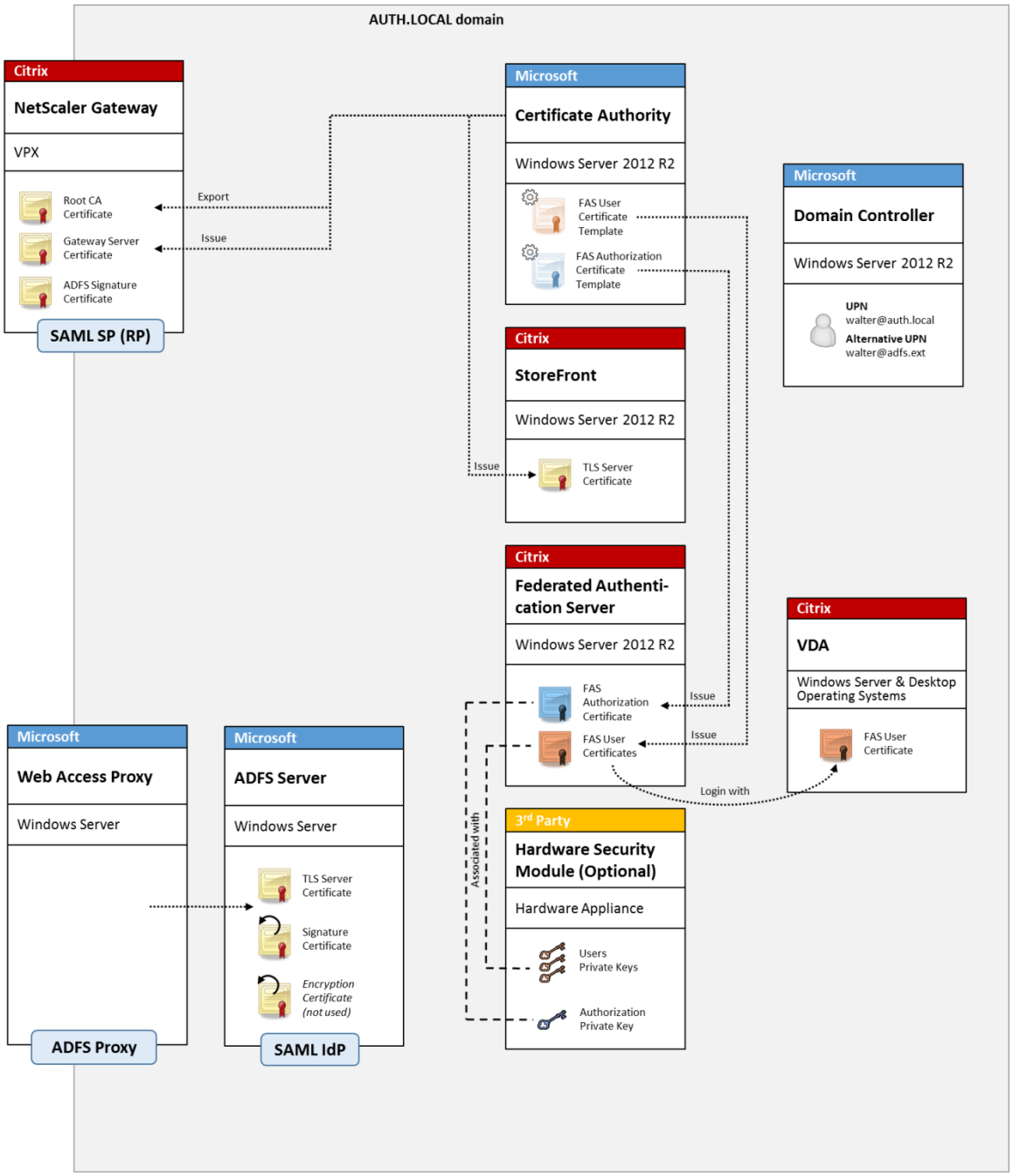
Verwandte Informationen

- Informationen zum Konfigurieren von NetScaler Gateway finden Sie unter How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and XenDesktop 7.6.
- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.

AD FS SAML-Bereitstellung

Eine wichtige NetScaler-Authentifizierungstechnologie ermöglicht die Integration in Microsoft AD FS zur Verwendung als SAML-Identitätsanbieter (IdP). Eine SAML-Assertion ist ein kryptografisch signierter XML-Block, der von einem vertrauenswürdigen IdP ausgestellt wird und einen Benutzer zur Anmeldung bei einem Computersystem autorisiert. Es bedeutet, dass der FAS-Server nun die Delegation der Authentifizierung eines Benutzers an den Microsoft AD FS-Server (oder einen anderen

SAML-fähigen IdP) gestattet.



AD FS wird häufig zur sicheren Authentifizierung von Benutzern bei Unternehmensressourcen remote über das Internet verwendet. Beispielsweise wird es häufig für die Office 365-Integration verwendet.

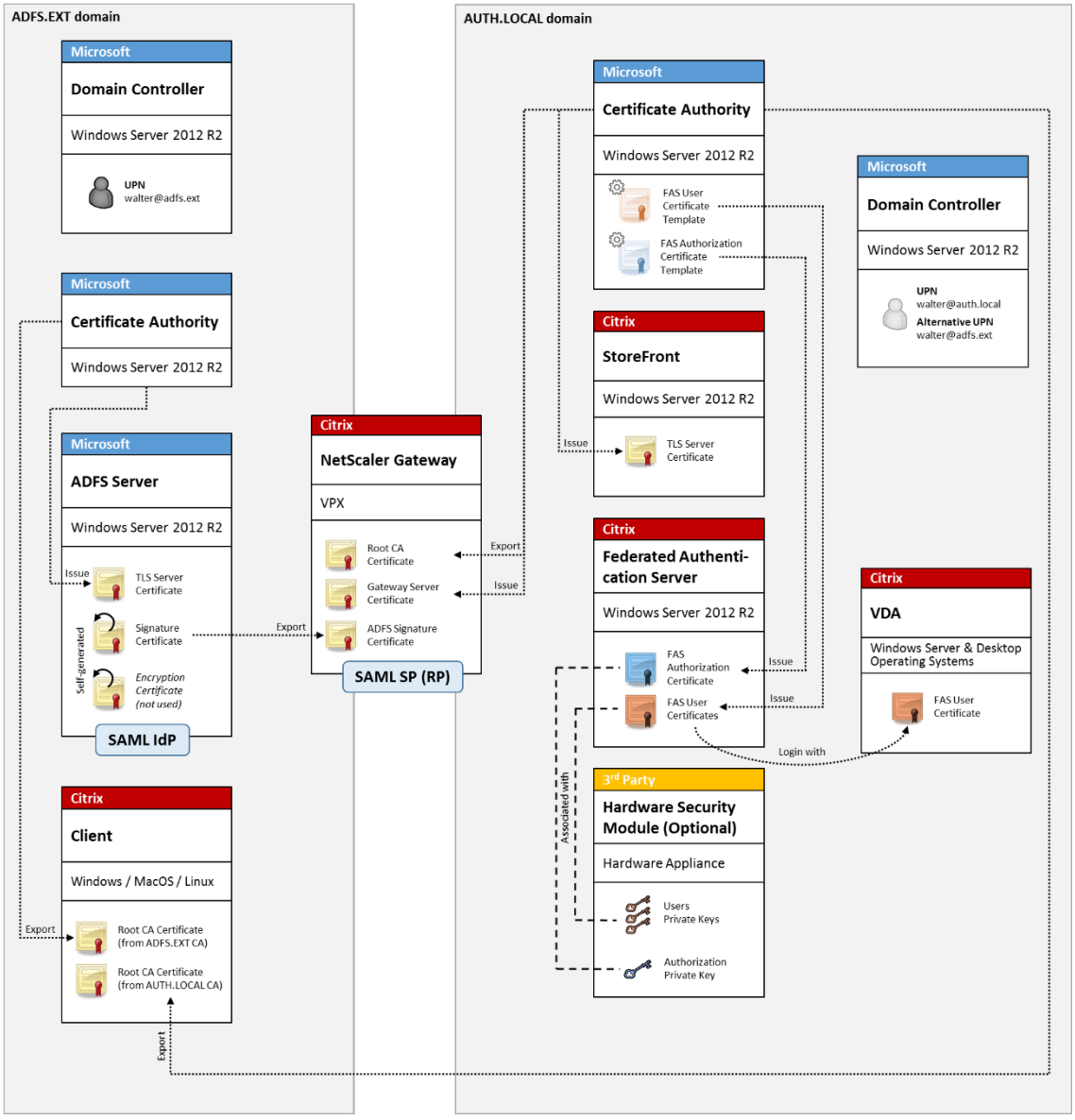
Verwandte Informationen

- Der Artikel AD FS-Bereitstellung des Verbundauthentifizierungsdiensts enthält detaillierte Informationen.

- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.
- Der Abschnitt NetScaler Gateway-Bereitstellung enthält Hinweise zur Konfiguration.

B2B-Kontozuordnung

Wenn zwei Unternehmen ihre Computersysteme gemeinsam verwenden möchten, wird häufig ein Active Directory-Verbunddienste-Server (AD FS) mit einer Vertrauensstellung eingerichtet. Dadurch können Benutzer in einem Unternehmen sich nahtlos bei dem Active Directory (AD) des zweiten authentifizieren. Bei der Anmeldung verwendet jeder Benutzer die Anmeldeinformationen für das eigene Unternehmen. AD FS ordnet dies automatisch einem "Schattenkonto"in der AD-Umgebung des Peerunternehmens zu.

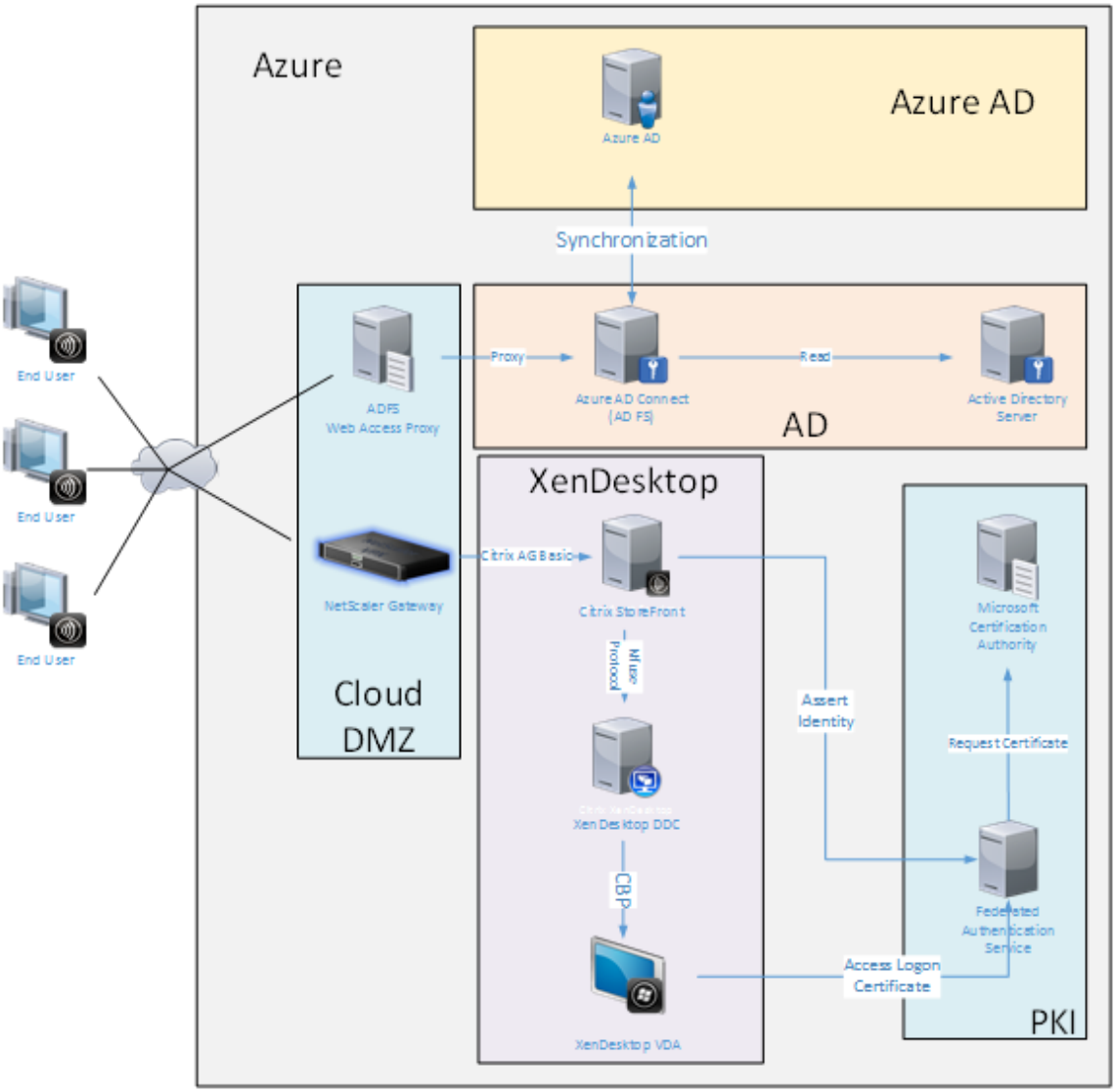


Verwandte Informationen

- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.

Einbindung in Azure AD unter Windows 10

Mit Windows 10 wurde das Konzept der Azure AD-Einbindung eingeführt. Im Konzept entspricht dies dem herkömmlichen Beitritt zu einer Windows-Domäne, zielt jedoch auf Verbindungen über das Internet ab. Es funktioniert gut mit Laptops und Tablets. Genau wie der herkömmliche Windows-Domänenbeitritt bietet Azure AD Funktionen, die Single Sign-On-Modelle für Unternehmenswebsites und -ressourcen zulassen. Diese sind allesamt Internet-fähig und können daher an jedem Standort mit Internetverbindung und nicht nur im Unternehmens-LAN verwendet werden.



Diese Bereitstellung ist ein Beispiel, bei dem das Konzept "Endbenutzer im Büro"effektiv nicht existiert. Die Registrierung und Authentifizierung von Laptops erfolgt vollständig über das Internet mit modernen Azure AD-Features.

Die Infrastruktur dieser Bereitstellung kann überall dort ausgeführt werden, wo eine IP-Adresse verfügbar ist: On-premises, bei einem Hostinganbieter, in Azure oder in einer anderen Cloud. Die Synchronisierung von Azure AD Connect stellt automatisch eine Verbindung mit Azure AD her. In der Beispielabbildung werden der Einfachheit halber Azure-VMs verwendet.

Verwandte Informationen

- Im Artikel Verbundauthentifizierungsdienst wird beschrieben, wie diese Komponente installiert und konfiguriert wird.
- Der Artikel Integration des Verbundauthentifizierungsdiensts in Azure Active Directory enthält detaillierte Informationen.

AD FS-Bereitstellung des Verbundauthentifizierungsdiensts

August 18, 2021

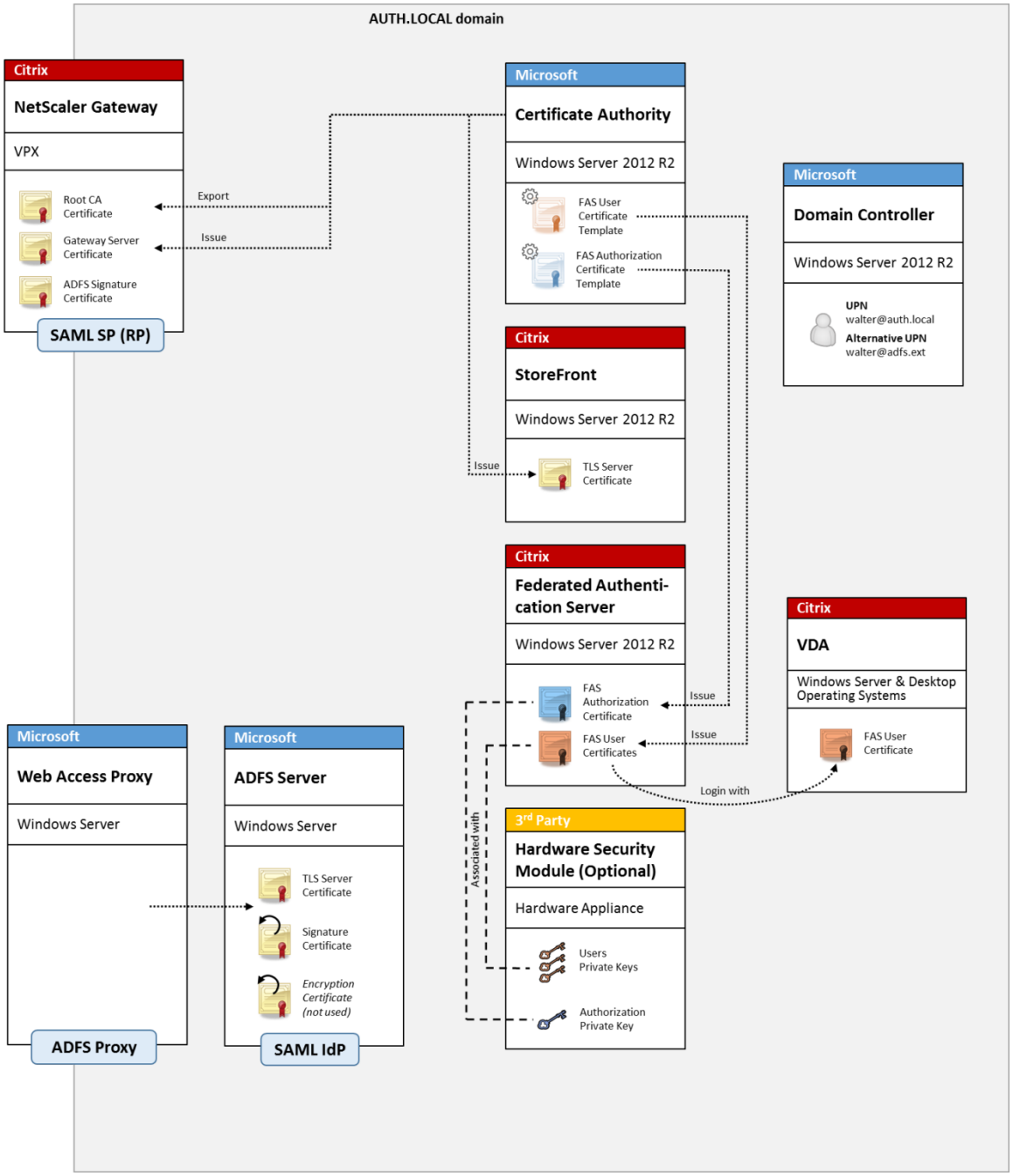
Einführung

In diesem Dokument wird beschrieben, wie Sie eine Citrix Umgebung in Microsoft Active Directory-Verbunddienste integrieren.

In vielen Organisationen wird AD FS zum Verwalten des sicheren Benutzerzugriffs auf Websites verwendet, die einen einzelnen Authentifizierungspunkt erfordern. Wenn beispielsweise Mitarbeitern zusätzliche Inhalte und Downloads zur Verfügung stehen, müssen diese durch standardmäßige Windows-Anmeldeinformationen geschützt werden.

Der Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ermöglicht zudem die Integration von Citrix NetScaler und Citrix StoreFront in das AD FS-Anmeldesystem und vereinfacht so die Anmeldung für das Personal.

Bei einer solchen Bereitstellung wird NetScaler als vertrauende Seite für Microsoft AD FS integriert.



Übersicht über SAML

SAML (Security Assertion Markup Language) ist eine einfaches System für die Webbrowser-Anmeldung, durch das eine Umleitung auf eine Anmeldeseite vorgenommen wird. Die Konfiguration umfasst folgende Elemente:

Umleitungs-URL (URL des Single Sign-On-Diensts)

Wenn NetScaler erkennt, dass ein Benutzer authentifiziert werden muss, weist es den Webbrowser zur Durchführung eines HTTP POST an eine SAML-Anmeldeseite auf dem AD FS-Server an. Dies ist normalerweise eine `https://`-Adresse des Formats `https://adfs.mycompany.com/adfs/ls`.

Der Webseiten-POST umfasst weitere Informationen, darunter eine Rückleitungsadresse, an die der Benutzer nach der Anmeldung zurückgeleitet wird.

Bezeichner (Ausstellername/EntityID)

Die EntityID ist ein eindeutiger Bezeichner, der von NetScaler in den POST-Daten an AD FS verwendet wird. Durch ihn wird AD FS darüber informiert, bei welchem Dienst der Benutzer versucht, sich anzumelden und welche Authentifizierungsrichtlinien anzuwenden sind. Wenn eine SAML-Authentifizierungs-XML ausgestellt wird, kann diese nur für die Anmeldung bei dem durch die EntityID bezeichneten Dienst verwendet werden.

Normalerweise ist die EntityID die URL der Anmeldeseite des NetScaler-Servers. Es kann jedoch eine beliebige andere EntityID verwendet werden, vorausgesetzt NetScaler und AD FS interpretieren sie beide als gültig: `https://ns.mycompany.com/application/logonpage`.

Rückleitungsadresse (Antwort-URL)

Wenn die Authentifizierung erfolgreich ist, weist AD FS den Webbrowser des Benutzers an, einen POST einer SAML-Authentifizierungs-XML an eine der Antwort-URLs vorzunehmen, die für die EntityID konfiguriert wurden. Das ist normalerweise eine `https://`-Adresse auf dem ursprünglichen NetScaler-Server im Format `https://ns.mycompany.com/cgi/samlauth`.

Sind mehrere Antwort-URLs konfiguriert, kann NetScaler eine aus dem ursprünglichen POST an AD FS wählen.

Signaturzertifikat (IDP-Zertifikat)

SAML-Authentifizierungs-XML-Blobs werden von AD FS kryptografisch mit seinem privaten Schlüssel signiert. Zur Überprüfung der Signatur muss NetScaler zur Prüfung solcher Signaturen mit dem öffentlichen Schlüssel in der Zertifikatdatei konfiguriert sein. Die Zertifikatdatei ist normalerweise eine vom AD FS-Server erhaltene Textdatei.

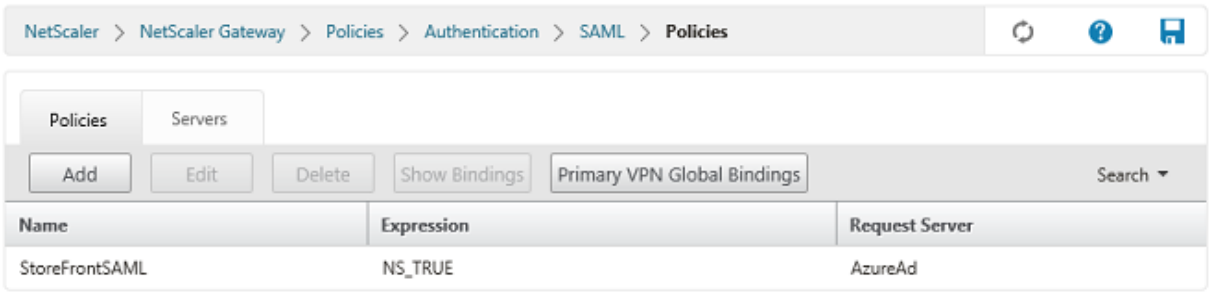
URL für Single Sign-Out (URL für einmaliges Abmelden)

AD FS und NetScaler unterstützen ein zentrales Abmeldesystem. Das ist eine URL, die von NetScaler regelmäßig abgefragt wird, um zu prüfen, ob das SAML-Authentifizierungs-XML-Blob immer noch die aktuell angemeldete Sitzung repräsentiert.

Dies ist ein optionales Feature, das nicht konfiguriert werden muss. Dies ist normalerweise eine `https://`-Adresse des Formats `https://adfs.mycompany.com/adfs/logout`. (Die Adresse darf nicht mit der URL für die einmalige Anmeldung identisch sein.)

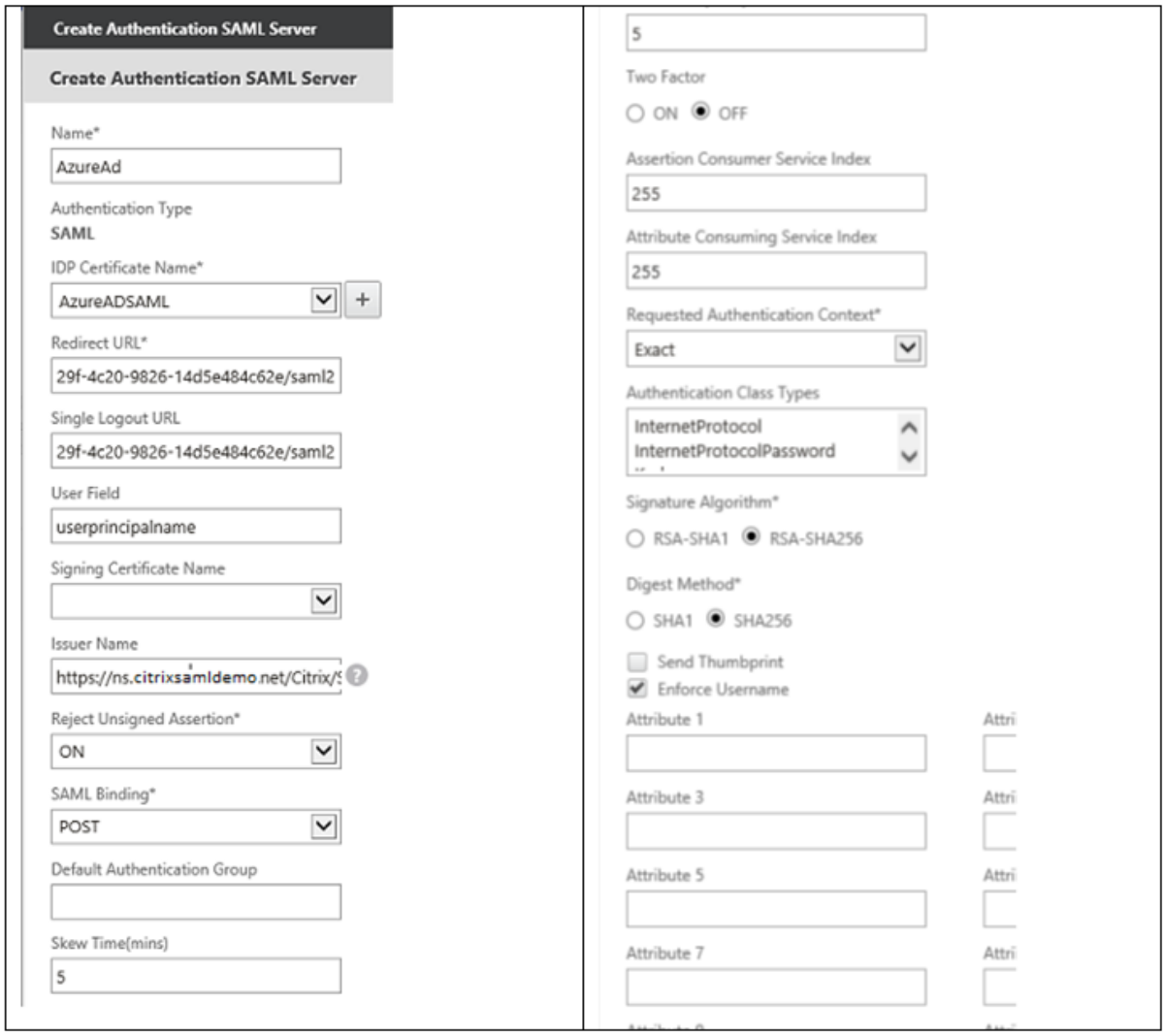
Konfiguration

Im Bereich NetScaler Gateway-Bereitstellung des Artikels Übersicht über die Architekturen des Verbundauthentifizierungsdiensts wird beschrieben, wie NetScaler Gateway mit dem NetScaler-Setupassistenten von XenApp und XenDesktop für die Standard-LDAP-Authentifizierungsoptionen konfiguriert wird. Nach diesem Arbeitsgang können Sie eine neue Authentifizierungsrichtlinie in NetScaler für die SAML-Authentifizierung erstellen. Diese kann dann die von dem NetScaler-Setupassistenten verwendete Standard-LDAP-Richtlinie ersetzen.



Ausfüllen der SAML-Richtlinie

Konfigurieren Sie den neuen SAML-IdP-Server mit den zuvor der AD FS-Verwaltungskonsole entnommenen Informationen. Wenn diese Richtlinie angewendet wird, leitet NetScaler Benutzer zur Anmeldung an AD FS um und akzeptiert das zurückgegebene, von AD FS signierte SAML-Authentifizierungstoken.



Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.

Integration des Verbundauthentifizierungsdiensts in Azure Active Directory

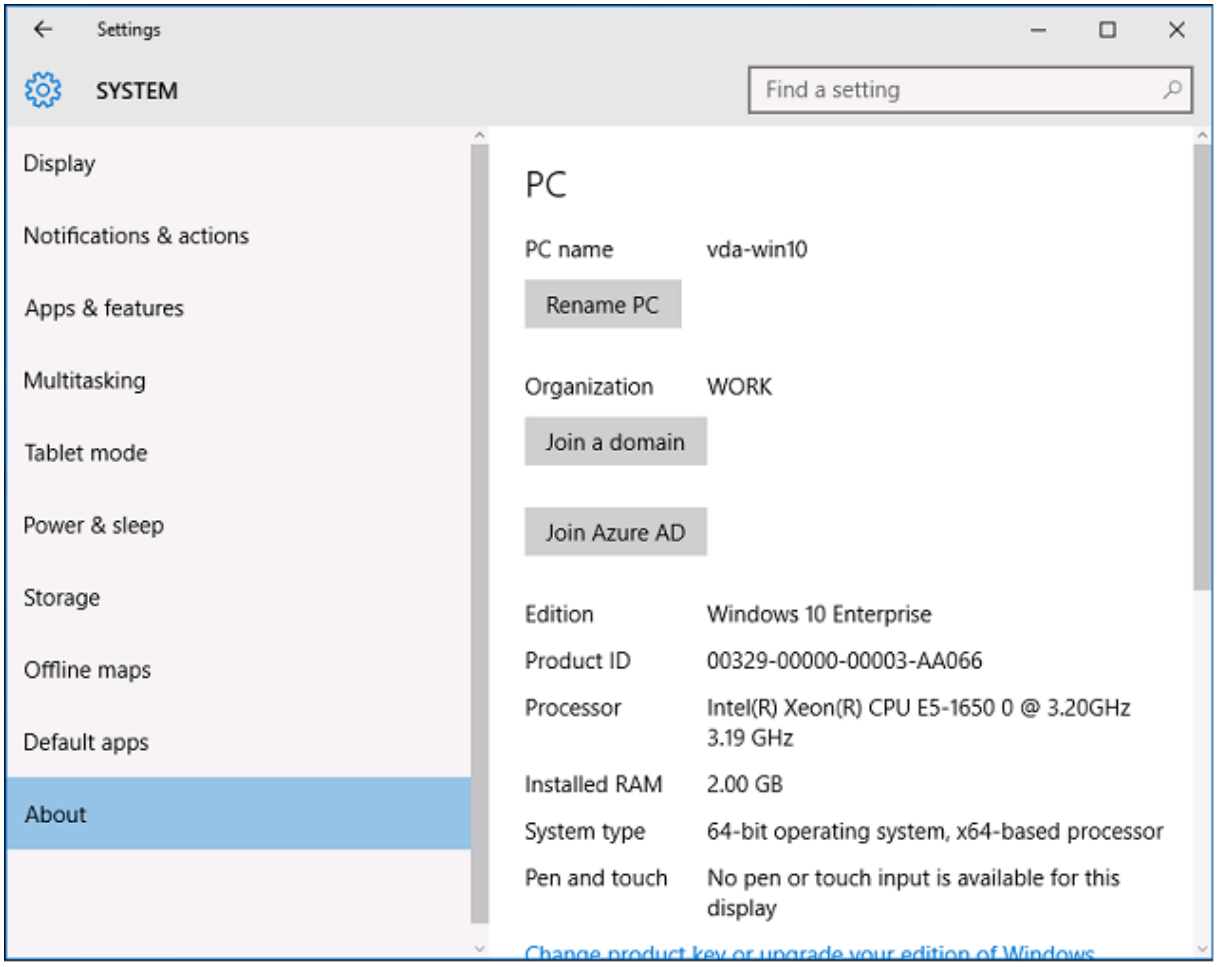
August 18, 2021

Einführung

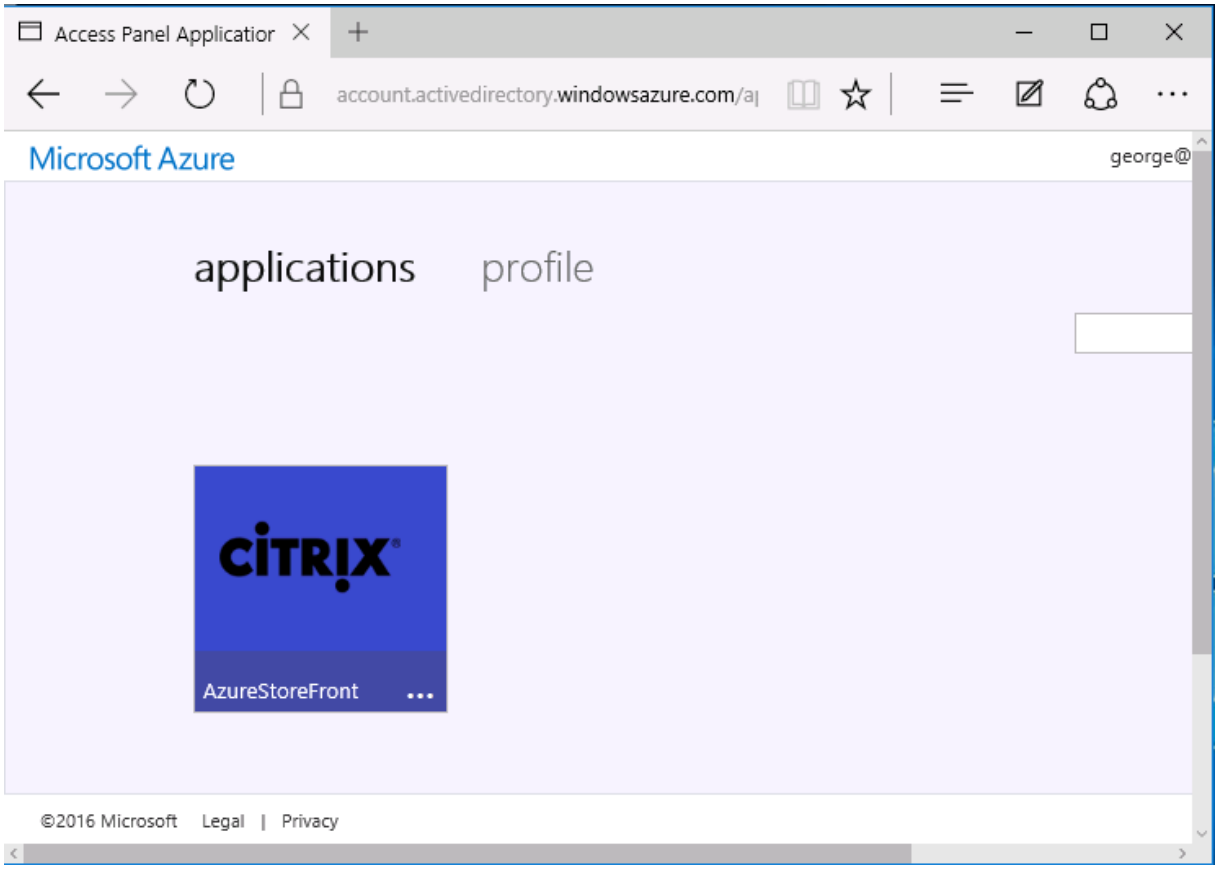
In diesem Dokument wird beschrieben, wie Sie eine Citrix Umgebung in Azure Active Directory unter Windows 10 integrieren.

Azure Active Directory wurde mit Windows 10 eingeführt und repräsentiert ein neues Modell für den Domänenbeitritt, bei dem Laptops im Roamingbetrieb über das Internet einer Unternehmensdomäne für Verwaltungszwecke und zum Single Sign-On beitreten können.

Die hier vorgestellte Beispielbereitstellung ist ein System, bei dem die IT neuen Benutzern eine Unternehmens-E-Mail-Adresse und einen Registrierungscode für ihre privaten Windows 10-Laptops zuteilt. Die Benutzer greifen auf diesen Code über die Option **System** > **Info** > **Azure AD beitreten** im Bereich **Einstellungen** zu.



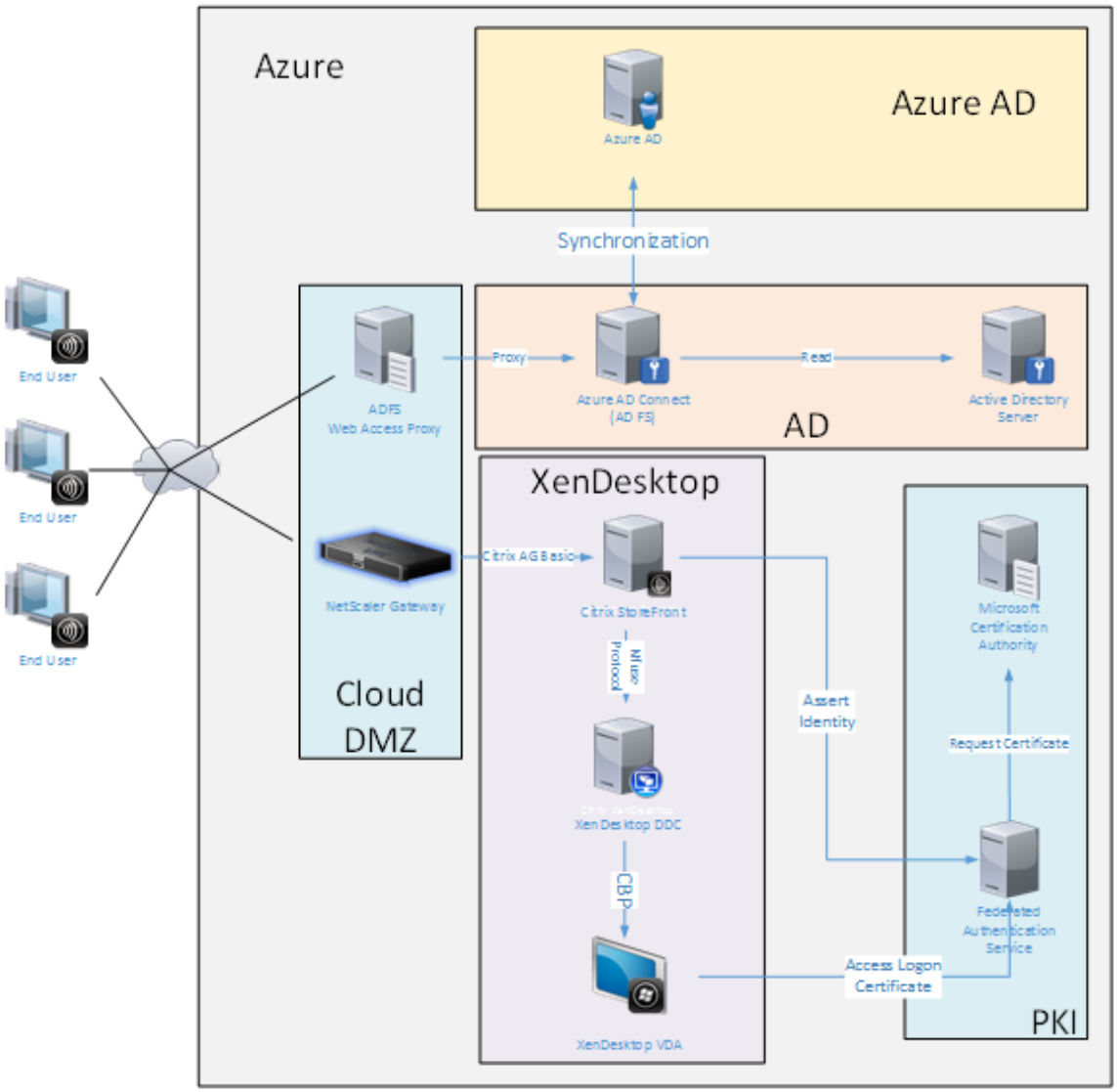
Nach der Registrierung eines Laptops führt der Microsoft Edge-Webbrowser automatisch die Anmeldung bei Unternehmenswebsites und veröffentlichten Citrix Anwendungen über die Azure-SaaS-Anwendungswebsite durch, die auch andere Azure-Anwendungen, wie Office 365, bietet.



Architektur

Diese Architektur repliziert innerhalb von Azure ein herkömmliches Unternehmensnetzwerk unter Integration moderner Cloudtechnologien, wie Azure Active Directory und Office 365. Die Endbenutzer werden alle als Remotebenutzer angesehen, das Konzept eines Büro-Intranets kommt nicht zur Anwendung.

Das Modell kann auch in Unternehmen mit lokalen Systemen verwendet werden, da die Azure AD Connect-Synchronisierung eine Verbindung mit Azure über das Internet herstellen kann.



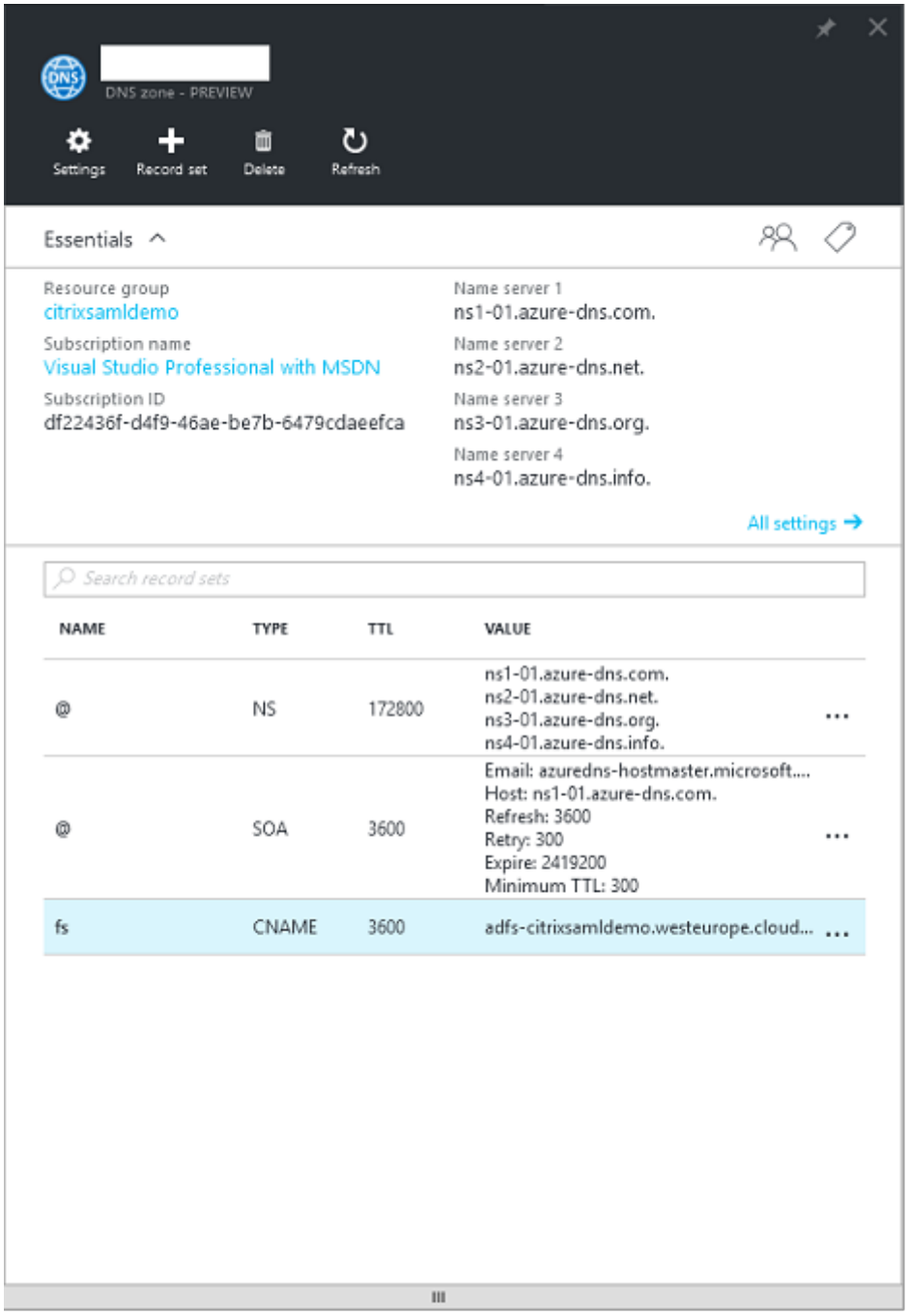
Sichere Verbindungen und Single Sign-On, wie sie konventionell per LAN mit Firewall und Kerberos/NTLM-Authentifizierung realisiert wurden, werden in dieser Architektur durch TLS-Verbindungen mit Azure und SAML ersetzt. Neue Dienste werden als Azure-Anwendungen, die Mitglied von Azure AD sind, erstellt. Vorhandene Anwendungen, die Active Directory erfordern (z. B. eine SQL Server-Datenbank), können mit einer Standard-AD-Server-VM im IaaS-Teil des Azure-Clouddiensts ausgeführt werden.

Wenn ein Benutzer eine herkömmliche Anwendung startet, erfolgt der Zugriff über die mit XenApp bzw. XenDesktop veröffentlichte Anwendung. Die verschiedenen Anwendungstypen werden auf der Seite **Azure-Anwendungen** unter Verwendung der Microsoft Edge-Single Sign-On-Features sortiert. Microsoft stellt außerdem Android- und iOS-Apps zur Verfügung, die Azure-Anwendungen aufzählen und starten können.

Erstellen einer DNS-Zone

Für Azure AD muss der Administrator eine öffentliche DNS-Adresse registrieren und die Delegierungszone für das Domänennamensuffix steuern. Hierfür kann das Azure-Feature "DNS-Zone"verwendet werden.

Im vorliegenden Beispiel lautet der Name der DNS-Zone "citrixsamldemo.net".



In der Konsole werden die Namen der Azure-DNS-Namensserver angezeigt. Auf diese muss in den NS-

Einträgen der DNS-Registrierungsstelle für die Zone verwiesen werden (z. B. citrixsamldemo.net. NS n1-01.azure-dns.com).

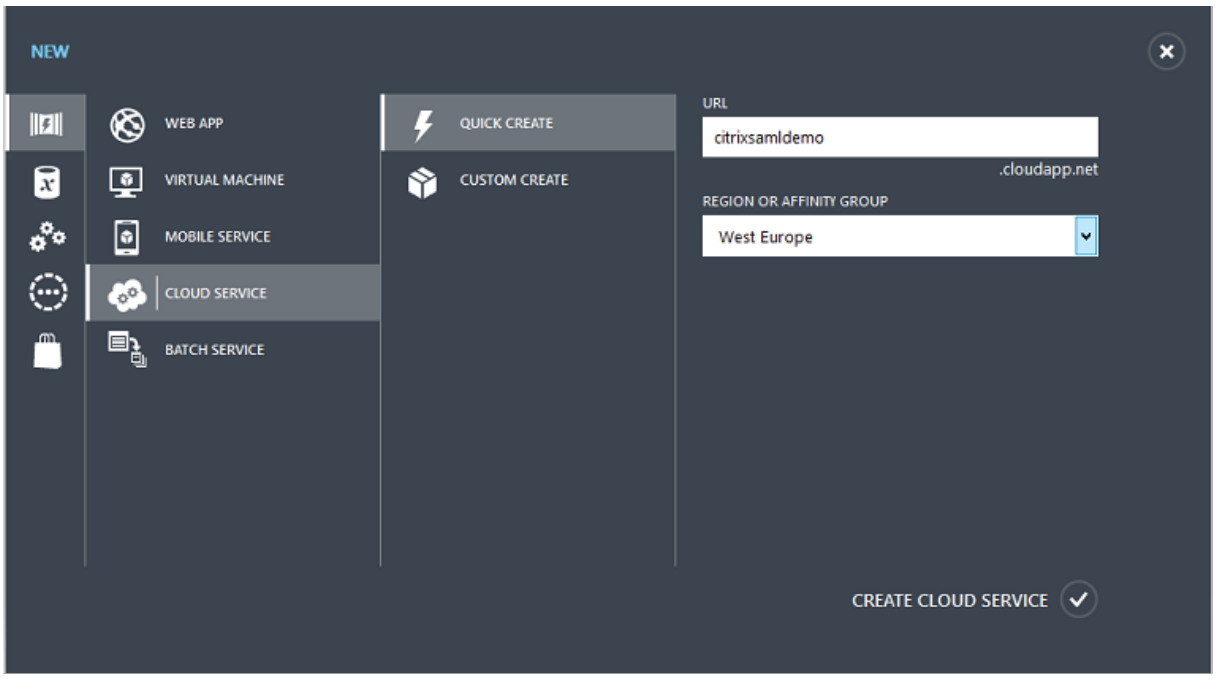
Beim Hinzufügen von Verweisen auf VMs, die in Azure ausgeführt werden, verwendet man am einfachsten den CNAME-Zeiger auf den in Azure verwalteten DNS-Eintrag für die jeweilige VM. Wenn sich die IP-Adresse der VM ändert, müssen Sie dann die DNS-Zonendatei nicht manuell aktualisieren.

In dieser Bereitstellung stimmen internes und externes DNS-Adresssuffix überein. Die Domäne ist citrixsamldemo.net und verwendet Split DNS (10.0.0.* intern).

Fügen Sie den Eintrag "fs.citrixsamldemo.net"hinzu, der auf den Webanwendungsproxyserver verweist. Dies ist der Verbunddienst für diese Zone.

Erstellen eines Clouddiensts

In diesem Beispiel wird eine Citrix Umgebung einschließlich einer AD-Umgebung mit einem in Azure ausgeführten AD FS-Server konfiguriert. Ein Clouddienst wird unter dem Namen "citrixsamldemo" erstellt.

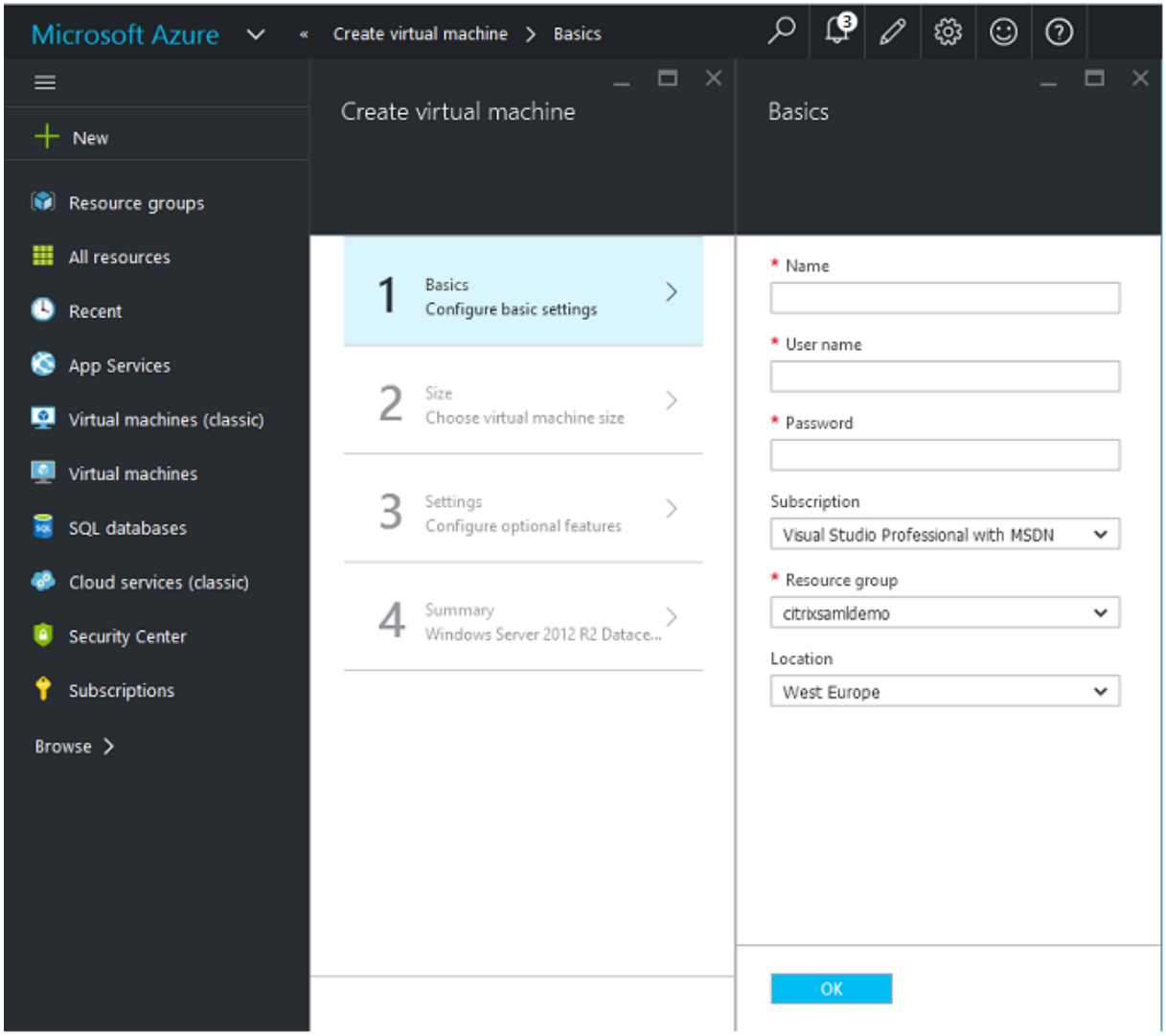


Erstellen virtueller Windows-Maschinen

Erstellen Sie fünf Windows-VMs, die im Clouddienst ausgeführt werden:

- Domänencontroller (domaincontrol)
- Azure Connect AD FS-Server (adfs)
- AD FS-Proxy für den Webzugriff (Webanwendungsproxy, kein Mitglied einer Domäne)

- Citrix XenDesktop Delivery Controller (DDC)
- Citrix XenDesktop Virtual Delivery Agent (VDA)



Domänencontroller

- Fügen Sie die Rollen **DNS-Server** und **Active Directory-Domänendienste** hinzu, um eine Active Directory-Standardbereitstellung zu erstellen (in diesem Beispiel citrixsamldemo.net). Nach Abschluss der Domänenpromotion fügen Sie die Rolle **Active Directory-Zertifikatdienste** hinzu.
- Erstellen Sie ein normales Benutzerkonto für Tests (z. B. George@citrixsamldemo.net).
- Da auf diesem Server DNS intern ausgeführt wird, müssen alle Server zur DNS-Auflösung auf diesem Server verweisen. Sie tun dies auf der Seite **Azure-DNS-Einstellungen**. (Weitere Informationen finden Sie im Anhang).

AD FS-Controller und Webanwendungsproxyserver

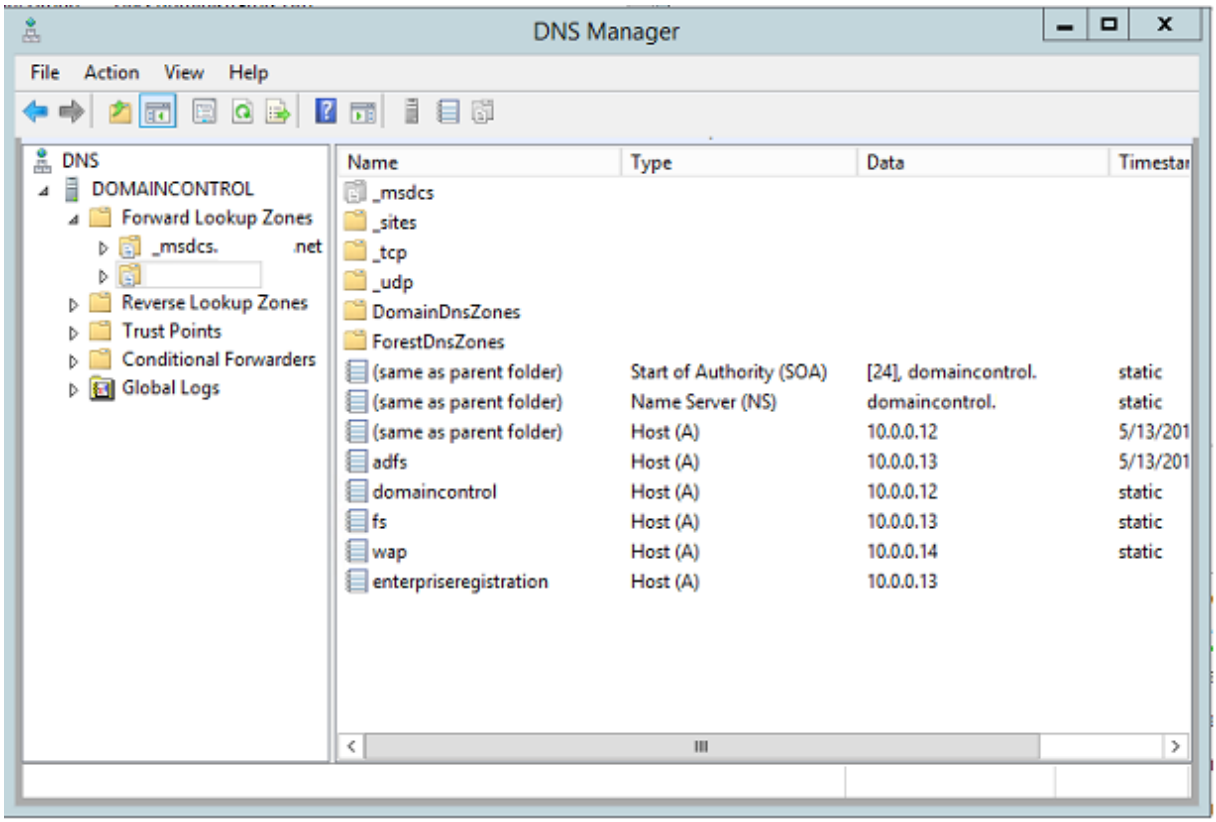
- Fügen Sie den AD FS-Server der Domäne citrixsamldemo hinzu. Der Webanwendungsproxyserver muss in einer isolierten Arbeitsgruppe bleiben. Registrieren Sie daher manuell eine DNS-Adresse beim AD-DNS.
- Führen Sie an diesen Servern das Cmdlet **Enable-PSRemoting** –**Force** aus, um PS-Remoting aus dem Azure AD Connect-Tool über Firewalls zuzulassen.

XenDesktop Delivery Controller und VDA

- Installieren Sie den XenApp- bzw. XenDesktop Delivery Controller und VDA auf den verbleibenden beiden Windows-Servern, die zur Domäne citrixsamldemo gehören.

Konfigurieren eines internen DNS

Nach Installation des Domänencontrollers konfigurieren Sie den DNS-Server für die interne citrixsamldemo.net-Dimension und als Weiterleiter an einen externen DNS-Server (z. B.: 8.8.8.8).

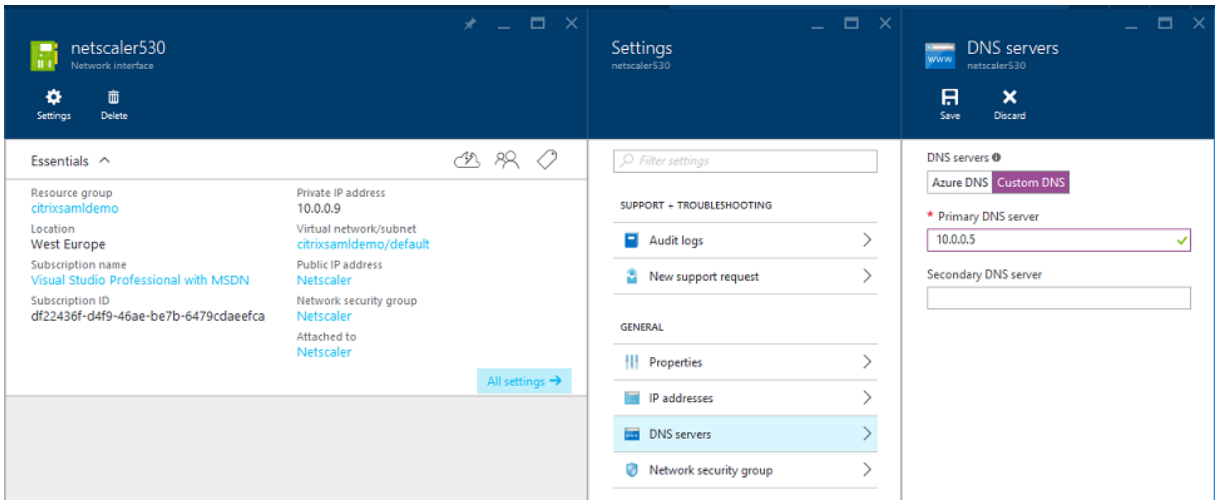


Fügen Sie für folgende Elemente einen statischen Eintrag hinzu:

- wap.citrixsamldemo.net (die Webanwendungsproxy-VM wird nicht der Domäne hinzugefügt)

- fs.citrixsamldemo.net (Adresse des internen Verbundservers)
- enterpriseregistration.citrixsaml.net (identisch mit fs.citrixsamldemo.net)

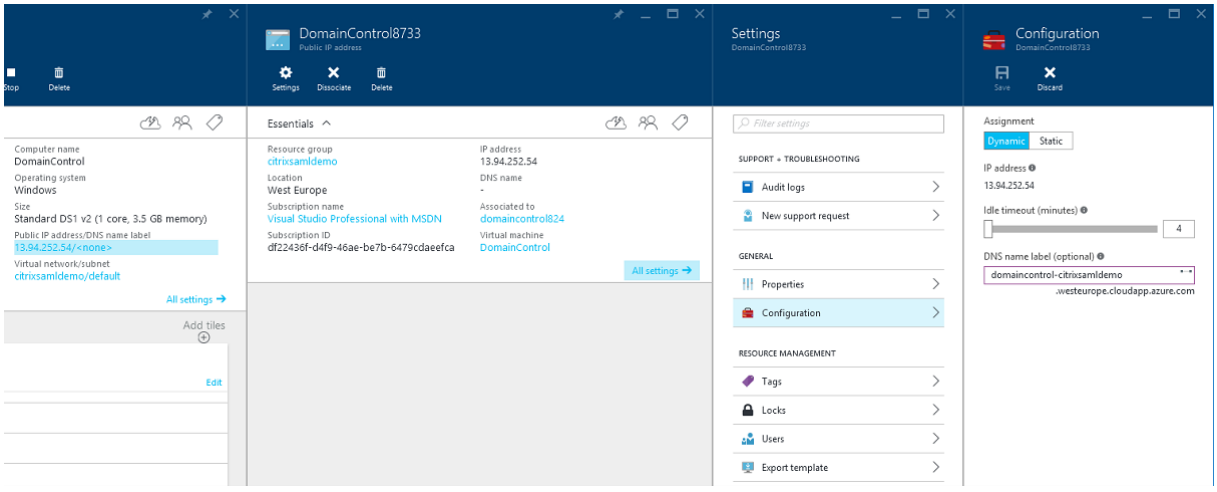
Alle in Azure ausgeführten VMs müssen zur ausschließlichen Verwendung dieses DNS-Servers konfiguriert werden. Sie können diese Konfiguration über die Netzwerkschnittstellen-GUI durchführen.



Standardmäßig wird die interne IP-Adresse (10.0.0.9) dynamisch zugewiesen. Sie können die IP-Adresse über die zugehörige Einstellung bleibend zuweisen. Diesen Schritt müssen Sie für den Webanwendungsproxyserver und den Domänencontroller durchführen.

Konfigurieren einer externen DNS-Adresse

Wenn eine virtuelle Maschine ausgeführt wird, verwendet Azure seinen eigenen DNS-Zonenserver, der auf die aktuelle, der VM zugewiesene, öffentliche IP-Adresse verweist. Dies kann als nützliches Feature aktiviert werden, da Azure standardmäßig IP-Adressen bei jedem VM-Start zuweist.

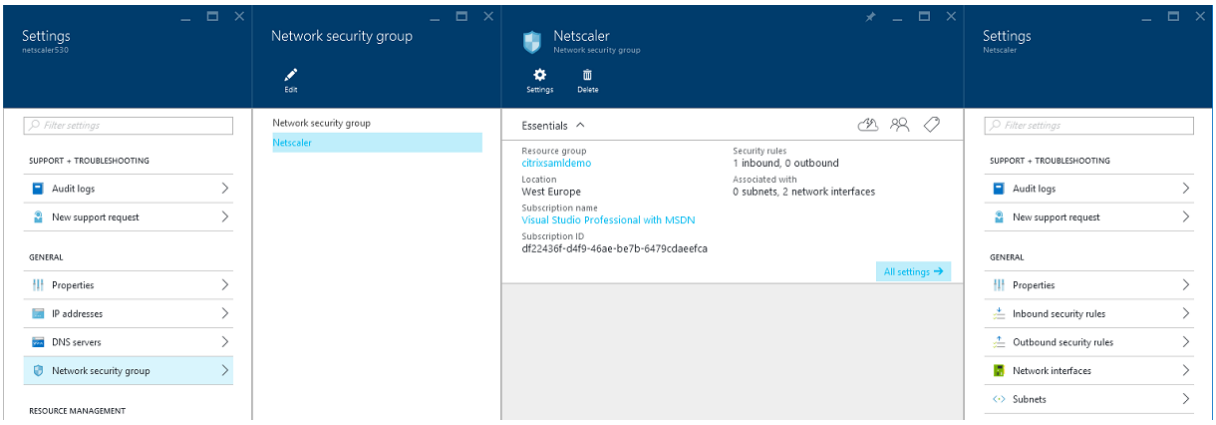


In diesem Beispiel wird dem Domänencontroller die DNS-Adresse “domaincontrol-citrixsamldemo.westeurope.clo
zugewiesen.

Nach Abschluss der Remotekonfiguration dürfen öffentliche IP-Adressen nur für die Webanwendungsproxy- und die NetScaler-VMs aktiviert sein. (Während der Konfiguration wird die öffentliche IP-Adresse für den RDP-Zugriff auf die Umgebung verwendet).

Konfigurieren von Sicherheitsgruppen

Von der Azure-Cloud werden Firewall-Regeln für den TCP/UDP-Zugriff auf VMs aus dem Internet mithilfe von Sicherheitsgruppen verwaltet. Standardmäßig lassen alle VMs RDP-Zugriff zu. Der NetScaler-Server und der Webanwendungsproxyserver müssen außerdem TLS an Port 443 zulassen.

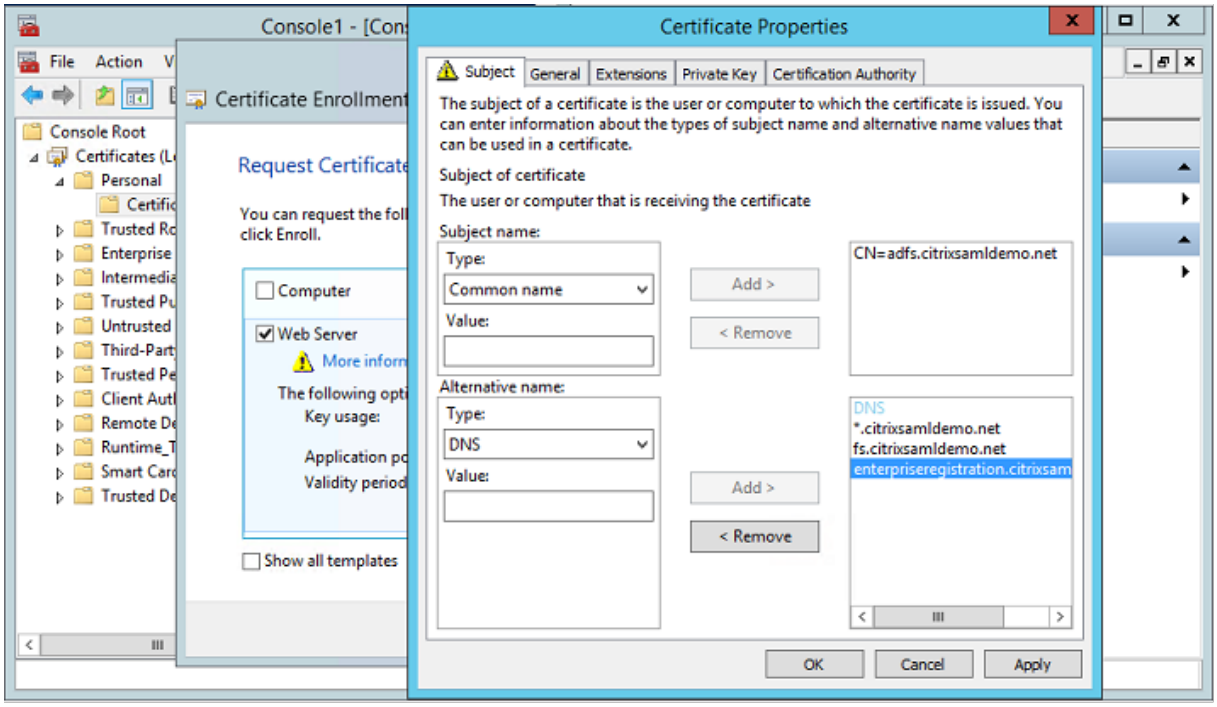


Erstellen eines AD FS-Zertifikats

Aktivieren Sie die Zertifikatvorlage **Webserver** in der Microsoft-Zertifizierungsstelle (CA). Dies ermöglicht die Erstellung eines Zertifikats mit benutzerdefinierten DNS-Adressen, das einschließlich privatem Schlüssel in eine PFX-Datei exportiert werden kann. Sie müssen dieses Zertifikat auf dem AD FS-Server und dem Webanwendungsproxyserver installieren, damit die PFX-Datei bevorzugte Option ist.

Stellen Sie ein Webserverzertifikat mit folgenden Antragstellernamen aus:

- Commonname:
  - adfs.citrixsamldemo.net (Computername)
- SubjectAltname:
  - *.citrixsamldemo.net [Zonenname]
  - fs.citrixsamldemo. net [Eintrag in DNS]
  - enterpriseregistration.citrixsamldemo.net



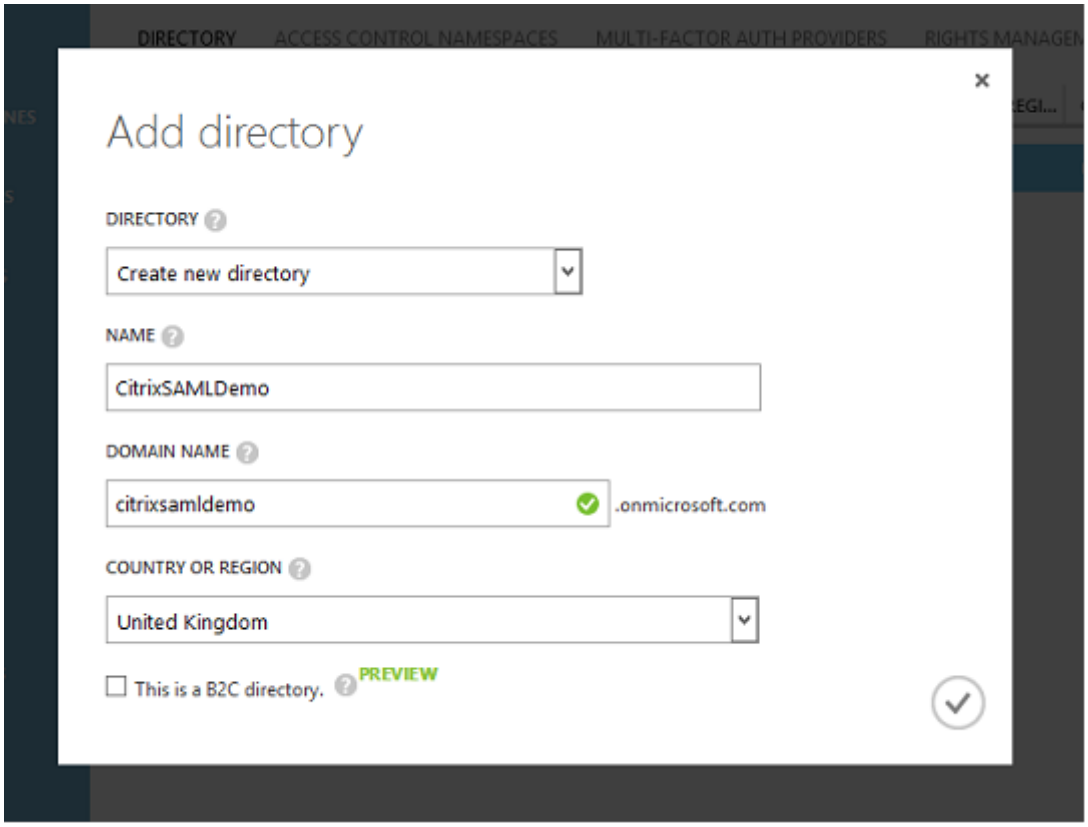
Exportieren Sie das Zertifikat mitsamt einem kennwortgeschützten privaten Schlüssel in eine PFX-Datei.

Einrichten von Azure Active Directory

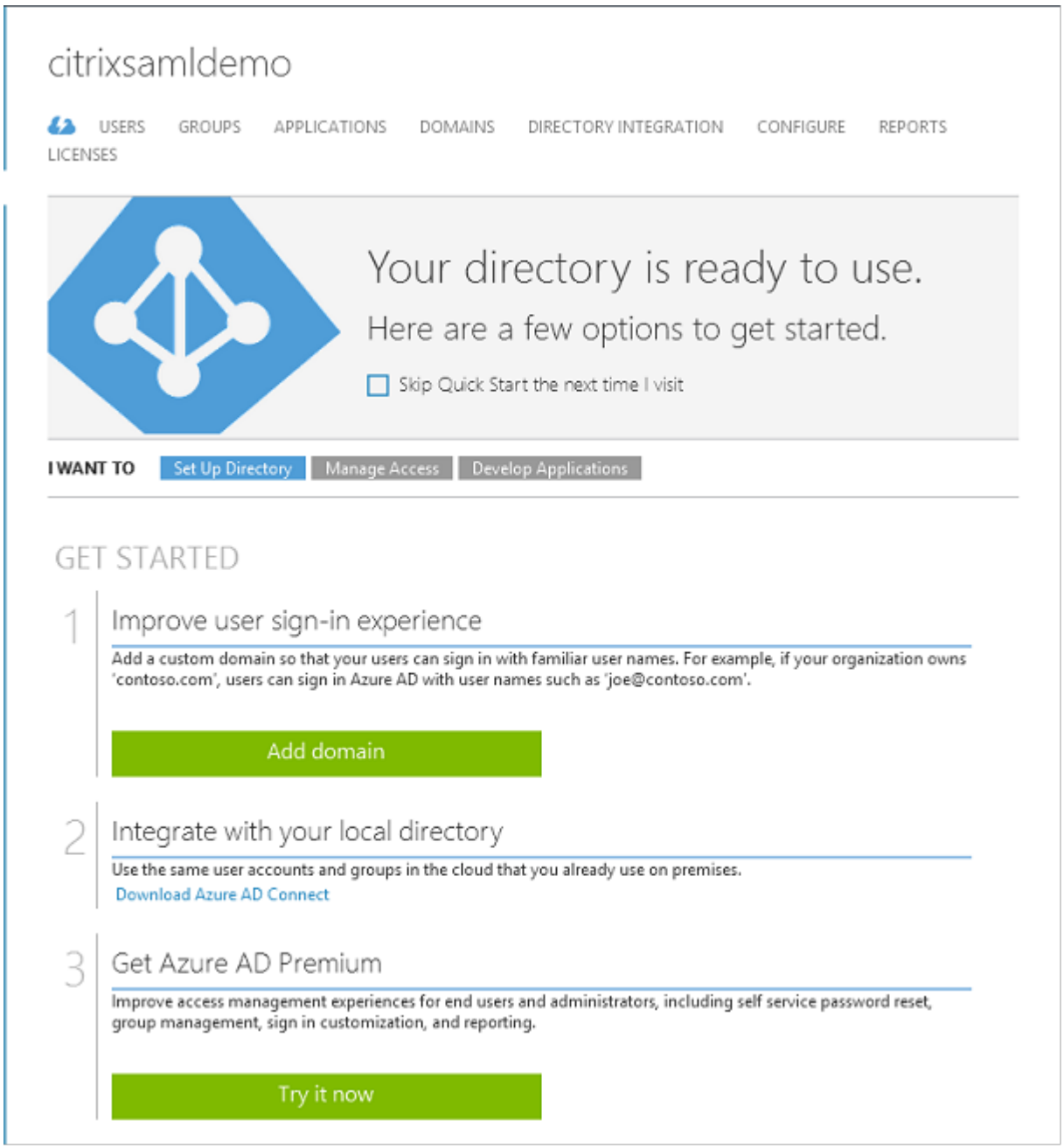
In diesem Abschnitt wird erläutert, wie eine neue Instanz von Azure AD eingerichtet und Benutzeridentitäten für die Windows 10-Einbindung in Azure AD erstellt werden.

Erstellen eines Verzeichnisses

Melden Sie sich beim Azure-Portal an und erstellen Sie ein Verzeichnis.

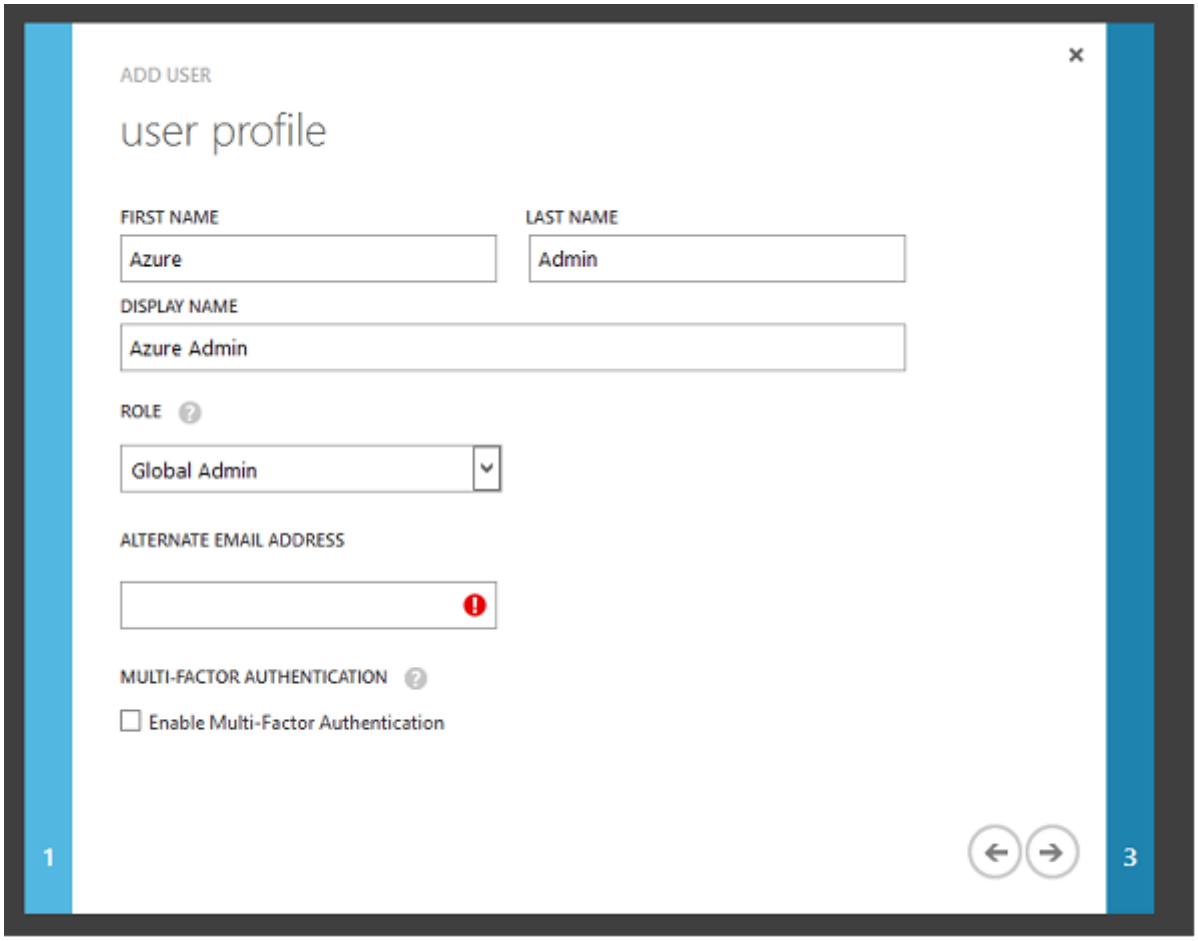


Zum Abschluss wird die Seite “Zusammenfassung”angezeigt.



Erstellen eines globalen Administrators (AzureAdmin)

Erstellen Sie einen globalen Administrator in Azure (in diesem Beispiel AzureAdmin@citrixsamldemo.onmicrosoft.c
und melden Sie sich mit dem neuen Konto an, um ein Kennwort einzurichten.



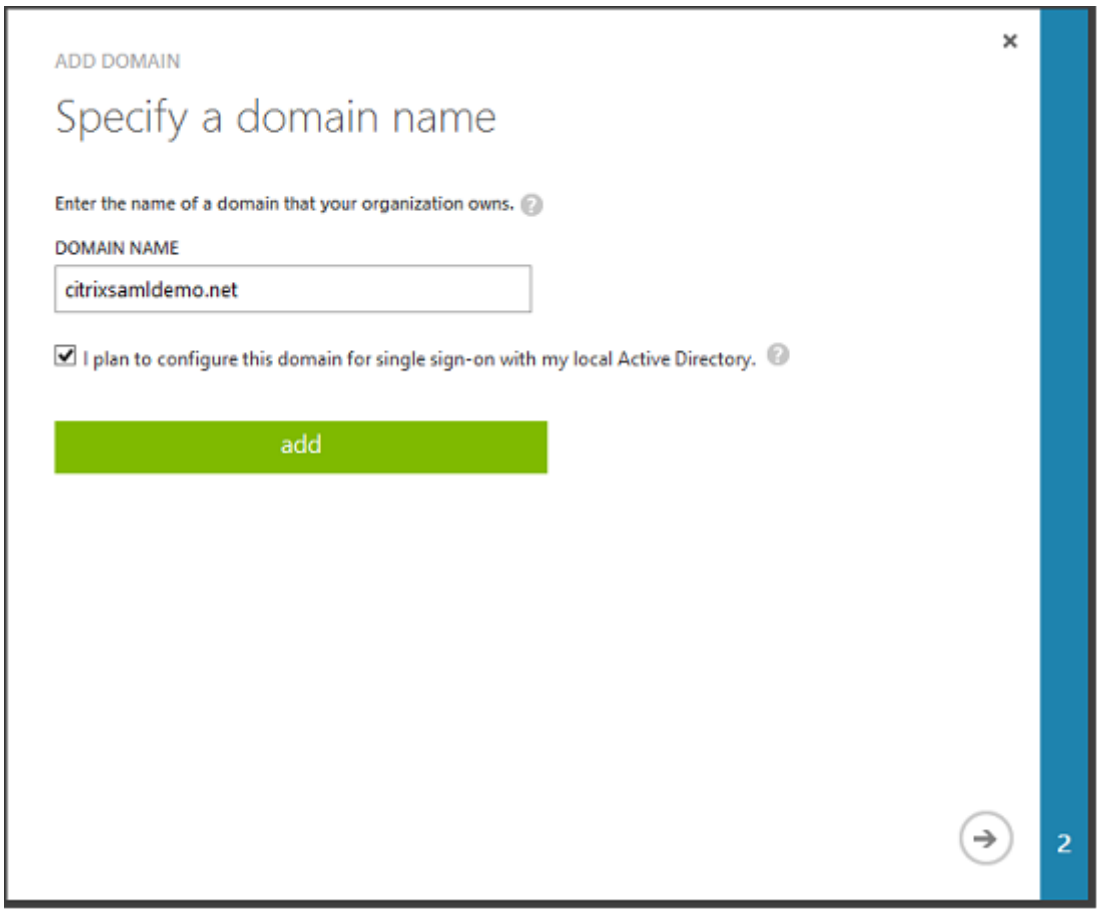
Registrieren der Domäne bei Azure AD

Standardmäßig werden Benutzer anhand einer E-Mail-Adresse im Format <*benutzer.name*>@<*firma*>.onmicrosoft.c identifiziert.

Dies funktioniert zwar ohne weitere Konfiguration, eine E-Mail-Adresse im Standardformat ist jedoch besser; sie sollte möglichst dem E-Mail-Konto des Endbenutzers entsprechen: <benutzer.name>@<firma>.com.

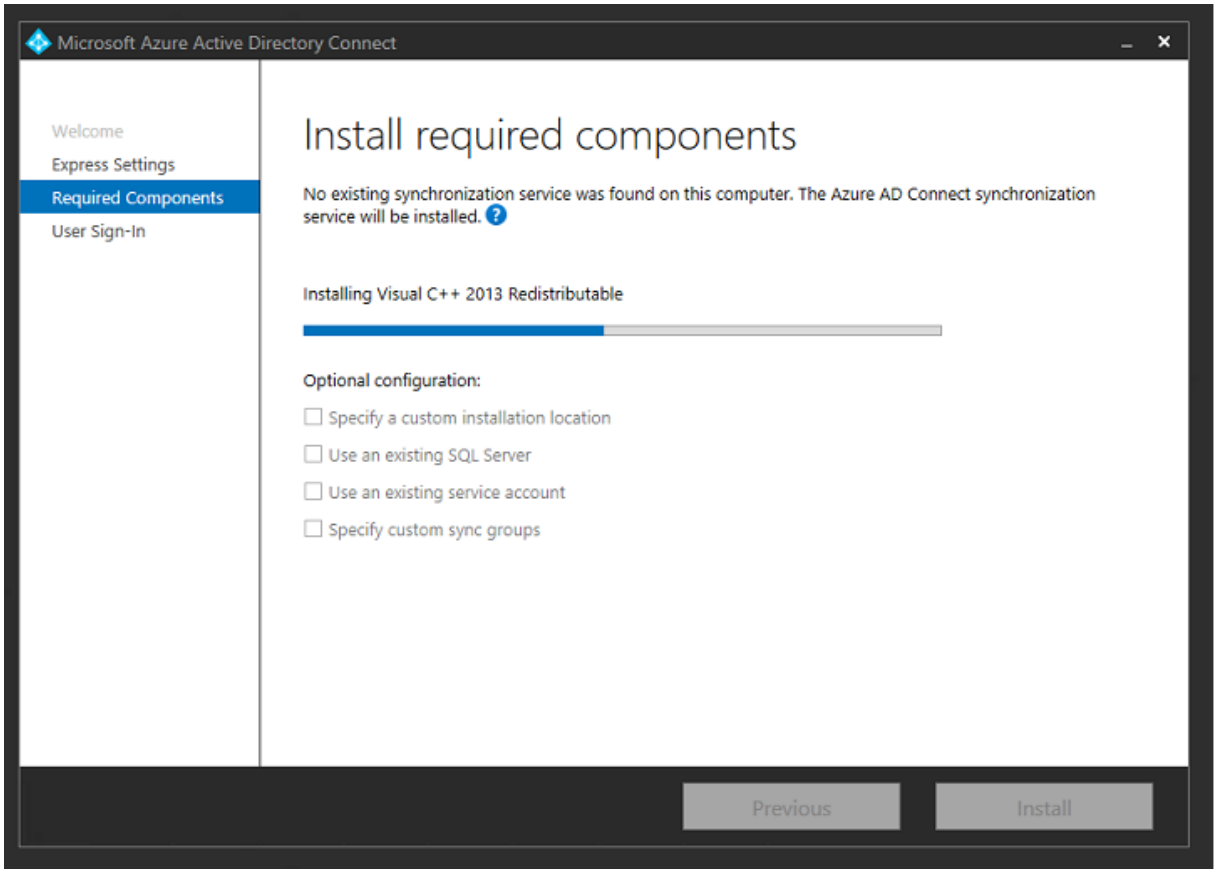
Die Aktion **Domäne hinzufügen** dient zum Konfigurieren der Umleitung von der tatsächlichen Unternehmensdomäne. In diesem Beispiel wird “citrixsamldemo.net”verwendet.

Wenn Sie AD FS für Single Sign-On einrichten, aktivieren Sie das Kontrollkästchen.

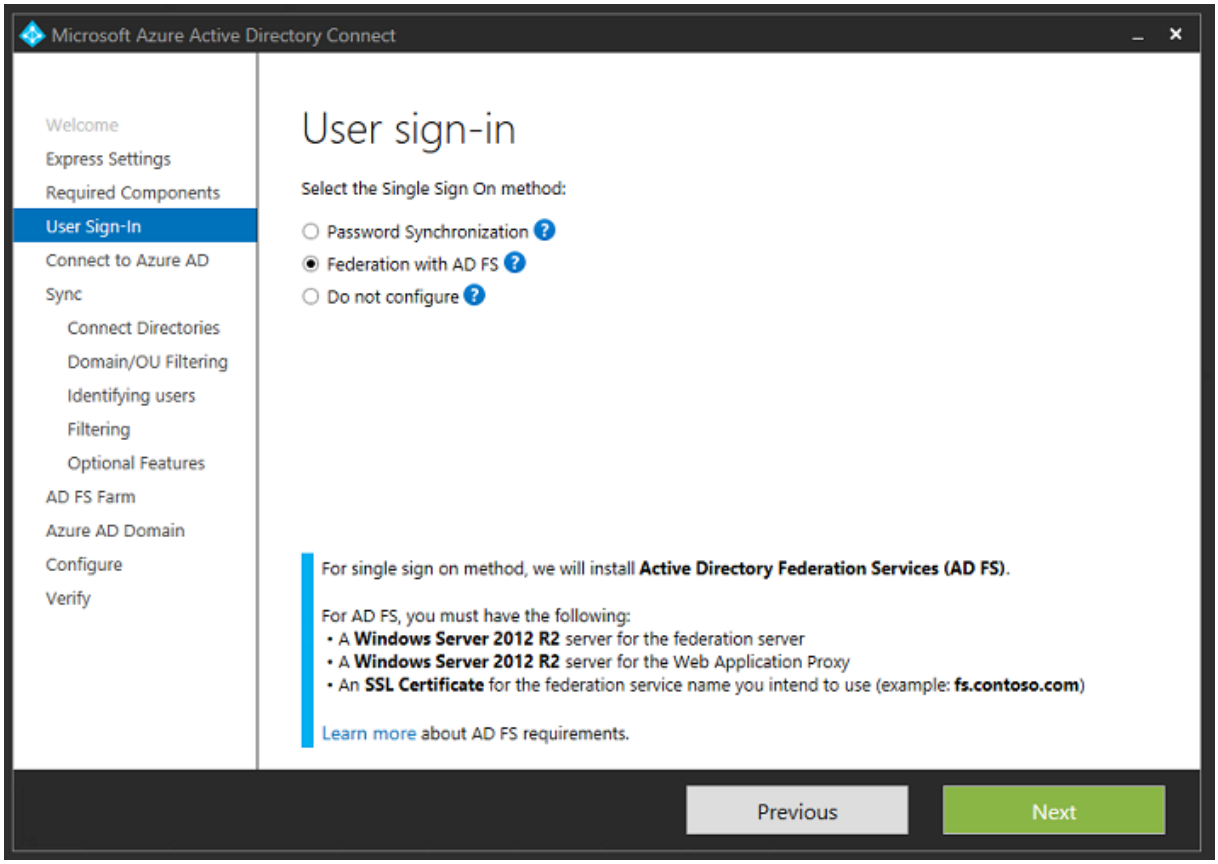


Installieren von Azure AD Connect

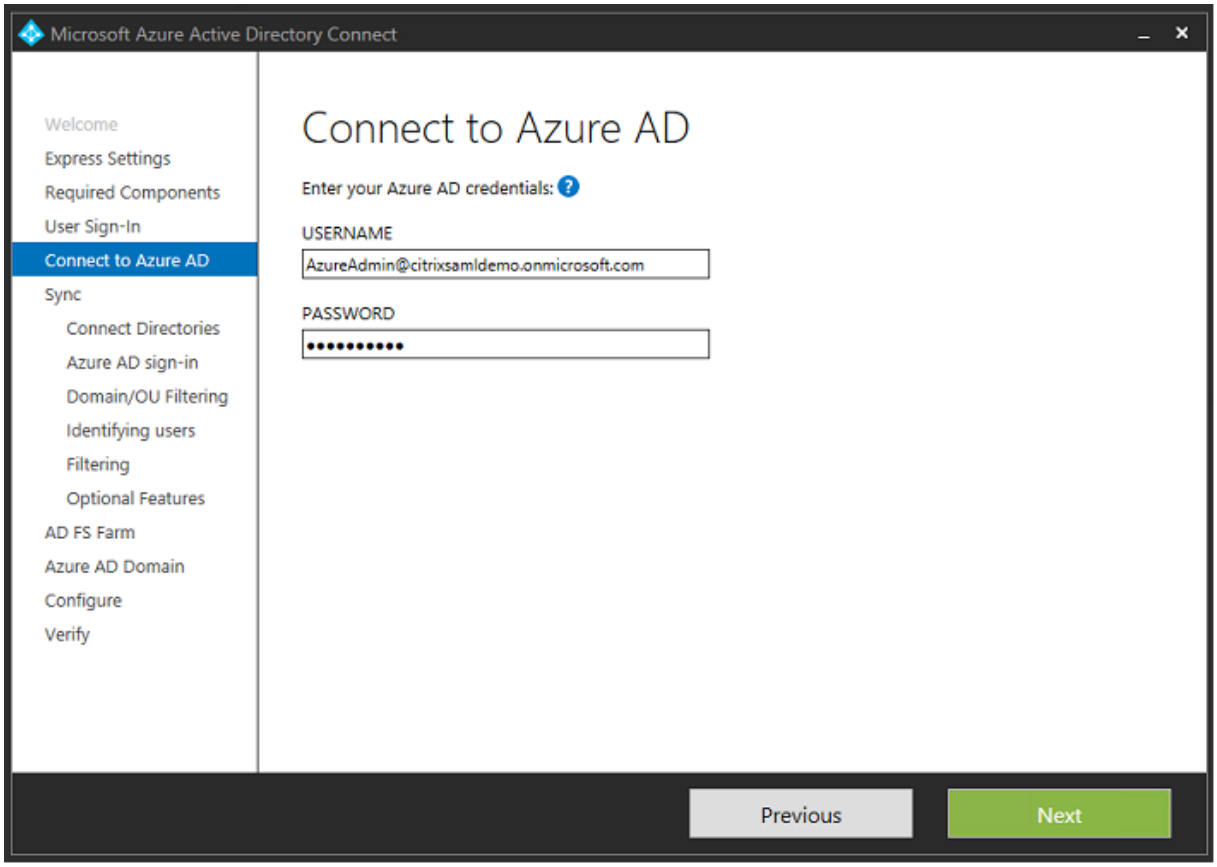
In Schritt 2 der Azure AD-Konfiguration werden Sie auf die Downloadseite für Azure AD Connect umgeleitet. Installieren Sie dieses Tool auf der AD FS-VM. Verwenden Sie **Benutzerdefinierte Installation** anstelle von **Express-Einstellungen**, damit AD FS-Optionen verfügbar sind.



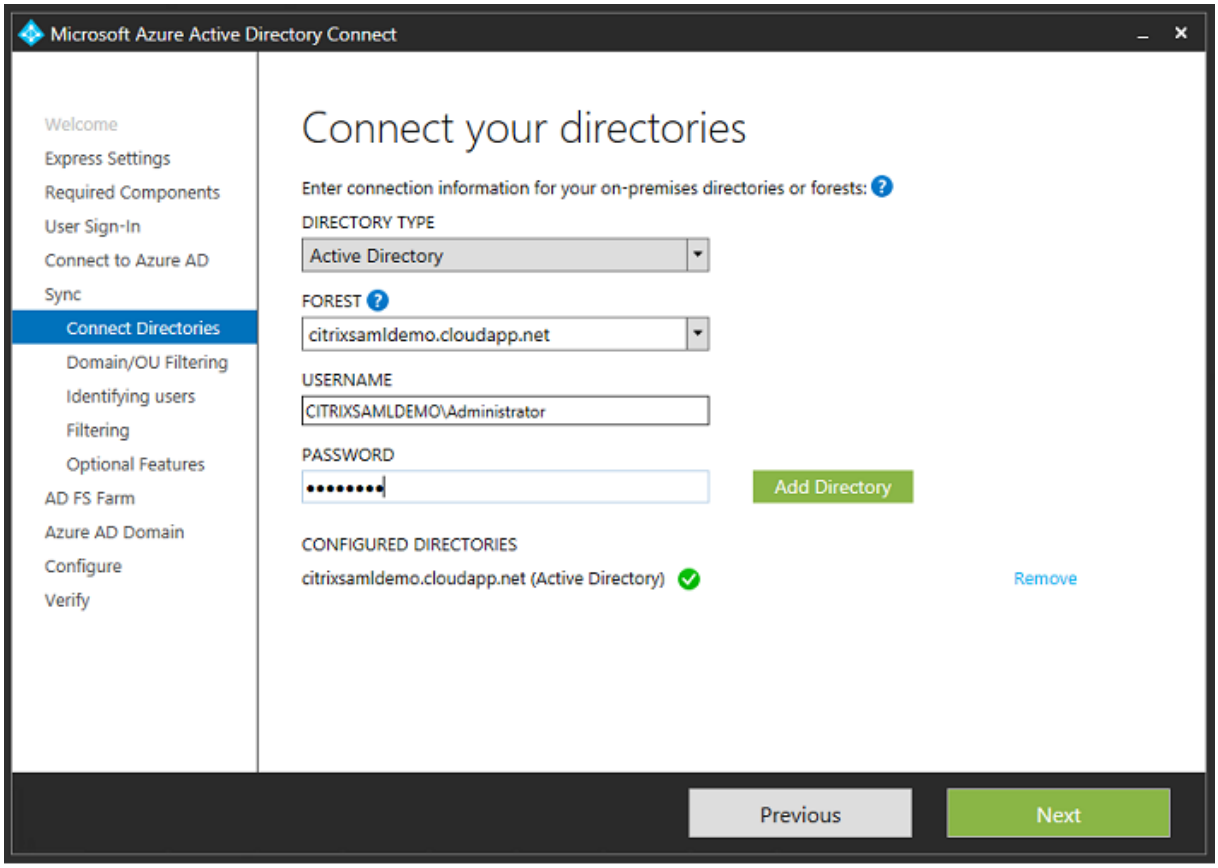
Wählen Sie die Single Sign-On-Option **Verbund mit AD FS**.



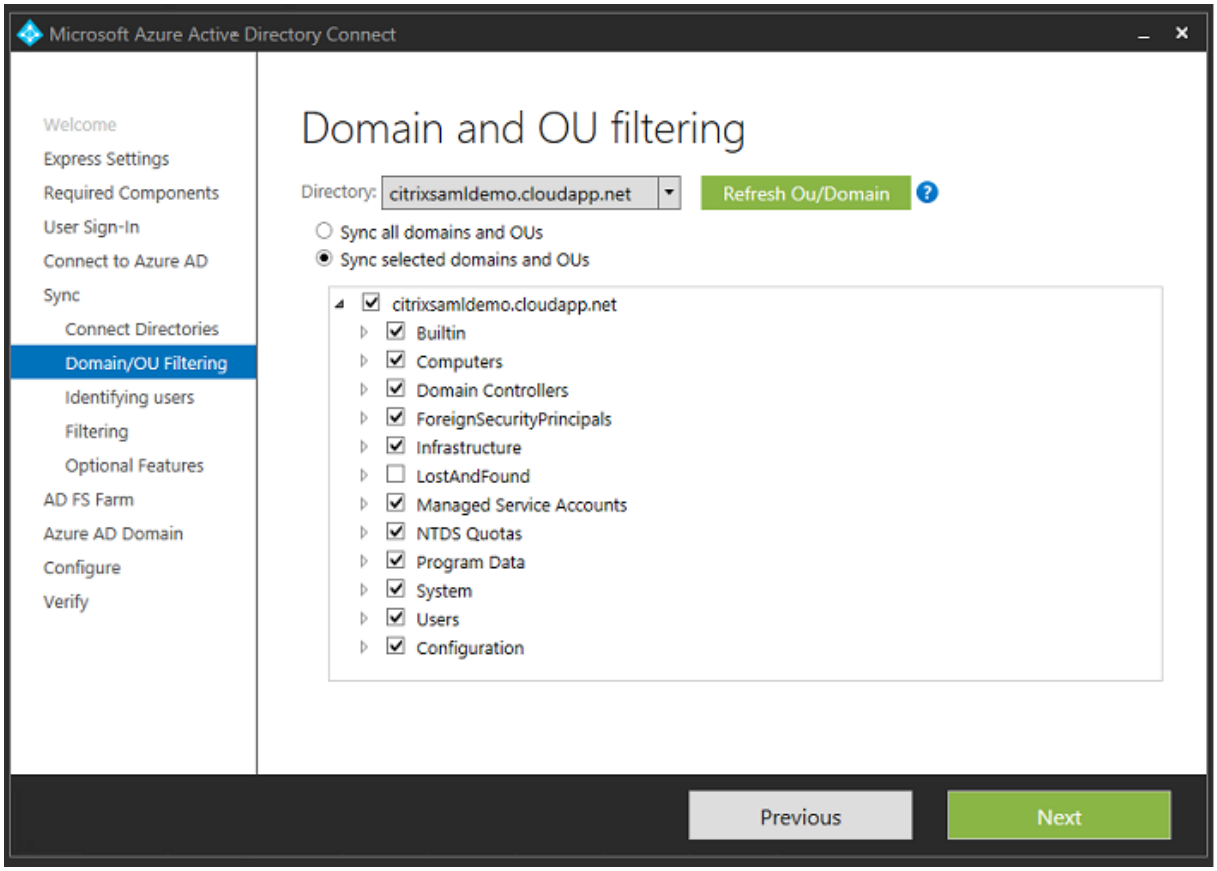
Stellen Sie eine Verbindung mit Azure unter Verwendung des zuvor erstellten Administratorkontos her.



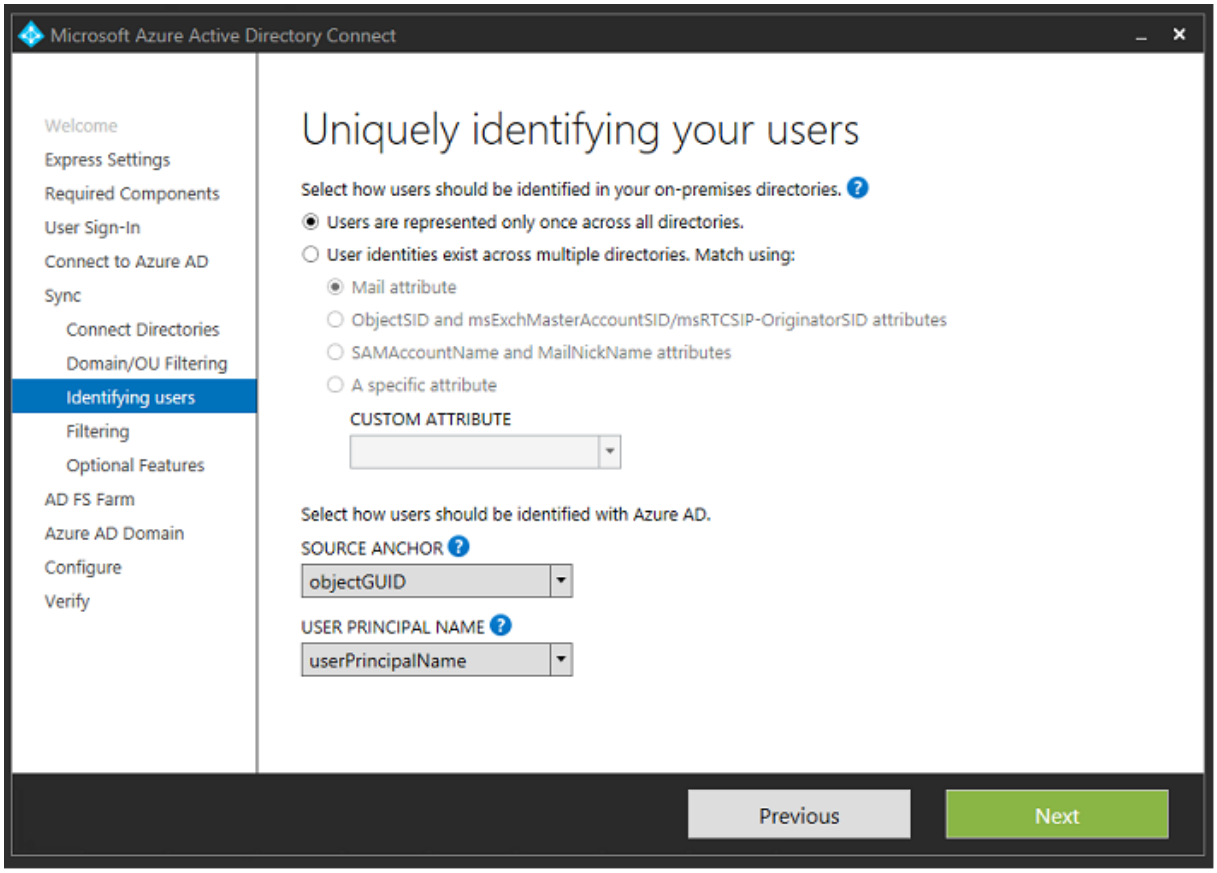
Wählen Sie die interne AD-Gesamtstruktur.



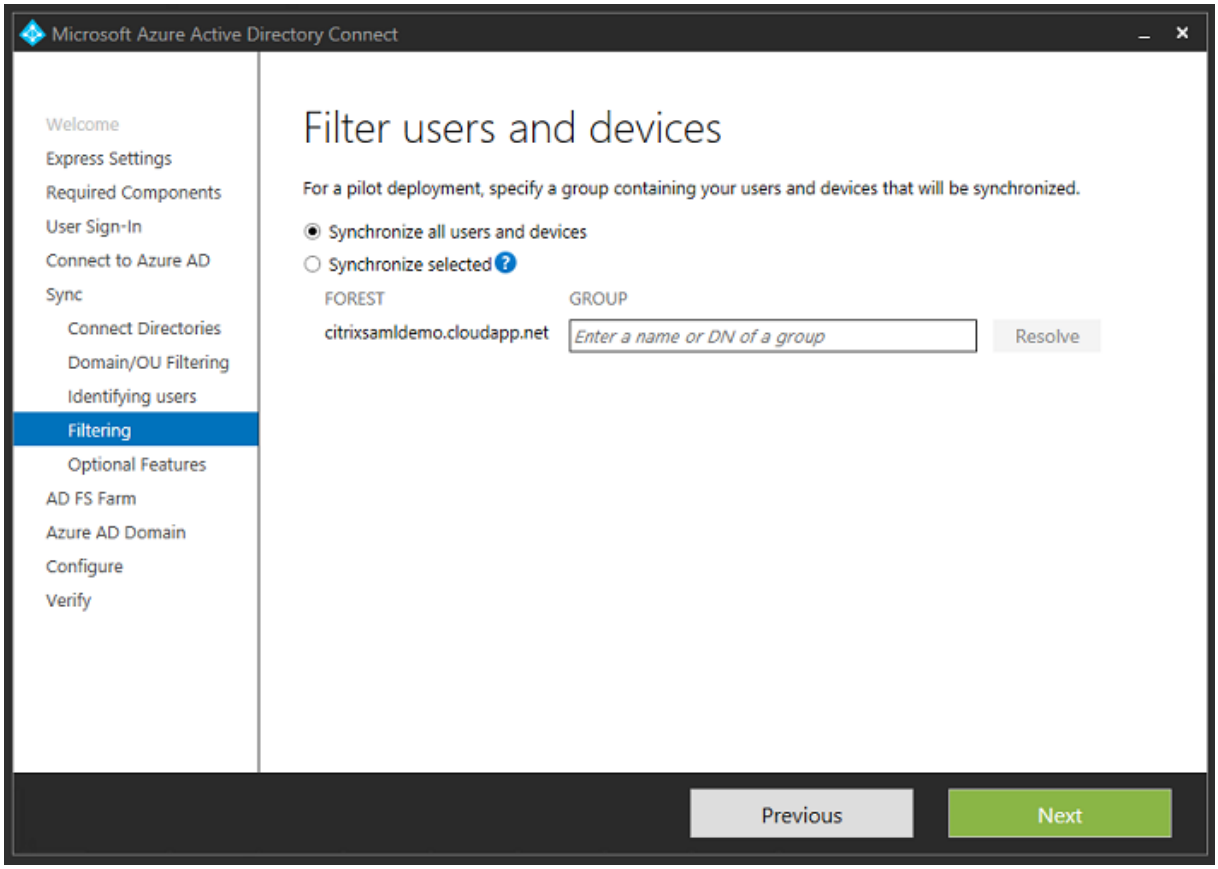
Synchronisieren Sie alle alten Active Directory-Objekte mit Azure AD.



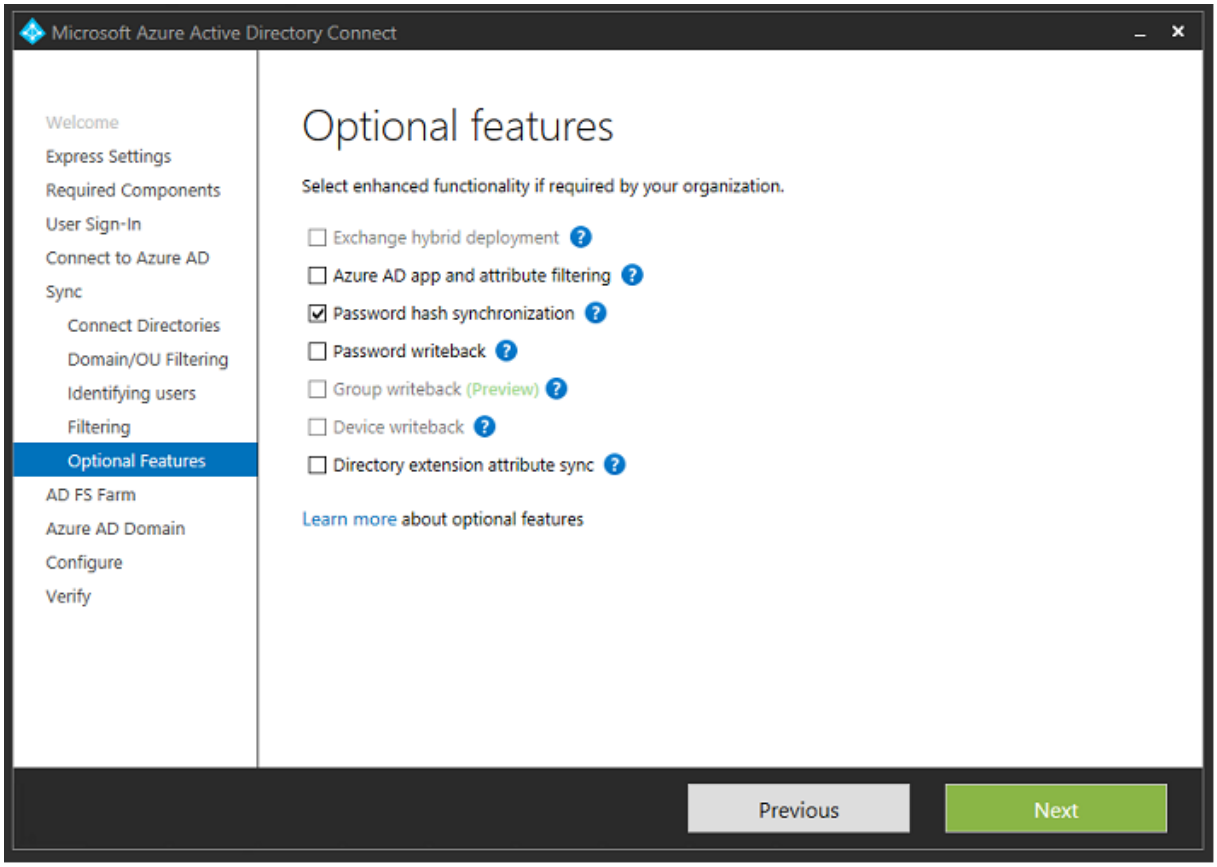
Bei einer einfachen Verzeichnisstruktur sind die Benutzernamen ausreichend eindeutig zur Identifizierung von Benutzern, die sich anmelden.



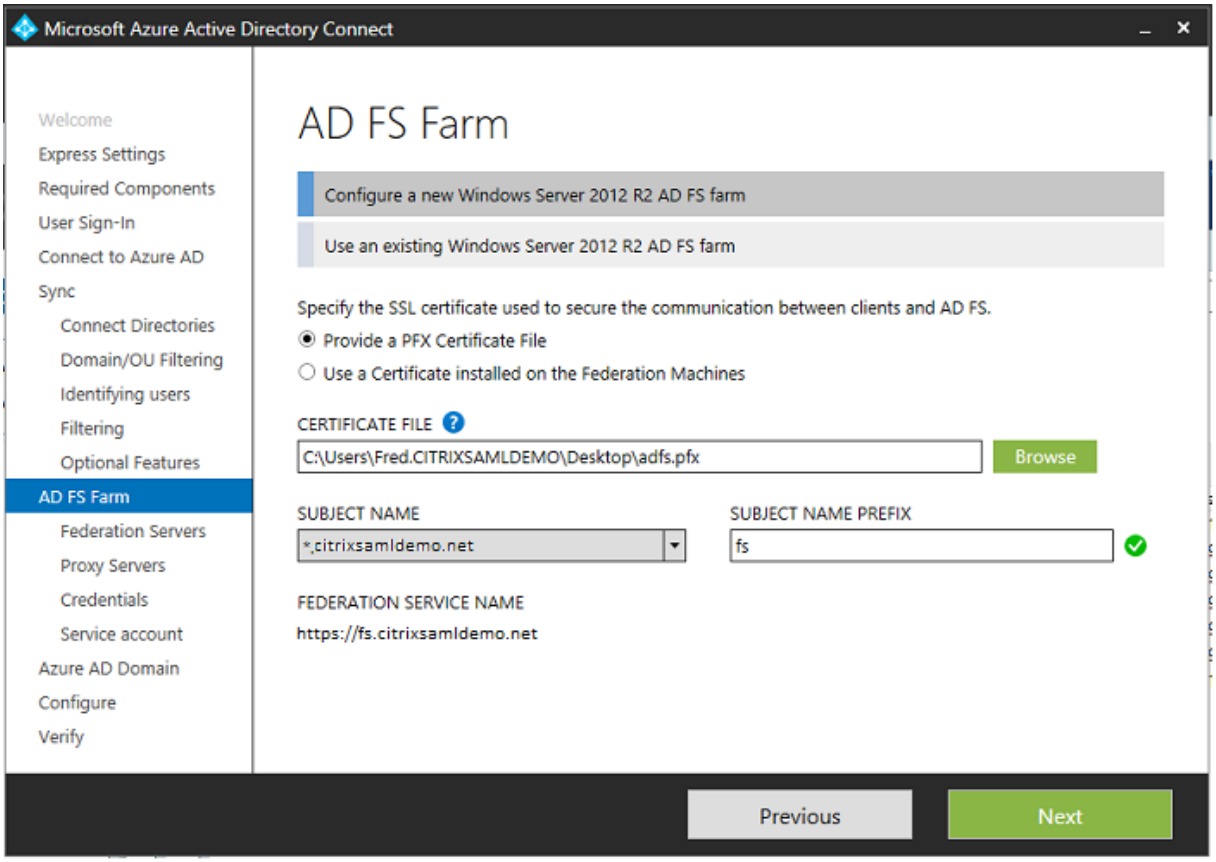
Akzeptieren Sie die Standardfilteroptionen oder schränken Sie Benutzer und Geräte auf bestimmte Gruppen ein.



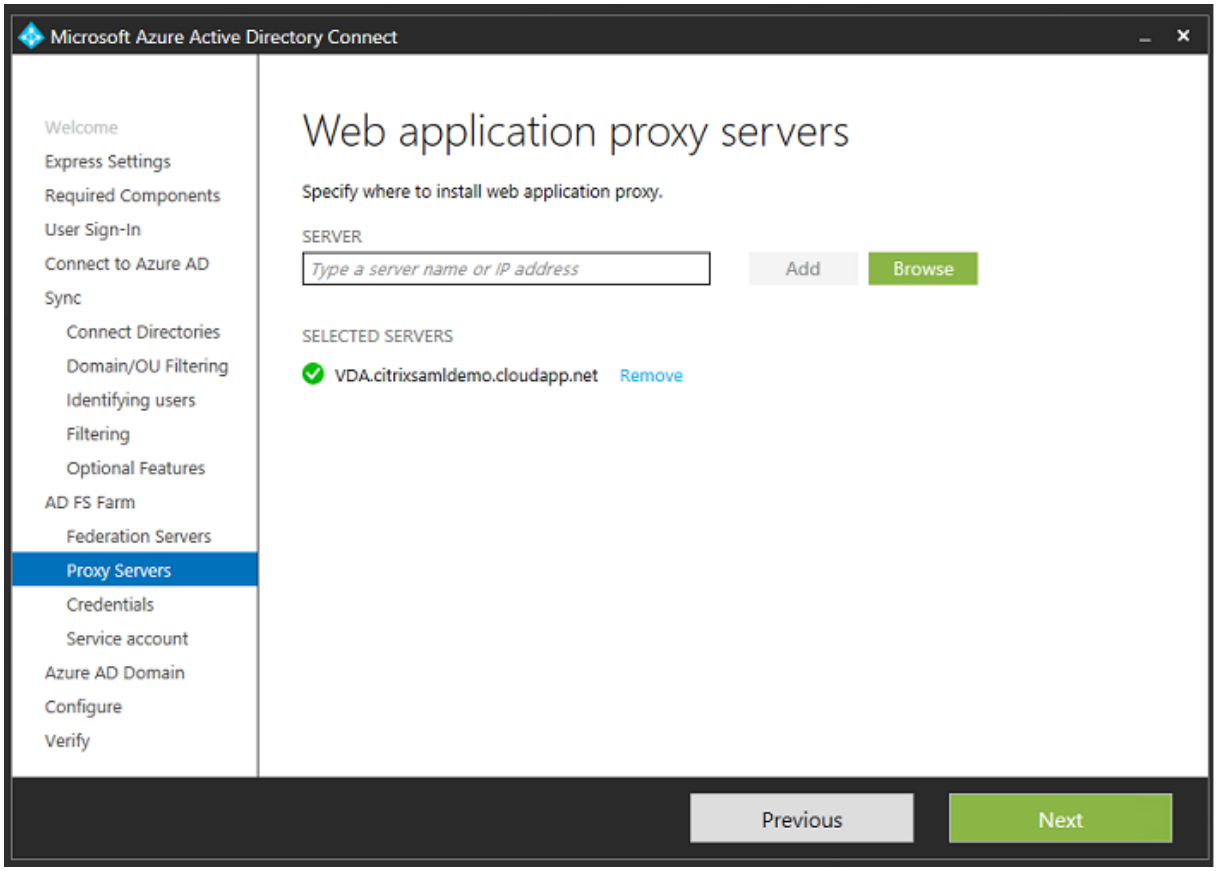
Falls gewünscht können Sie die Azure AD-Kennwörter mit Active Directory synchronisieren. Das ist für die AD FS-basierte Authentifizierung normalerweise nicht nötig.



Wählen Sie die Zertifikat-PFX-Datei für AD FS unter Angabe von “fs.citrixsamldemo.net”als DNS-Namen aus.

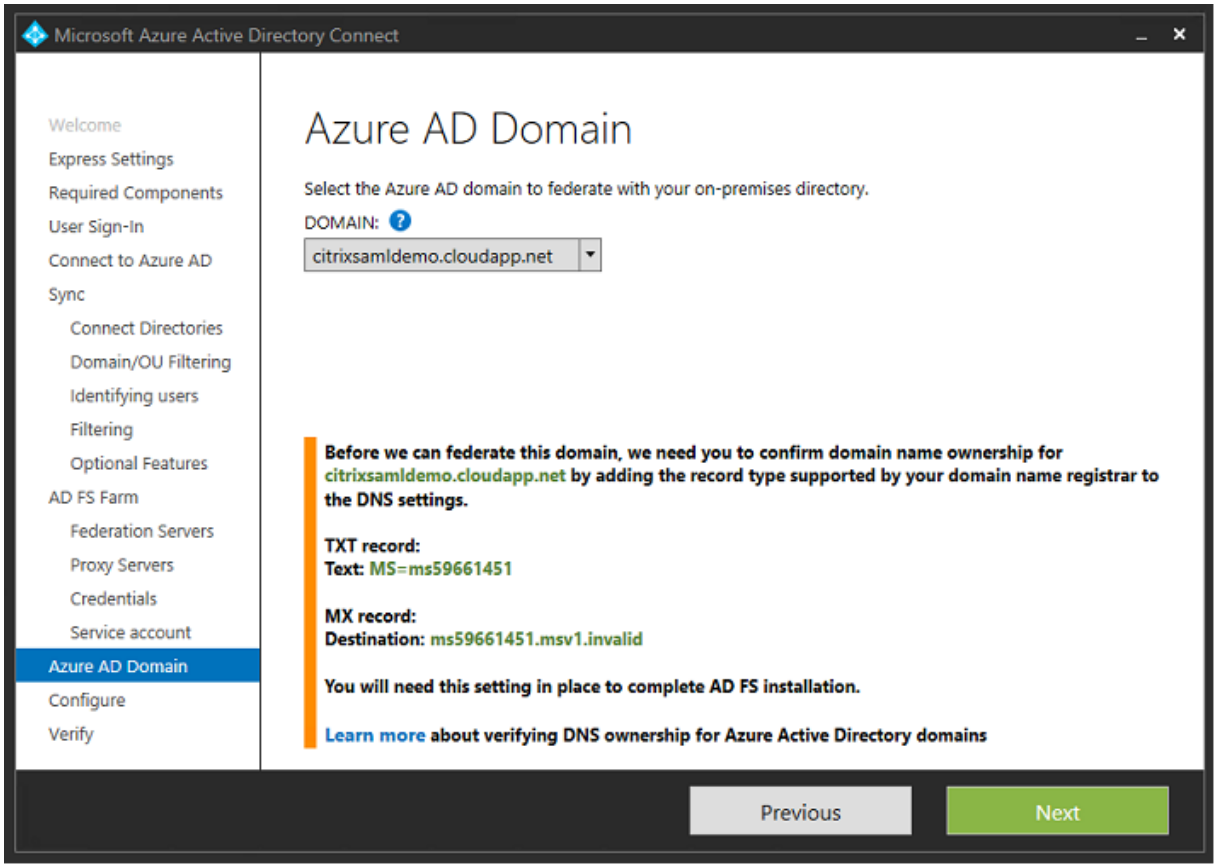


Wenn Sie zur Auswahl eines Proxyservers aufgefordert werden, geben Sie die Adresse des wap.citrixsamldemo.net-Servers ein. Sie müssen u. U. das Cmdlet **Enable-PSRemoting** –**Force** als Administrator auf dem Webanwendungsproxyserver ausführen, damit Azure AD diesen konfigurieren kann.

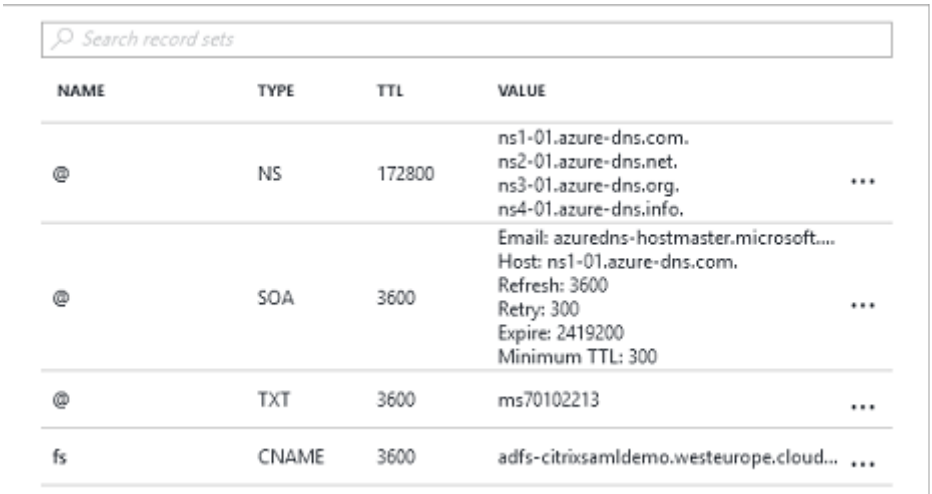


Hinweis: Wenn dieser Schritt aufgrund von Problemen mit der Remote PowerShell-Vertrauensstellung fehlschlägt, versuchen Sie den Beitritt des Webanwendungsproxyservers zur Domäne.

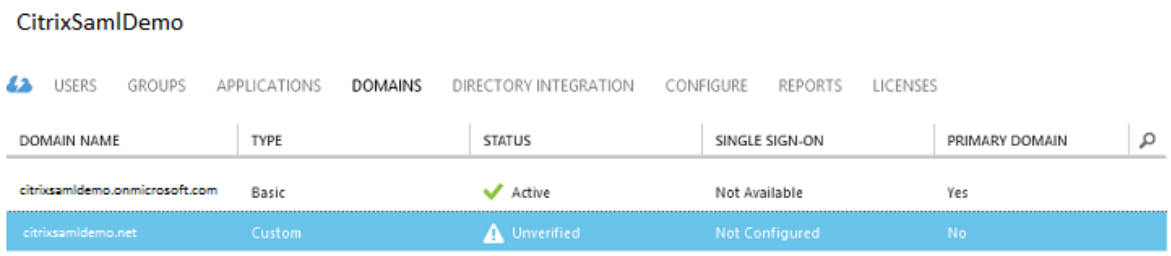
Verwenden Sie für die restlichen Schritte des Assistenten die Standardadministratorkennwörter und erstellen Sie ein Dienstkonto für AD FS. Von Azure AD Connect wird dann zur Überprüfung der Eigentümerschaft der DNS-Zone aufgefordert.



Fügen Sie die TXT- und MX-Einträge den DNS-Adresseinträgen in Azure hinzu.

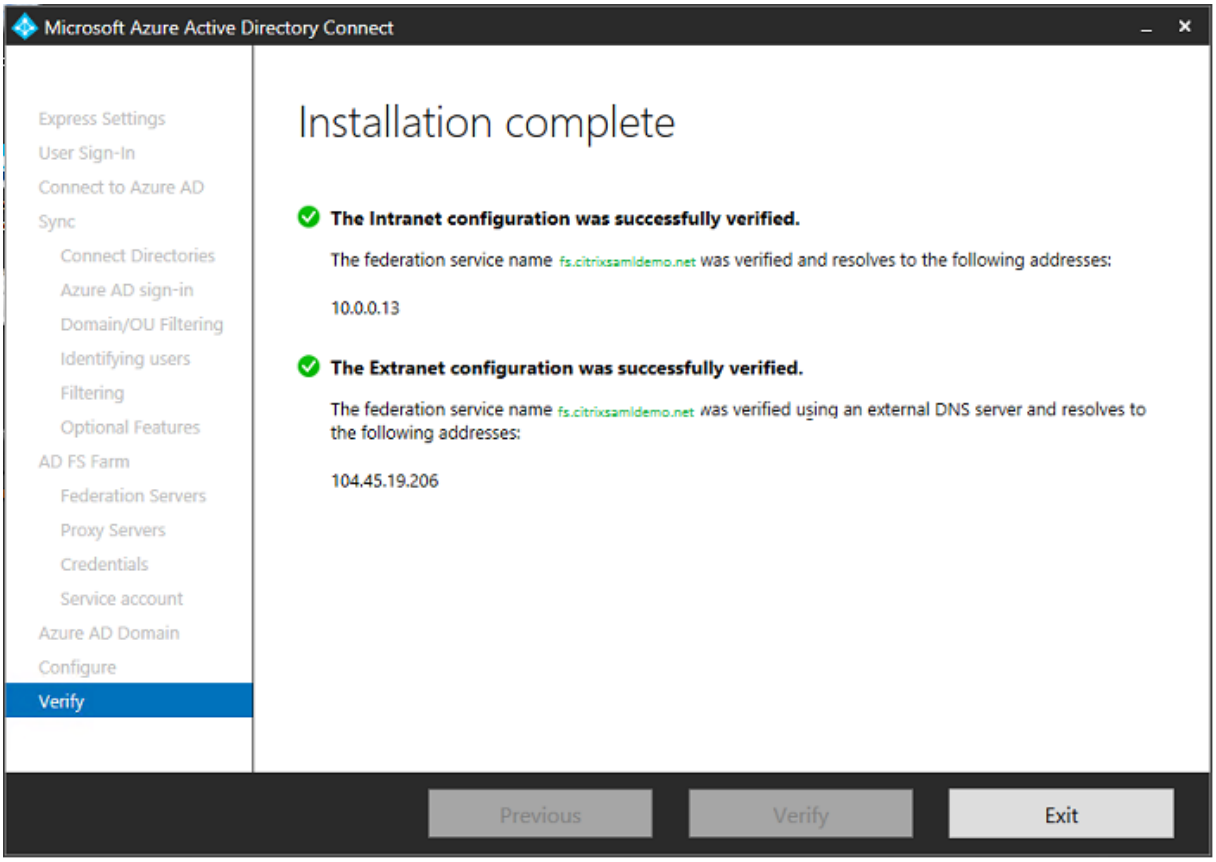


Klicken Sie in der Azure-Verwaltungskonsole auf **Überprüfen**.



Hinweis: Wenn dieser Schritt fehlschlägt, können Sie die Domäne vor Ausführung von Azure AD Connect überprüfen.

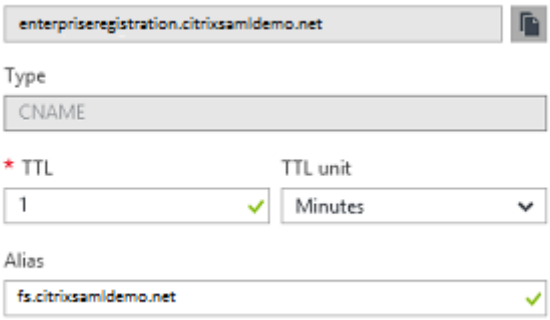
Nach Anschluss wird die externe Adresse fs.citrixsamldemo.net über Port 443 angesprochen.



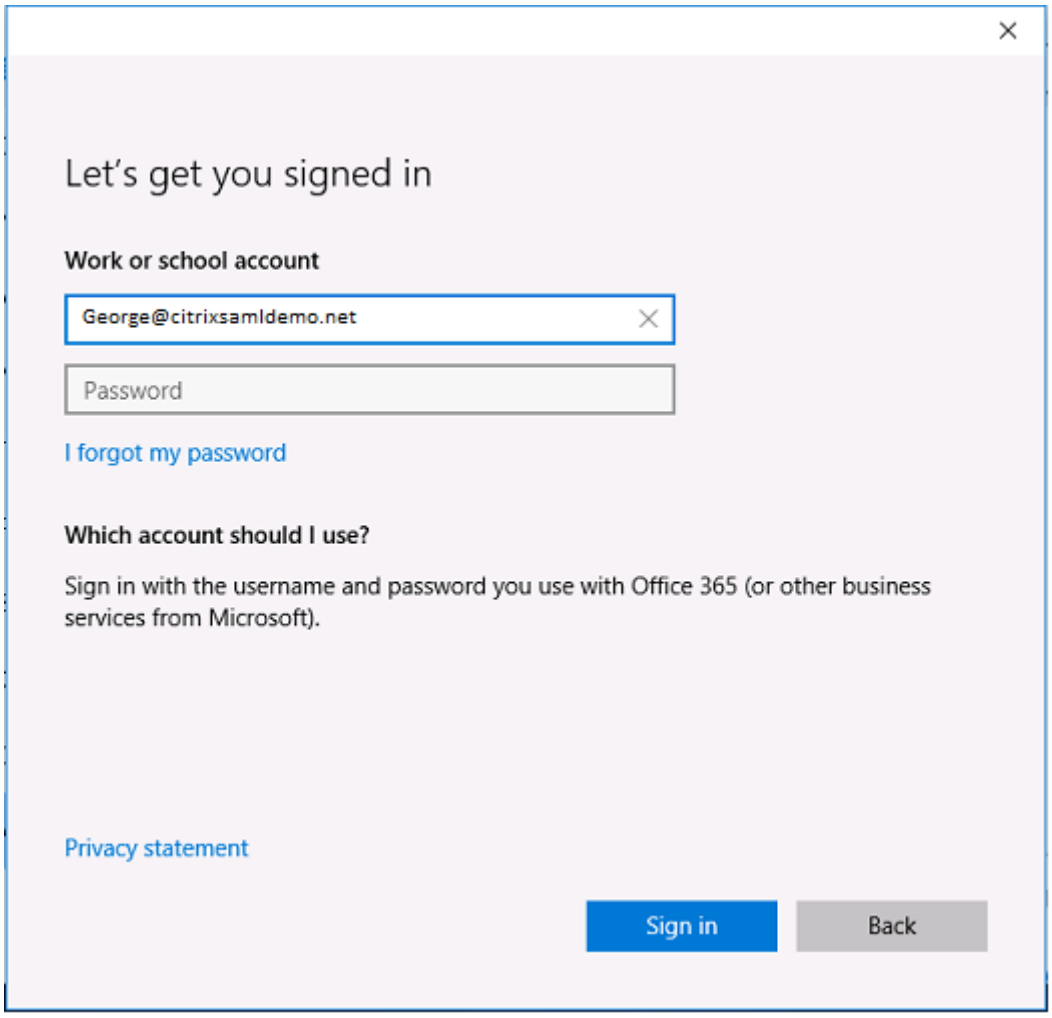
Aktivieren der Azure AD-Einbindung

Wenn ein Benutzer eine E-Mail-Adresse eingibt, sodass Windows 10 einen Beitritt zu Azure AD durchführen kann, wird das DNS-Suffix zur Erstellung eines CNAME-DNS-Eintrags verwendet, der auf ADFS: enterpriseregistration.<upnsuffix> verweisen muss.

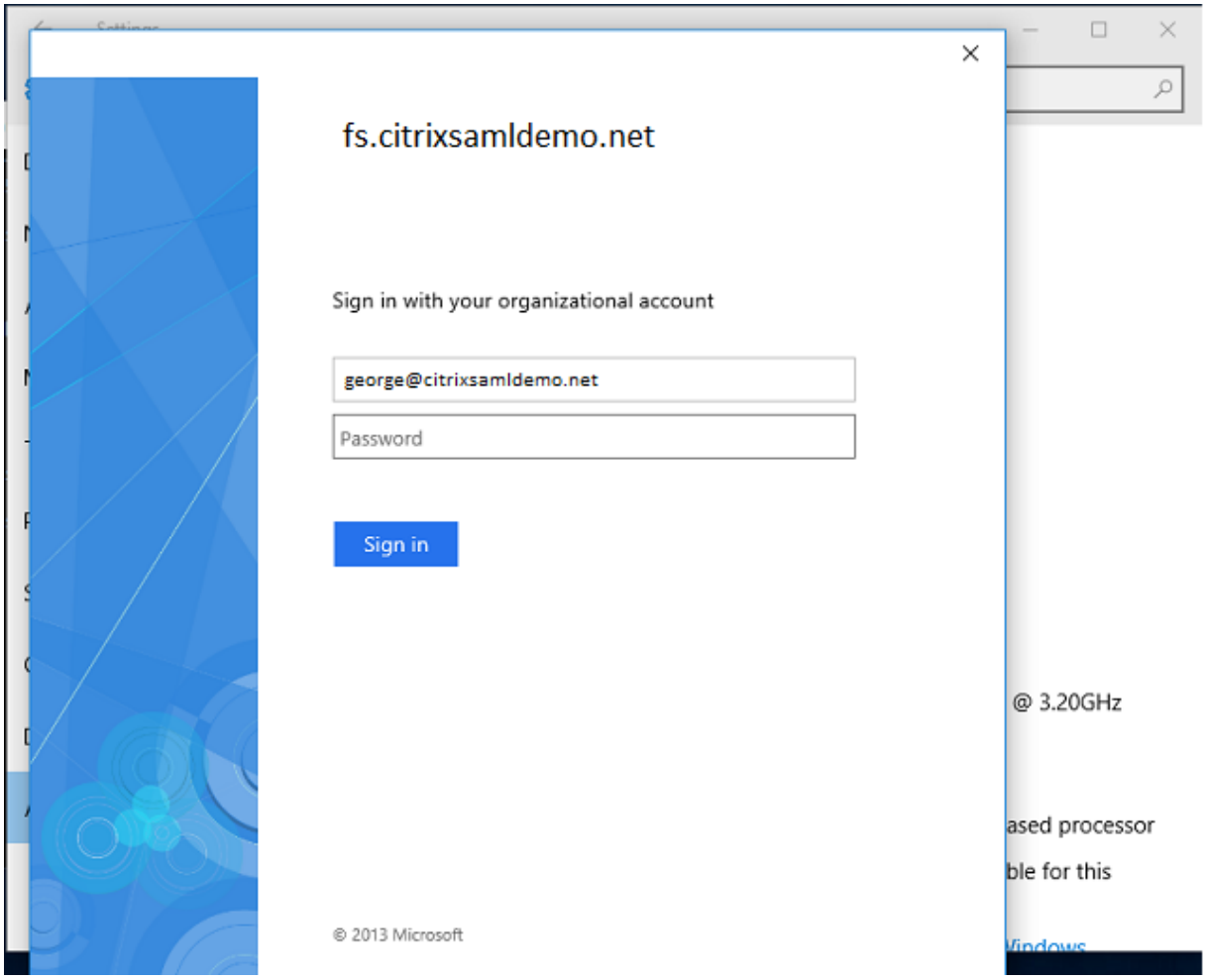
In diesem Beispiel ist dies fs.citrixsamldemo.net.

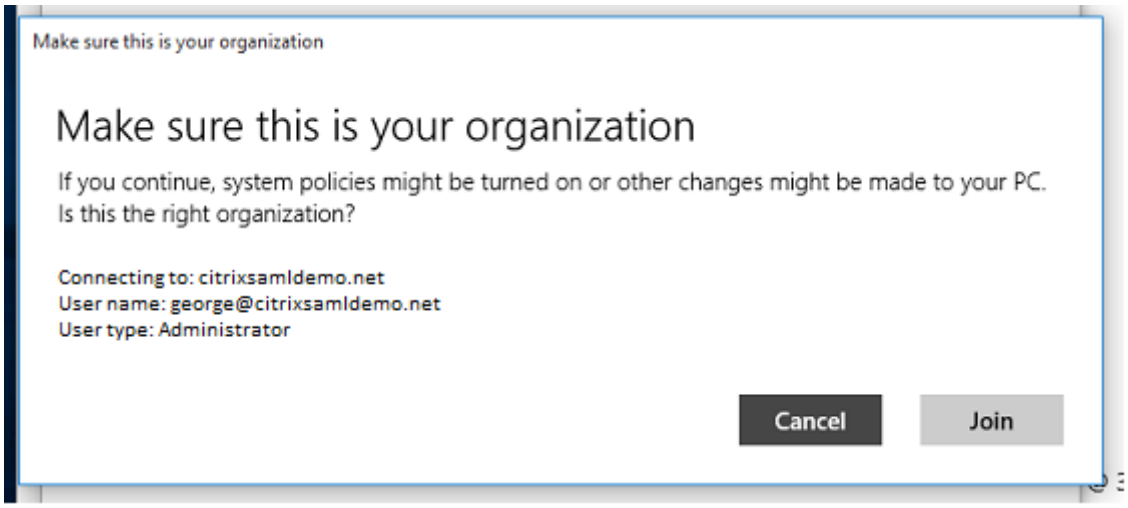


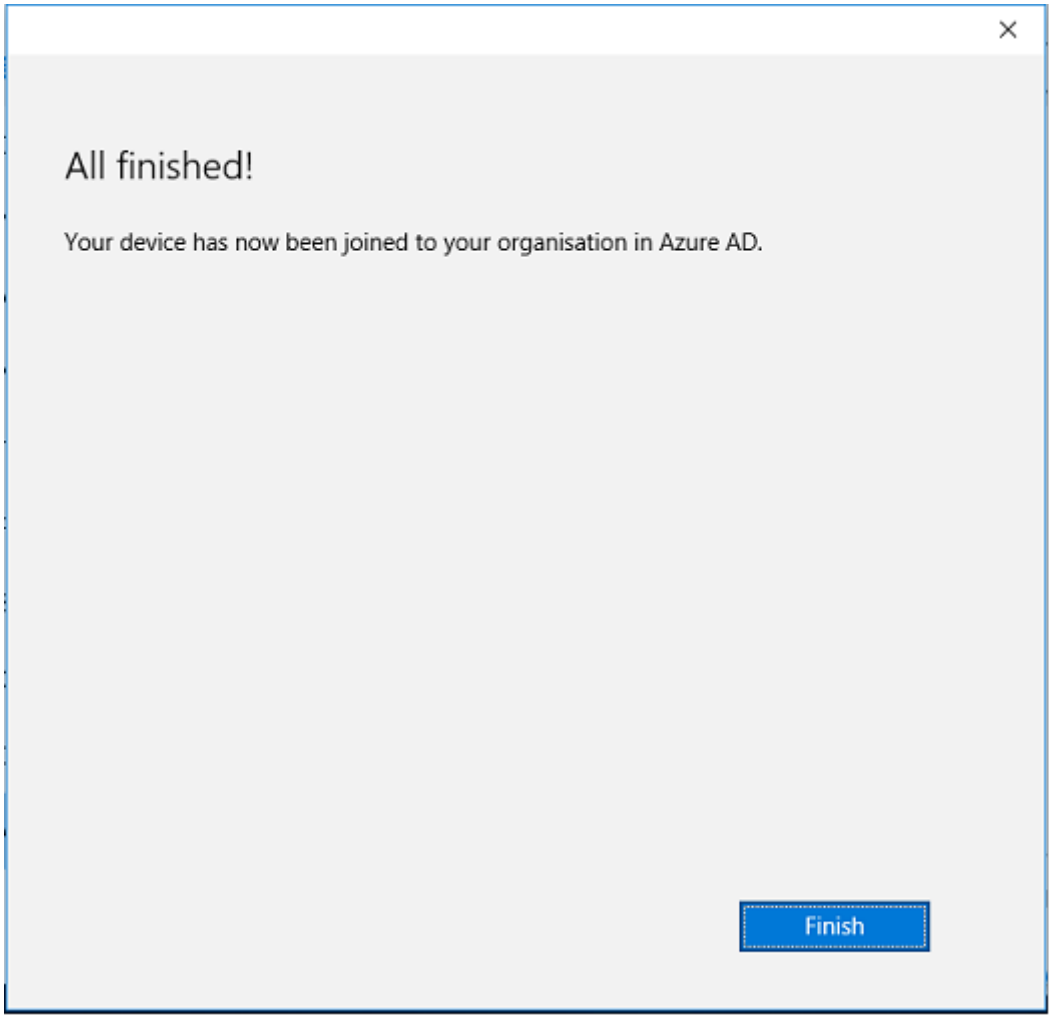
Wenn Sie keine öffentliche Zertifizierungsstelle verwenden, installieren Sie das AD FS-Stammzertifikat auf dem Windows 10-Computer, damit Windows dem AD FS-Server vertraut. Führen Sie einen Azure AD-Domänenbeitritt unter Verwendung des zuvor erstellten Standardbenutzerkontos durch.



Der UPN muss mit dem von dem AD FS-Domänencontroller erkannten UPN übereinstimmen.





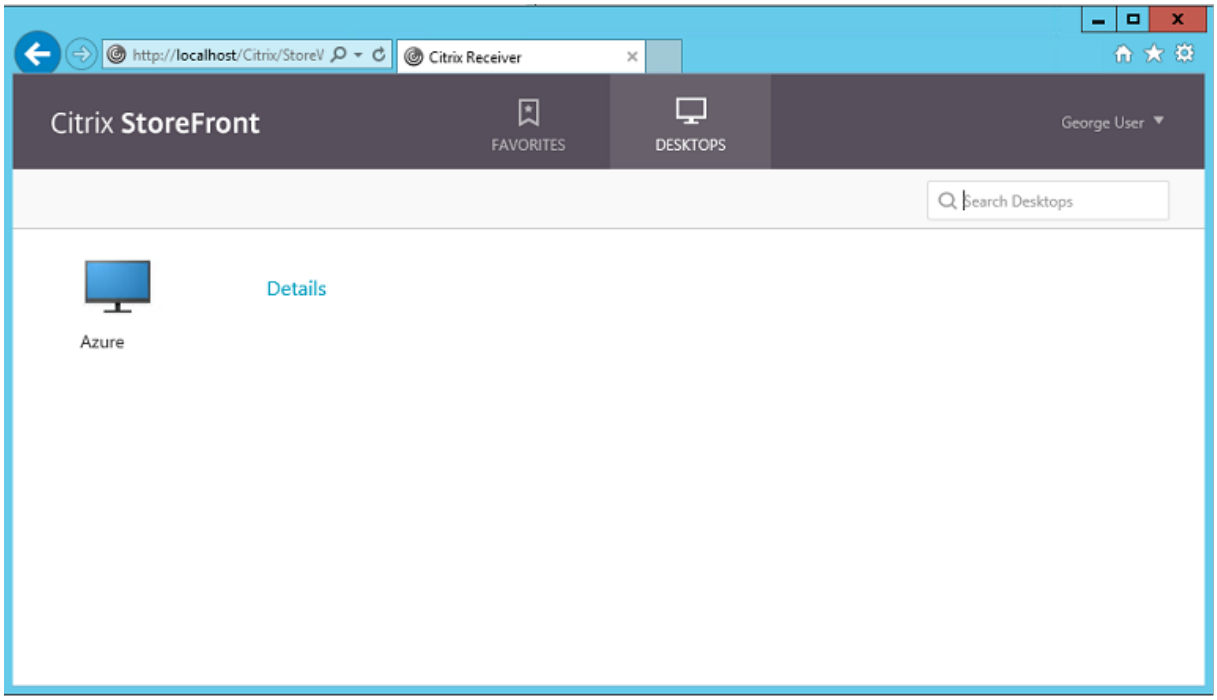


Prüfen Sie den Erfolg der Azure AD-Einbindung, indem Sie die Maschine neu starten und sich mit der E-Mail-Adresse des Benutzers anmelden. Nach der Anmeldung starten Sie Microsoft Edge und stellen Sie eine Verbindung mit https://myapps.microsoft.com her. Die Website müsste Single Sign-On automatisch verwenden.

Installieren von XenApp oder XenDesktop

Sie können die virtuellen Maschinen für Delivery Controller und VDA in Azure direkt vom XenApp- bzw. XenDesktop-ISO-Image normal installieren.

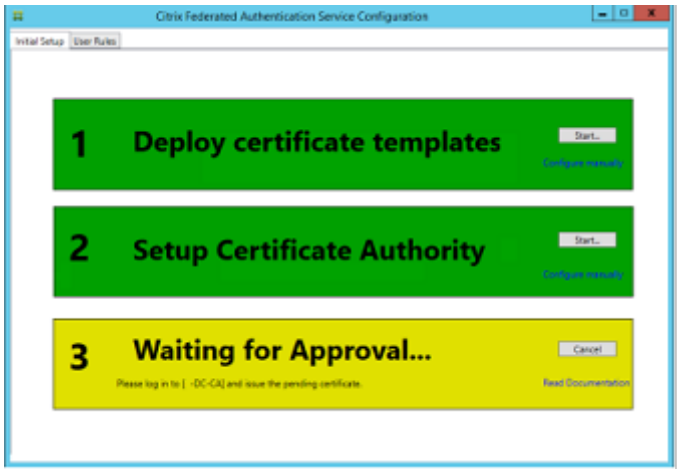
In diesem Beispiel wird StoreFront auf demselben Server wie der Delivery Controller installiert. Der VDA wird als eigenständiger Windows 2012 R2 RDS-Worker ohne Integration in Maschinenerstellungsdienste installiert (optional könnte dies aber konfiguriert werden). Vergewissern Sie sich bevor Sie fortfahren, dass der Benutzer George@citrixsamldemo.net sich mit einem Kennwort authentifizieren kann.

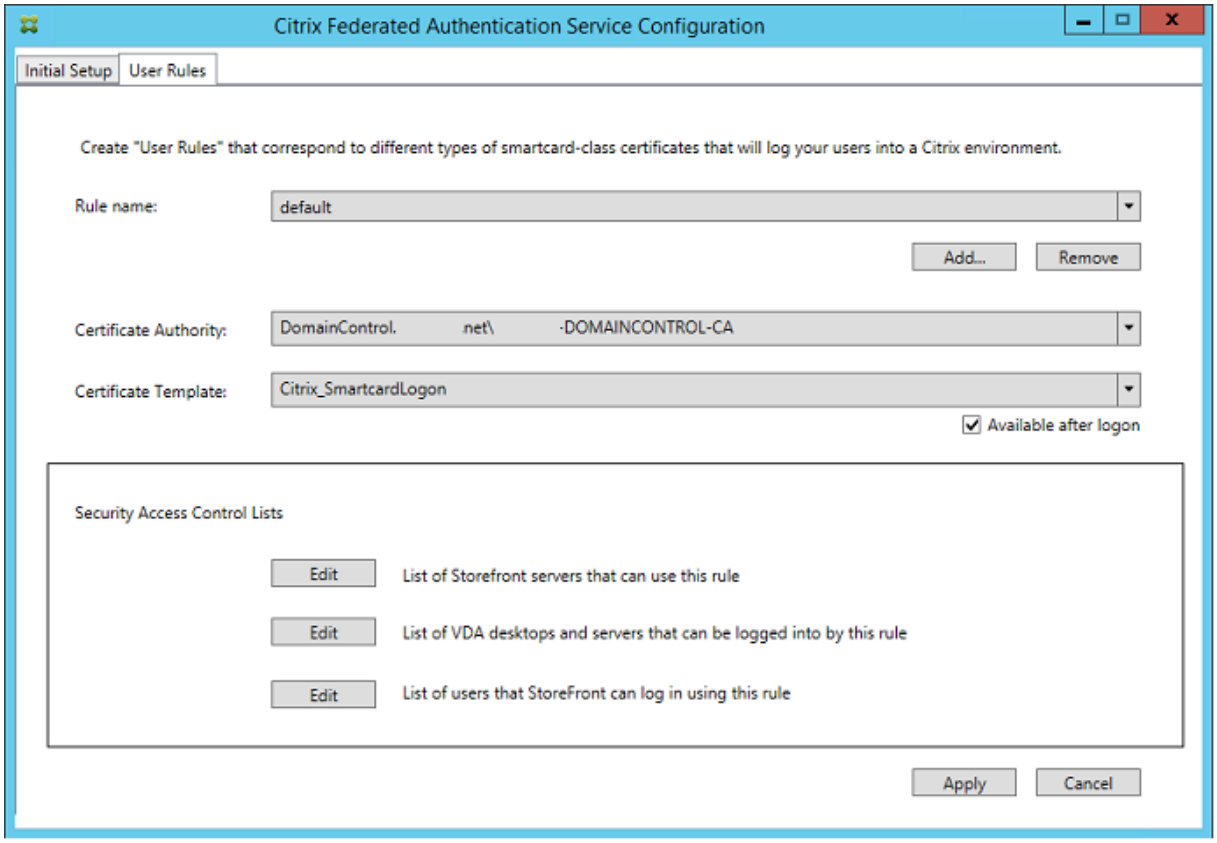


Führen Sie das PowerShell-Cmdlet **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** auf dem Controller aus, damit StoreFront eine Authentifizierung ohne Anmeldeinformationen des Benutzers durchführen kann.

Installieren des Verbundauthentifizierungsdiensts

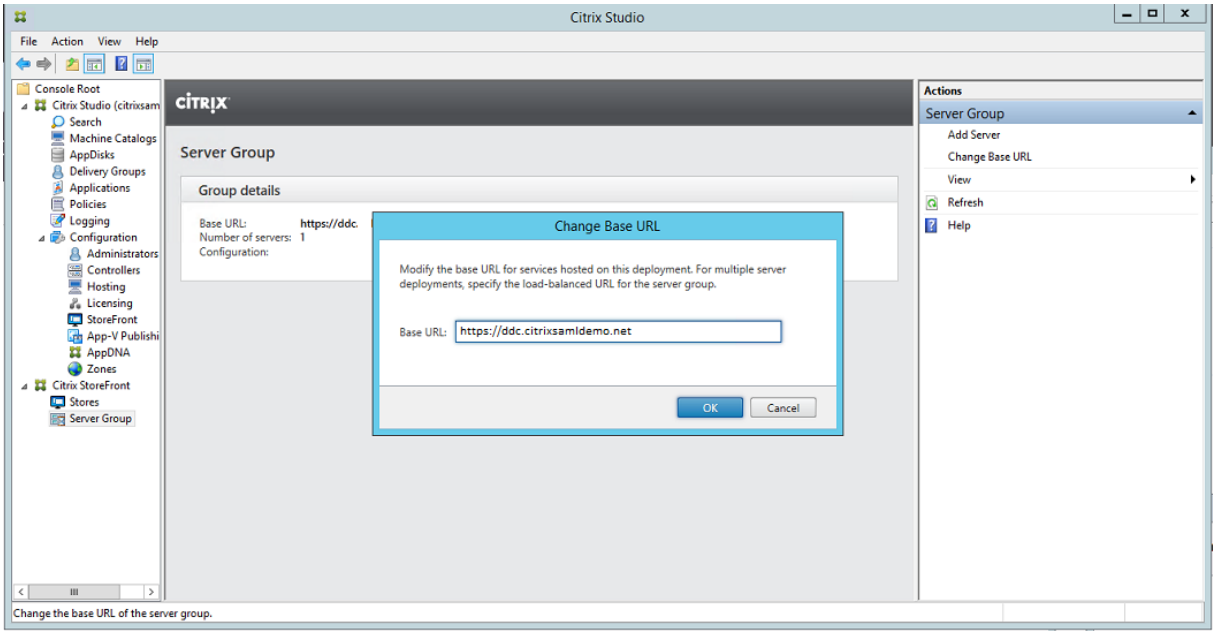
Installieren Sie den Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) auf dem AD FS-Server und konfigurieren Sie eine Regel, durch die der Controller als vertrauenswürdige StoreFront agiert.



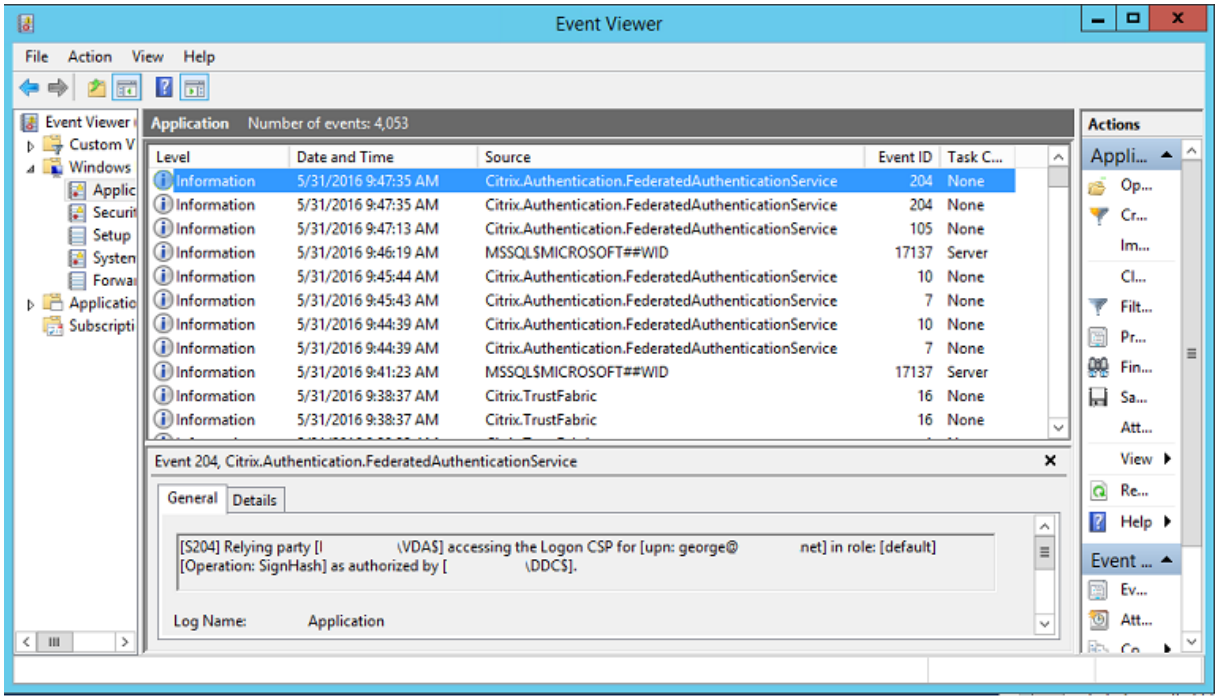


Konfigurieren von StoreFront

Fordern Sie ein Computerzertifikat für den Delivery Controller an und konfigurieren Sie IIS und StoreFront für HTTPS, indem Sie eine IIS-Bindung für Port 443 festlegen und die StoreFront-Basisadresse in “https:”ändern.

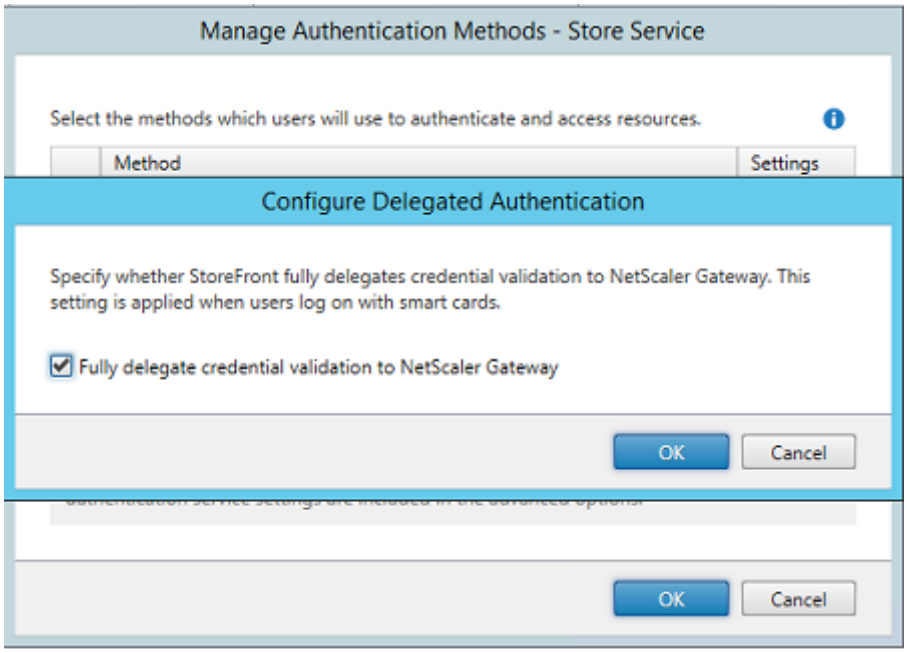


Konfigurieren Sie StoreFront für die Verwendung des FAS-Servers (mit dem PowerShell-Skript aus dem Artikel Verbundauthentifizierungsdienst) und führen Sie Azure-intern einen Test durch. Vergewissern Sie sich dabei, dass die Anmeldung über FAS geht, indem Sie die Ereignisanzeige des FAS-Servers prüfen.

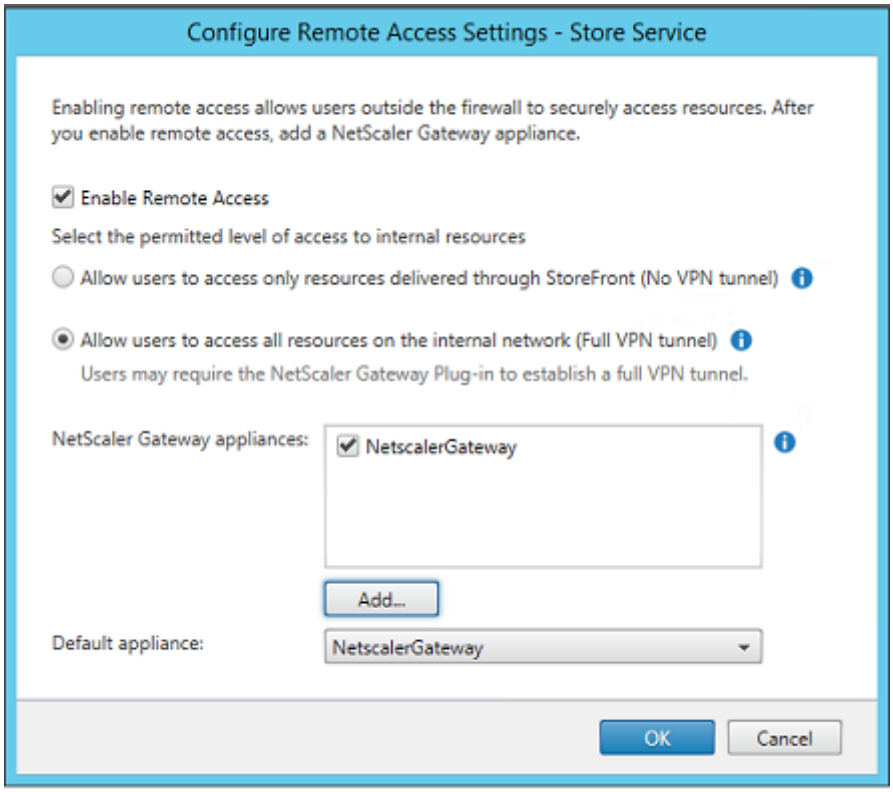


Konfigurieren von StoreFront zur Verwendung von NetScaler

Konfigurieren Sie im Bereich **Authentifizierungsmethoden verwalten** der StoreFront-Verwaltungskonsole StoreFront für die Authentifizierung über NetScaler.

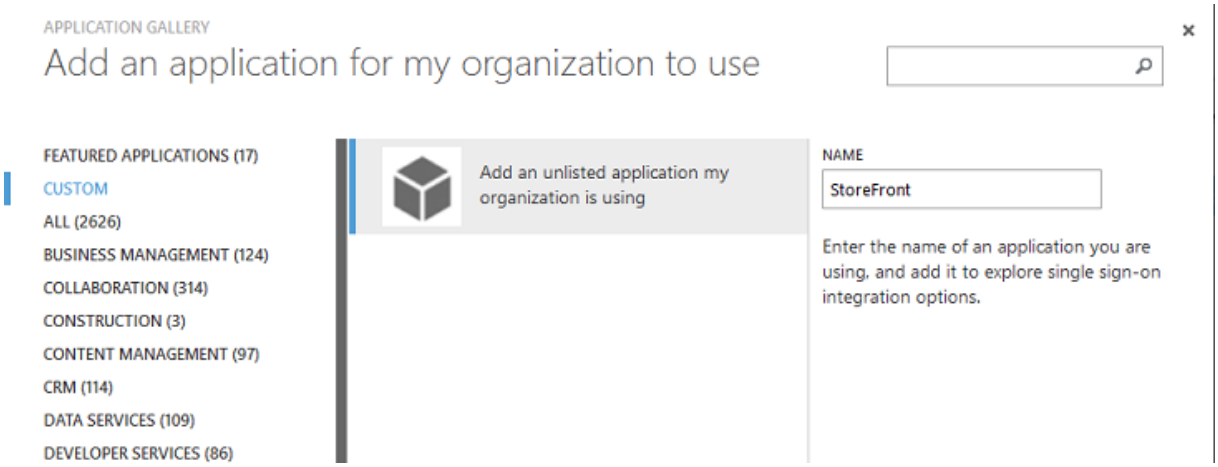


Zum Integrieren der NetScaler-Authentifizierungsoptionen konfigurieren Sie eine Secure Ticket Authority (STA) und konfigurieren Sie die NetScaler Gateway-Adresse.



Konfigurieren einer neuen Azure-Anwendung für das Single Sign-On bei StoreFront

In diesem Abschnitt werden die Single Sign-On-Features von Azure AD SAML 2.0 verwendet, die zurzeit ein Azure Active Directory Premium-Abonnement erfordern. Wählen Sie in der Azure AD-Verwaltung **Neue Anwendung** und **Anwendung aus dem Katalog hinzufügen**.



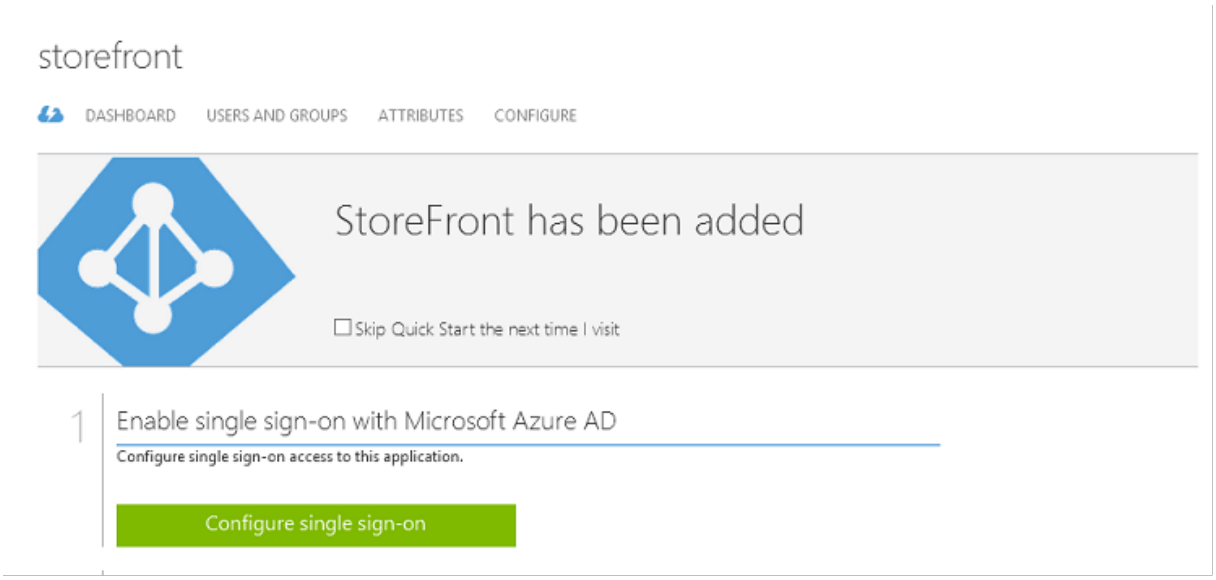
Wählen Sie **BENUTZERDEFINIERT > Eine nicht aufgeführte von meiner Organisation eingesetzte Anwendung hinzufügen**, um eine neue benutzerdefinierte Anwendung für die Benutzer zu erstellen.

Konfigurieren eines Symbols

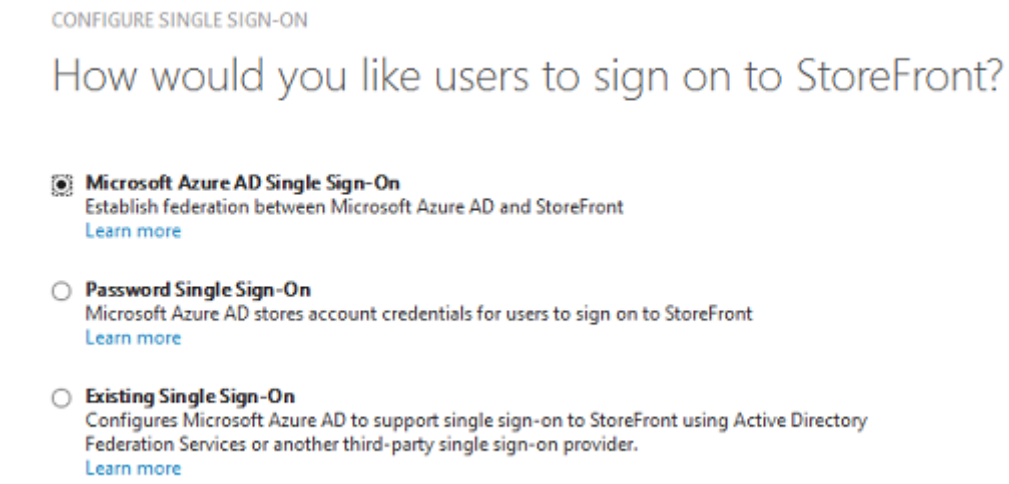
Erstellen Sie ein 215 x 215 Pixel großes Bild und laden Sie es auf der Seite KONFIGURIEREN hoch, um es als Symbol für die Anwendung zu verwenden.

Konfigurieren der SAML-Authentifizierung

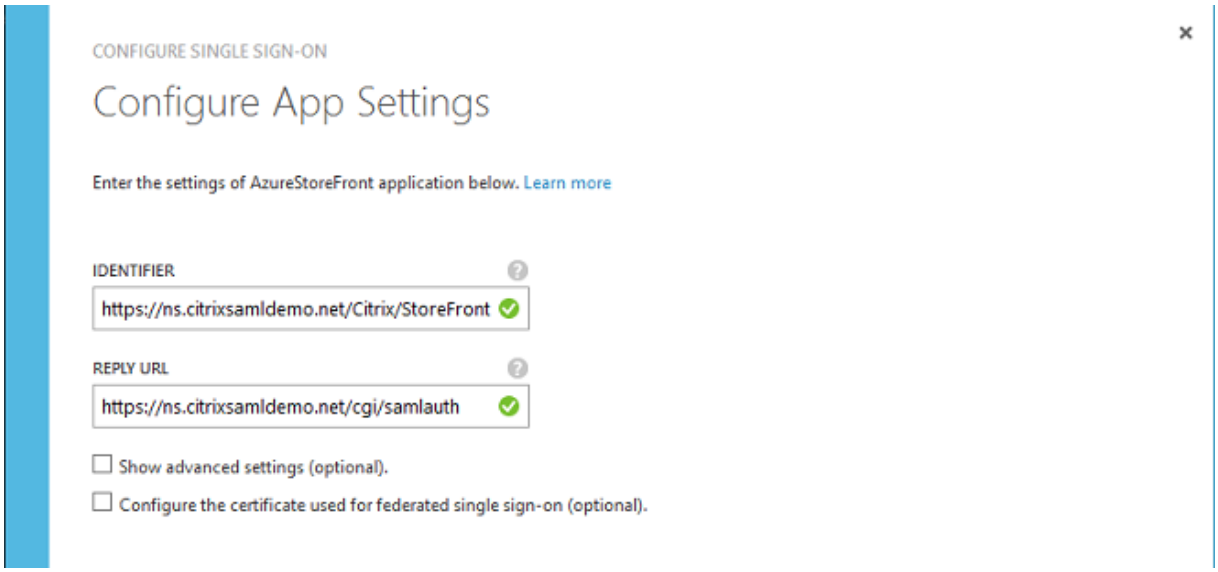
Kehren Sie auf die Dashboard-Übersichtsseite zurück und wählen Sie **Single Sign-On konfigurieren**.



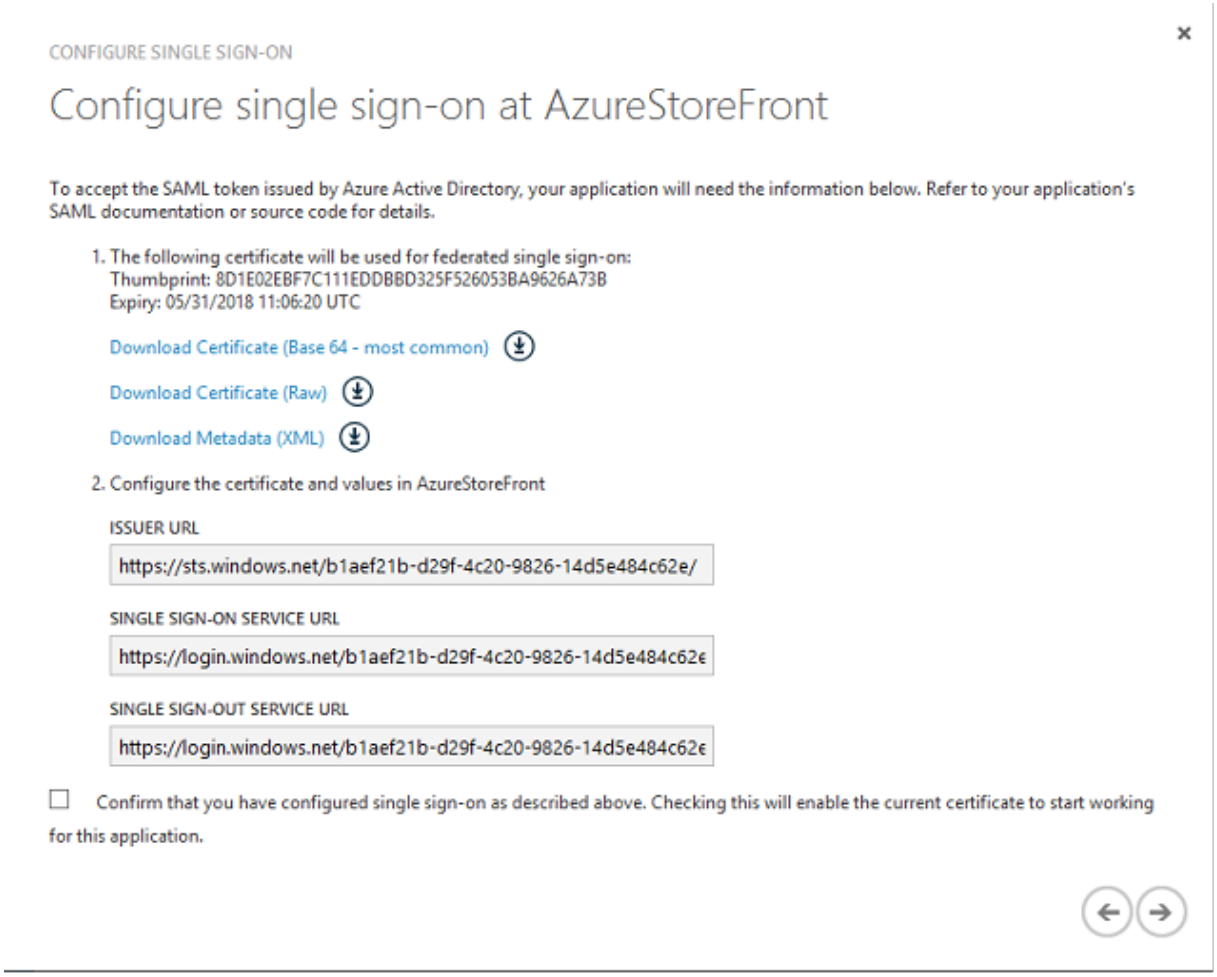
In dieser Bereitstellung wird die SAML 2.0-Authentifizierung verwendet. Dies entspricht **Single Sign-On** in Microsoft Azure AD.



Die **Kennung** darf eine beliebige Zeichenfolge sein (sie muss mit der für NetScaler bereitgestellten Konfiguration übereinstimmen). Im vorliegenden Beispiel ist die **Antwort-URL** auf dem NetScaler-Server /cgi/samlauth.



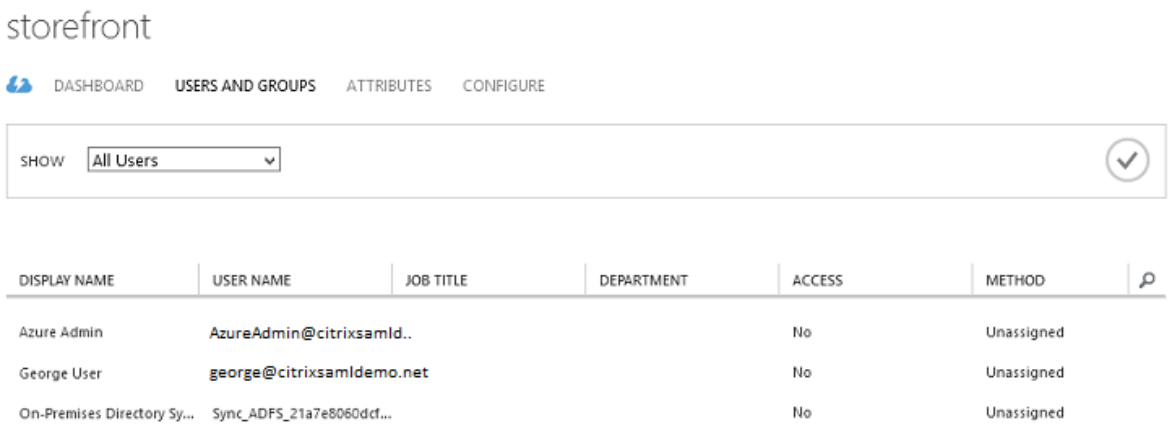
Die nächste Seite enthält Informationen zum Konfigurieren von NetScaler als vertrauende Seite für Azure AD.



Laden Sie das vertrauenswürdige Base-64-Signaturzertifikat herunter und kopieren Sie die Sign-On- und die Sign-Out-URL. Diese fügen Sie später bei der NetScaler-Konfiguration ein.

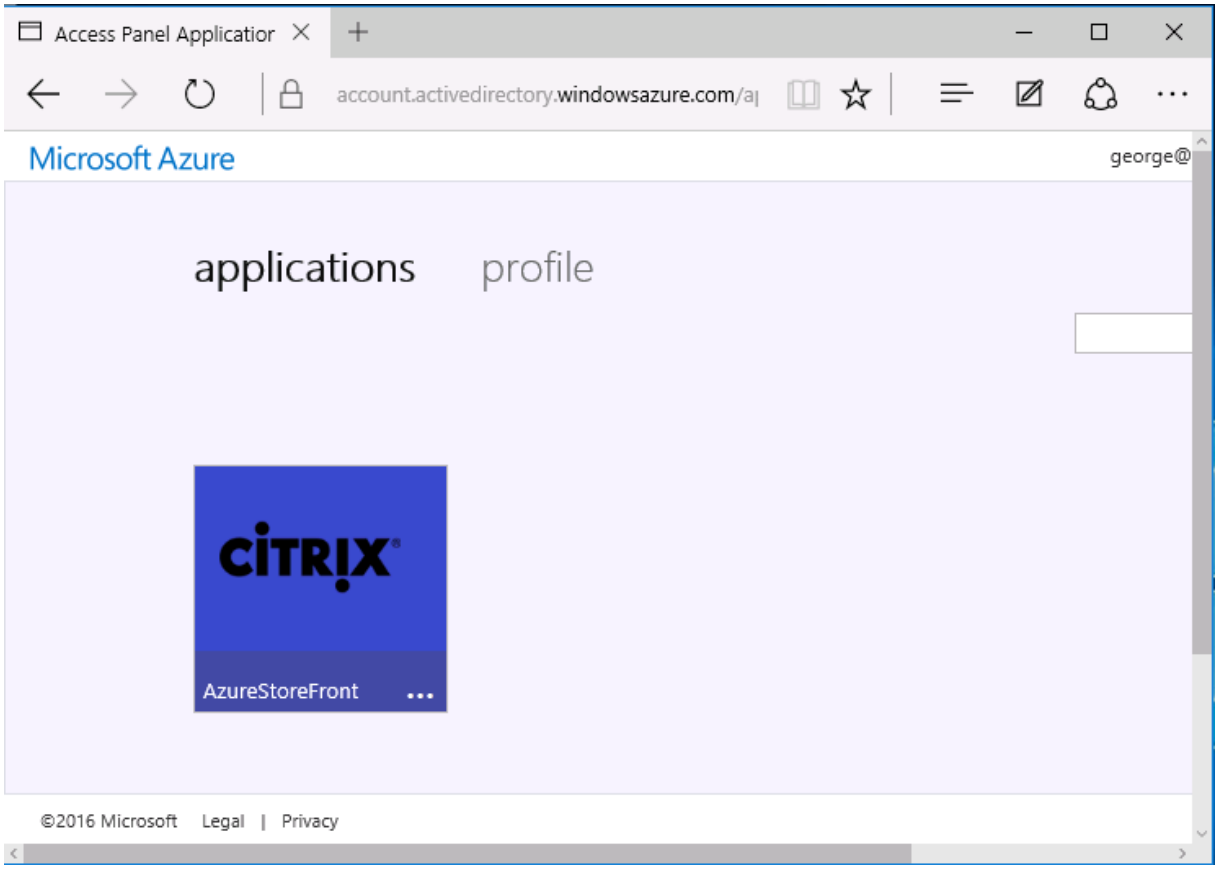
Zuweisen der Anwendung zu Benutzern

Der letzte Schritt besteht in der Aktivierung der Anwendung, damit sie für die Benutzer auf der Steuerungsseite "myapps.microsoft.com"angezeigt wird. Dafür wird die Seite BENUTZER UND GRUPPEN verwendet. Weisen Sie Zugriff für die über Azure AD Connect synchronisierten Domänenbenutzerkonten zu. Andere Konten können ebenfalls verwendet werden, sie müssen jedoch explizit zugeordnet werden, da sie nicht dem Muster <user>@<domain> entsprechen.



Seite "MyApps"

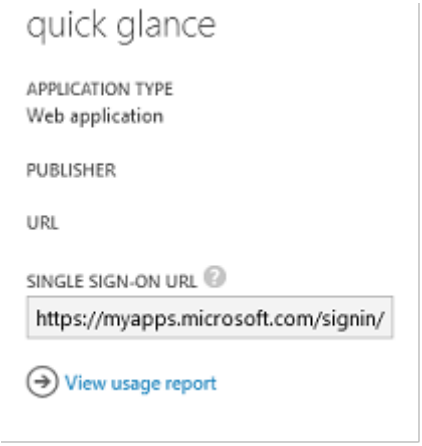
Wenn die Anwendung konfiguriert wurde, wird sie in der Azure-Anwendungsliste angezeigt, wenn die Benutzer https://myapps.microsoft.com besuchen.



Wenn Windows 10 Azure AD beigetreten ist, unterstützt es Single Sign-On für Azure-Anwendungen. Bei einem Klick auf das Symbol wird der Browser an die zuvor konfigurierte SAML-Webseite cgi/samlauth umgeleitet.

URL für Single Sign-On

Kehren Sie zu der Anwendung im Azure AD-Dashboard zurück. Es gibt jetzt eine Single Sign-On-URL für die Anwendung. Diese URL wird zur Erstellung von Browserlinks und Startmenüverknüpfungen verwendet, die die Benutzer direkt an StoreFront umleiten.



Fügen Sie diese URL in einen Webbrowser ein, um sicherzustellen, dass Sie von Azure AD an die zuvor konfigurierte NetScaler-Webseite cgi/samlauth umgeleitet werden. Dies funktioniert nur dann, wenn ein Benutzer zugewiesen wurde, zudem ist Single Sign-On nur bei Anmeldungssitzungen möglich, wenn Windows 10 Azure AD beigetreten ist. (Andere Benutzer werden aufgefordert, ihre Azure AD-Anmeldeinformationen einzugeben.)

Installieren und Konfigurieren von NetScaler Gateway

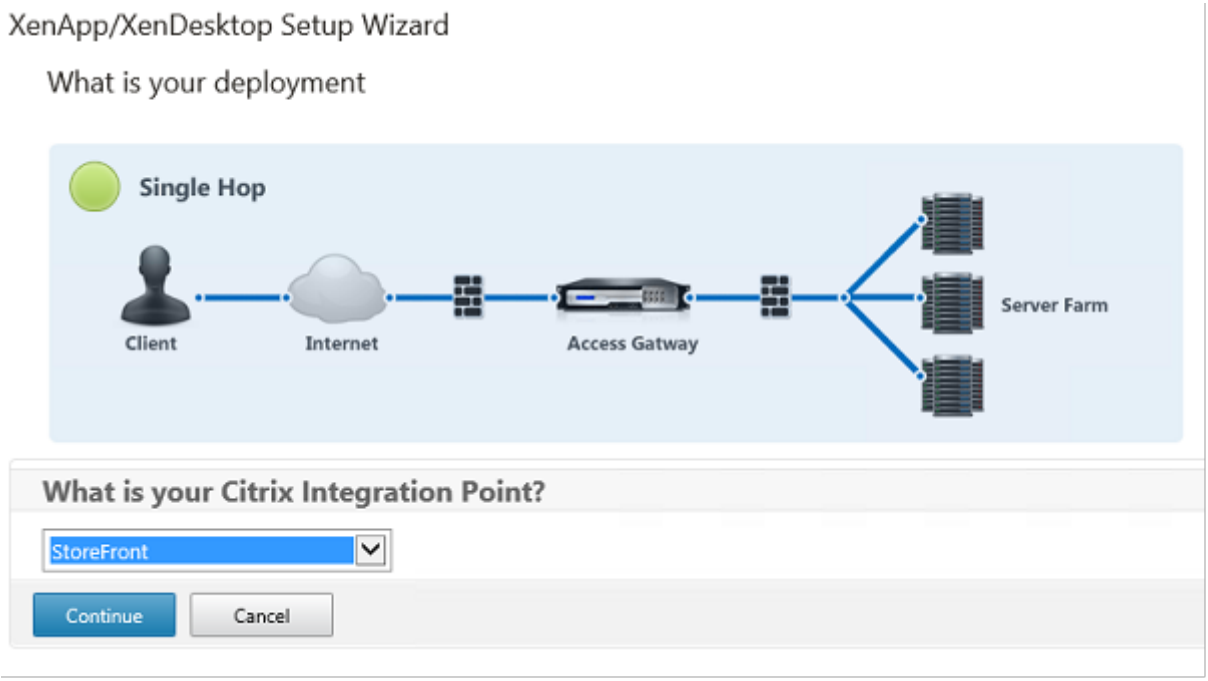
Für den Remote-Zugriff auf die Bereitstellung wird in diesem Beispiel eine separate VM mit NetScaler verwendet. Diese kann im Azure-Store erworben werden. In diesem Beispiel wird die “Bring your own License”-Lizenzversion für NetScaler 11.0 verwendet.

Melden Sie sich bei der NetScaler-VM an, indem Sie im Webbrowser die interne IP-Adresse und die bei der Benutzerauthentifizierung angegebenen Anmeldeinformationen eingeben. Sie müssen das Kennwort des nsroot-Benutzers in einer Azure AD-VM ändern.

Fügen Sie Lizenzen hinzu (führen Sie nach dem Hinzufügen jeder Lizenz einen **Neustart** durch) und verweisen Sie die DNS-Auflösung an den Microsoft-Domänencontroller.

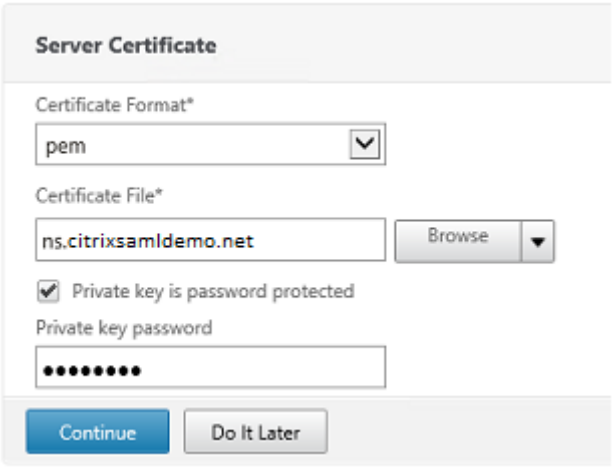
Ausführen des XenApp- und XenDesktop-Setupassistenten

In diesem Beispiel wird zunächst eine einfache StoreFront-Integration ohne SAML konfiguriert. Wenn diese Bereitstellung betriebsbereit ist, wird eine SAML-Anmelderichtlinie hinzugefügt.



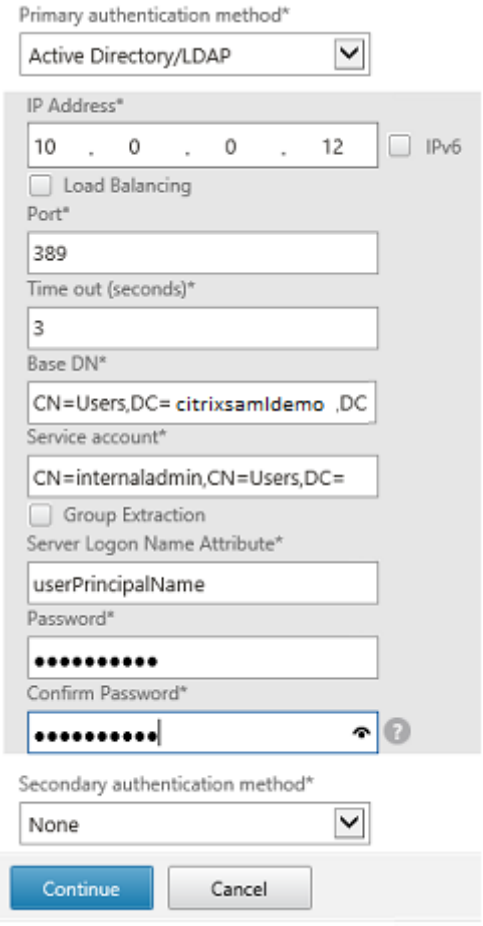
Wählen Sie die standardmäßigen NetScaler-StoreFront-Einstellungen. Zur Verwendung in Microsoft Azure wird in diesem Beispiel Port 4433 anstelle von Port 443 konfiguriert. Alternativ können Sie eine Portweiterleitung einrichten oder die Zuweisung der Verwaltungswebsite von NetScaler ändern.

Der Einfachheit halber wird in diesem Beispiel ein in einer Datei gespeichertes, vorhandenes Serverzertifikat mit privatem Schlüssel hochgeladen.



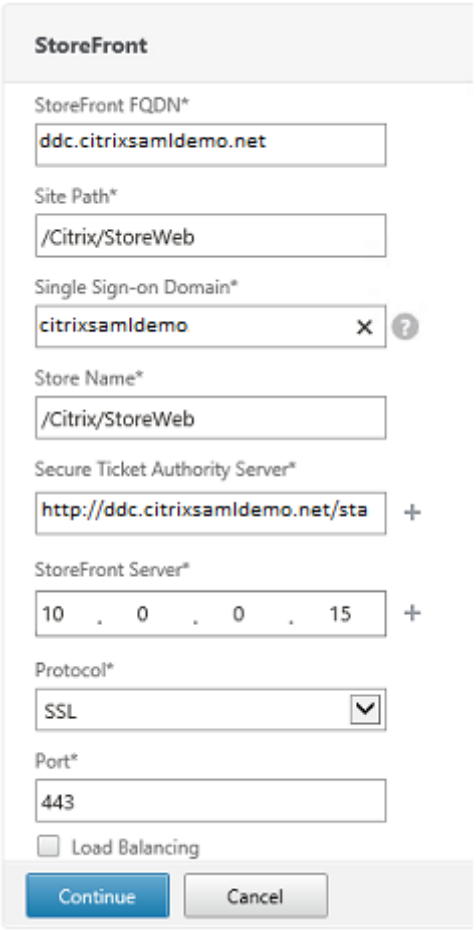
Konfigurieren des Domänencontrollers für die AD-Kontoverwaltung

Der Domänencontroller wird zur Kontoauflösung verwendet. Fügen Sie daher seine IP-Adresse in die primäre Authentifizierungsmethode ein. Beachten Sie die in den einzelnen Feldern im Dialogfeld erforderlichen Formate.



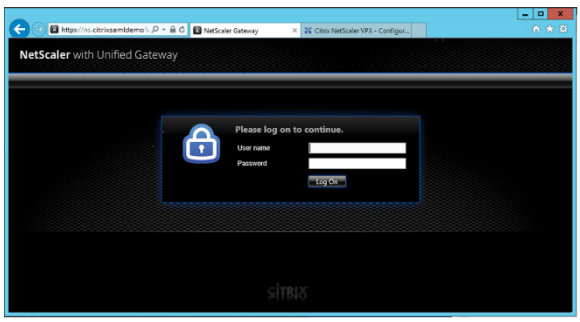
Konfigurieren der StoreFront-Adresse

In diesem Beispiel wurde StoreFront für HTTPS konfiguriert. Wählen Sie daher die SSL-Protokolloptionen.



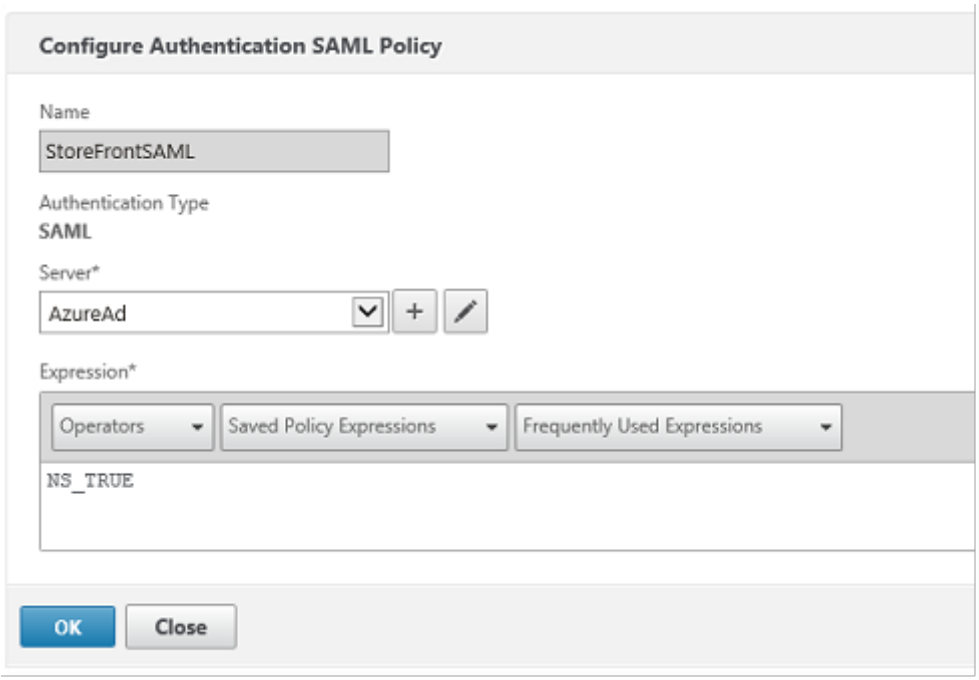
Prüfen der NetScaler-Bereitstellung

Stellen Sie eine Verbindung mit NetScaler her und überprüfen Sie, ob Authentifizierung und Start mit den Anmeldeinformationen funktionieren.

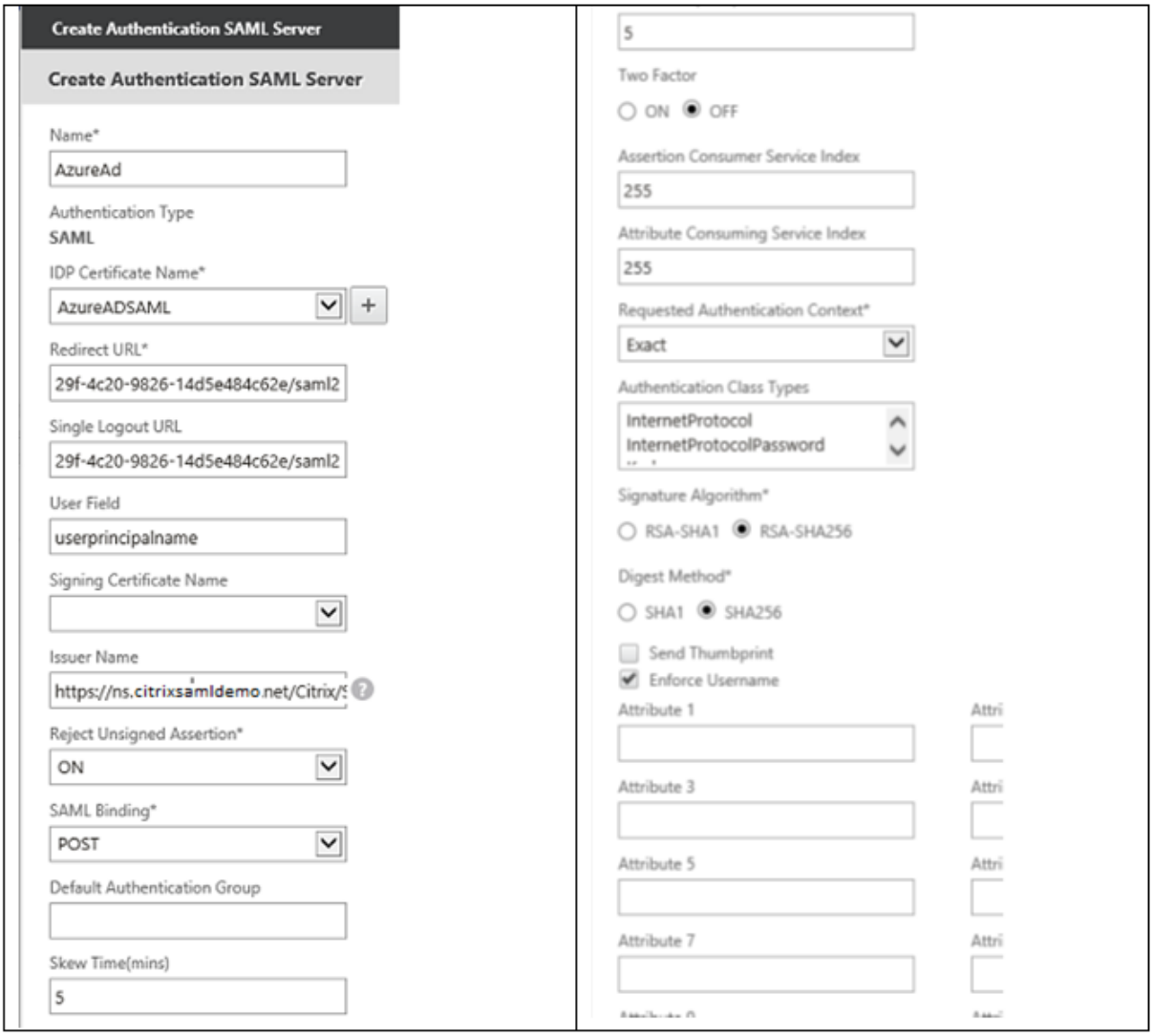


Aktivieren der Unterstützung für die NetScaler-SAML-Authentifizierung

Die Verwendung von SAML bei StoreFront ähnelt der Verwendung von SAML für andere Websites. Fügen Sie eine neue SAML-Richtlinie mit dem Ausdruck **NS_TRUE** hinzu.



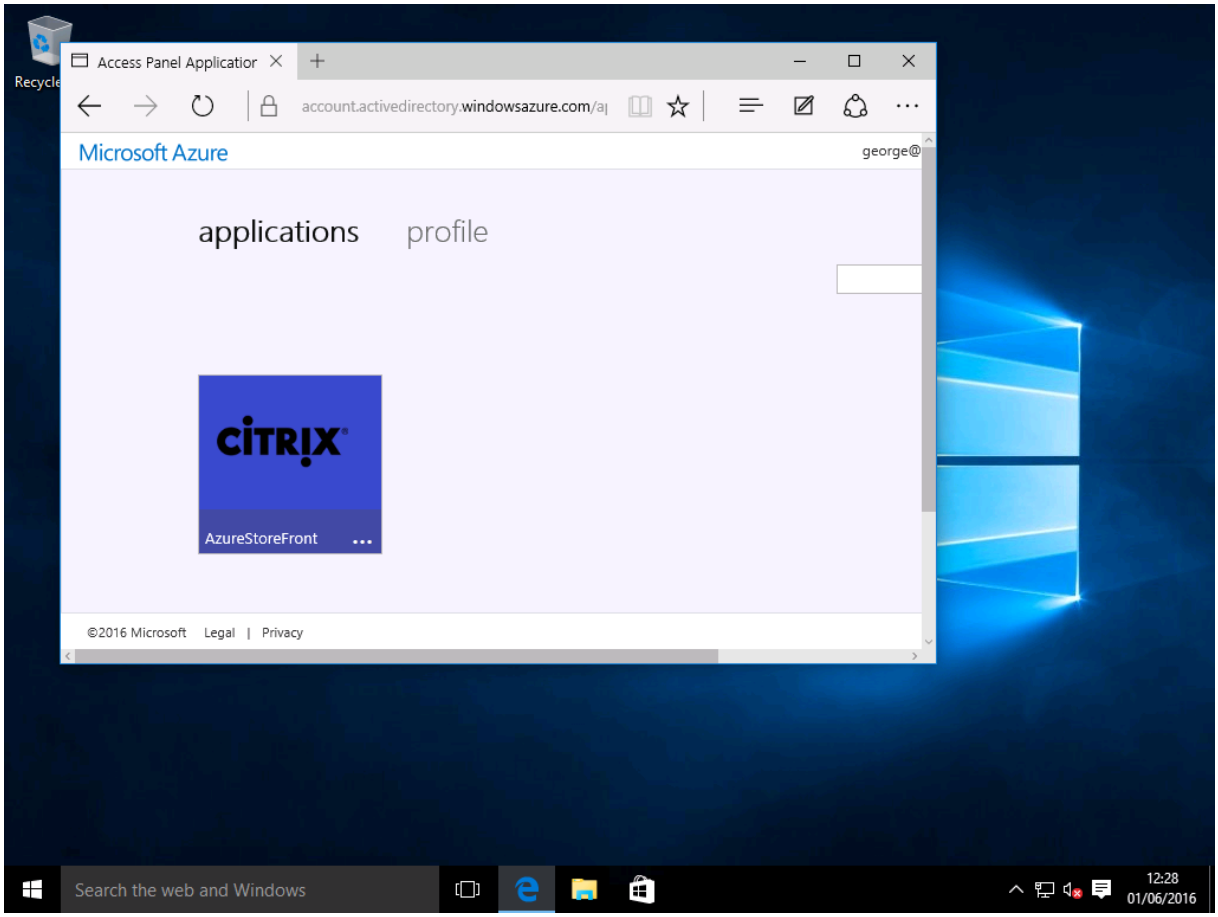
Konfigurieren Sie den neuen SAML-IdP-Server mit den zuvor von Azure AD erhaltenen Informationen.



Überprüfen des Gesamtsystems

Melden Sie sich bei einem Azure AD beigetretenen Windows 10-Desktop mit einem in Azure AD registrierten Konto an. Starten Sie Microsoft Edge und stellen Sie eine Verbindung mit https://myapps.microsoft.com her.

Im Webbrowser müssten nun die Azure AD-Anwendungen für den Benutzer angezeigt werden.



Vergewissern Sie sich, dass bei einem Klick auf das Symbol eine Umleitung an einen authentifizierten StoreFront-Server erfolgt.

Prüfen Sie außerdem, ob bei direkten Verbindungen mit der Single Sign-On-URL und mit der NetScaler-Site eine Umleitung an Microsoft Azure und zurück stattfindet.

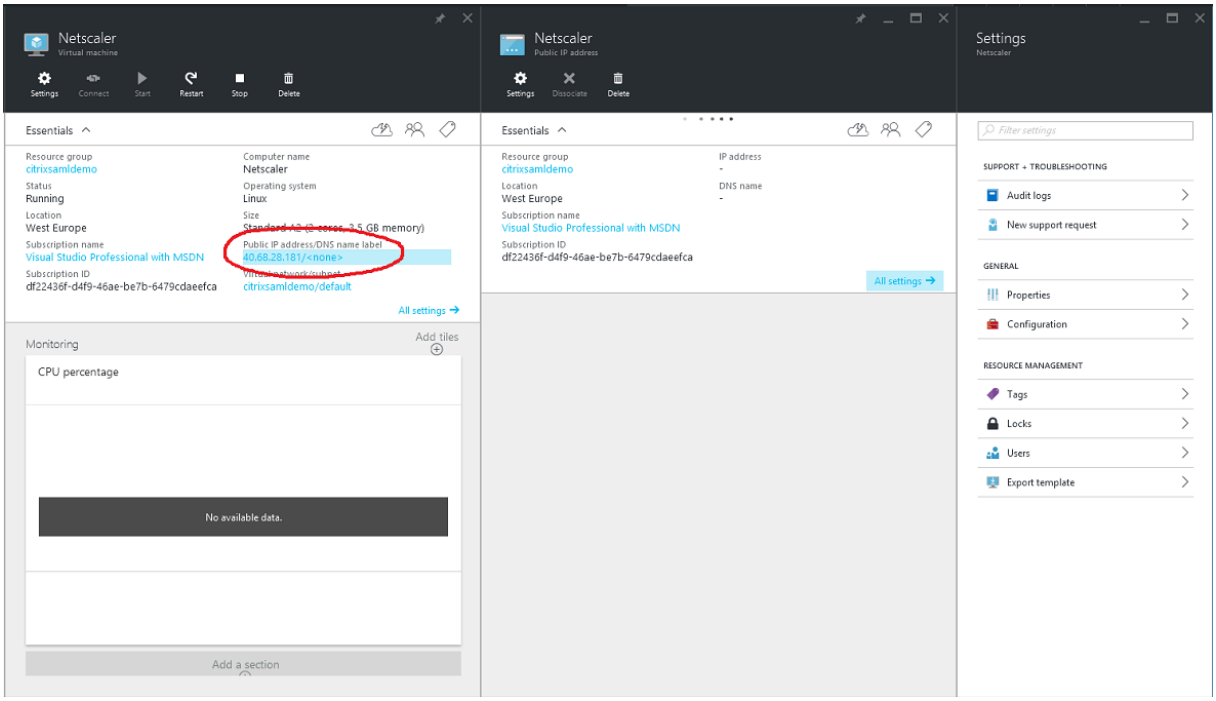
Vergewissern Sie sich zuletzt, dass dieselben URLs auch bei nicht Azure AD beigetretenen Maschinen funktionieren (allerdings ist hier bei der ersten Verbindung ein Sign-On bei Azure AD erforderlich).

Anhang

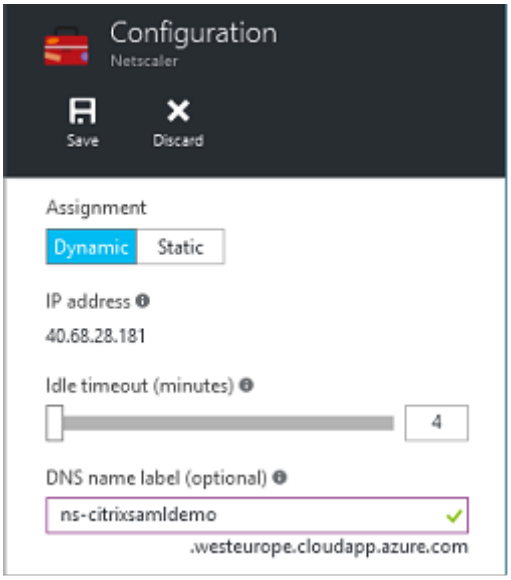
Wenn Sie eine VM in Azure einrichten, müssen verschiedene Standardoptionen konfiguriert werden.

Angeben einer öffentlichen IP-Adresse und einer DNS-Adresse

Azure weist allen VMs eine IP-Adresse im internen Subnetz zu (in diesem Beispiel 10.*.*.*). Standardmäßig wird auch eine öffentliche IP-Adresse angegeben, auf die durch eine dynamisch aktualisierte DNS-Bezeichnung verwiesen werden kann.



Wählen Sie **Configuration** für **Public IP address/DNS name label**. Wählen Sie eine öffentliche DNS-Adresse für die VM. Diese kann für CNAME-Verweise in anderen DNS-Zonendateien verwendet werden, damit alle DNS-Einträge richtig auf die VM verweisen, selbst wenn die IP-Adresse neu zugewiesen wird.

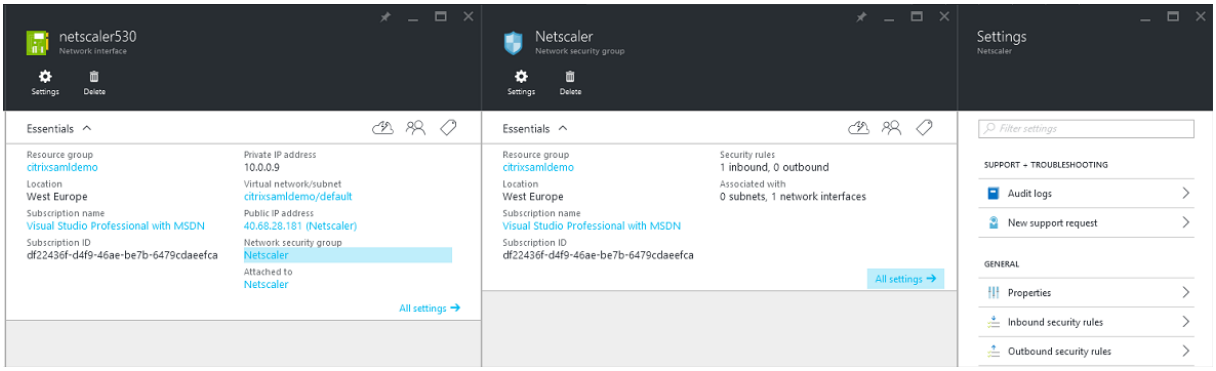


Einrichten von Firewallregeln (Sicherheitsgruppe)

Auf jede VM in einer Cloud werden automatisch einige Firewallregeln angewendet, die als Sicherheitsgruppe bezeichnet werden. Die Sicherheitsgruppe steuert den Datenverkehr von der öffentlichen an

die private IP-Adresse. Standardmäßig lässt Azure die RDP-Weiterleitung an alle VMs zu. Der NetScaler- und der AD FS-Server müssen ebenfalls TLS-Datenverkehr (443) weiterleiten.

Öffnen Sie **Network Interfaces** für eine VM und klicken Sie dann auf **Network Security Group**. Konfigurieren Sie **Inbound security rules** zum Zulassen des erforderlichen Datenverkehrs im Netzwerk.



Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.

Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts

Die folgenden Artikel enthalten Anweisungen für die Konfiguration und Verwaltung des Verbundauthentifizierungsdiensts (FAS):

- Schutz privater Schlüssel
- Konfiguration der Zertifizierungsstelle
- Sicherheit und Netzwerkmanagement
- Problembehandlung von Windows-Anmeldeproblemen
- PowerShell SDK Cmdlet-Hilfedateien

Verwandte Informationen

- Primäre Referenz für die Installation und anfängliche Einrichtung des FAS ist der Artikel Verbundauthentifizierungsdienst.

- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichsten FAS-Architekturen sowie Links zu Artikeln über komplexere Architekturen.

Konfiguration einer Zertifizierungsstelle für den Verbundauthentifizierungsdienst

January 21, 2022

Dieser Abschnitt beschreibt die erweiterte Konfiguration des Citrix Verbundauthentifizierungsdiensts (Federated Authentication Service, FAS) für die Integration mit Zertifizierungsstellenservern, die nicht von der FAS-Verwaltungskonsole unterstützt werden. In den Anweisungen werden PowerShell-APIs verwendet, die der Verbundauthentifizierungsdienst bietet. Grundlegende Kenntnisse von PowerShell werden für die Ausführung der Anweisungen in diesem Abschnitt vorausgesetzt.

Einrichten mehrerer Zertifizierungsstellenserver für die Verwendung im FAS

In diesem Abschnitt wird beschrieben, wie Sie einen FAS-Server so einrichten, dass mehrere Zertifizierungsstellenserver Zertifikate ausstellen können. Dies ermöglicht Lastausgleich und Failover für die Zertifizierungsstellenserver.

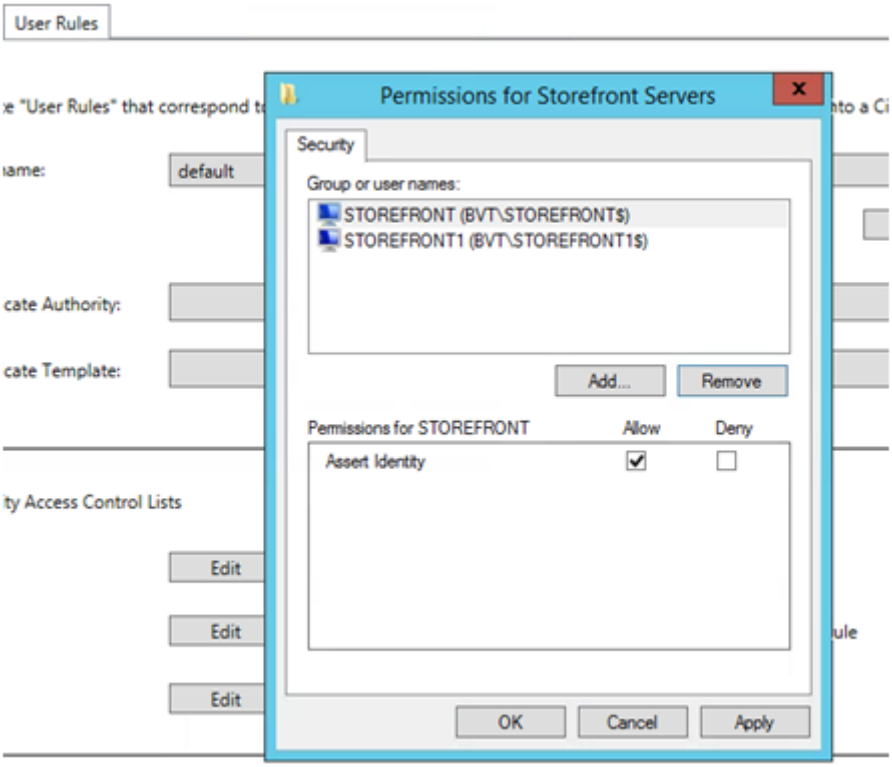
Schritt 1: Ermitteln, wie viele CA-Server FAS findet

Bestimmen Sie mit dem Cmdlet Get-FASMsCertificateAuthority, mit welchen Zertifizierungsstellenservern FAS eine Verbindung herstellen kann. Das folgende Beispiel zeigt, dass FAS mit drei Zertifizierungsstellenservern eine Verbindung herstellen kann.

```
PS > Add-PSSnapin Citrix*
PS > Get-FasMsCertificateAuthority

Address                         IsDefault   PublishedTemplates
-------                         ---------   ------------------

DC1.bvt.local\bvt-DC1-CA        False       {
 Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local     False       {
 Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local     False       {
 Citrix_SmartcardLogon, Citrix_Regis...
```


Schritt 2: Ändern der vorhandenen Zertifikatdefinition

Citrix empfiehlt, dass Sie mit der FAS-Verwaltungskonsole (und nicht mit PowerShell) eine Rolle erstellen. Auf diese Weise müssen Sie den SDL nicht später manuell hinzufügen. Im folgenden Beispiel wird eine Rolle namens "Default"erstellt, in der die Zugriffsregel konfiguriert ist:

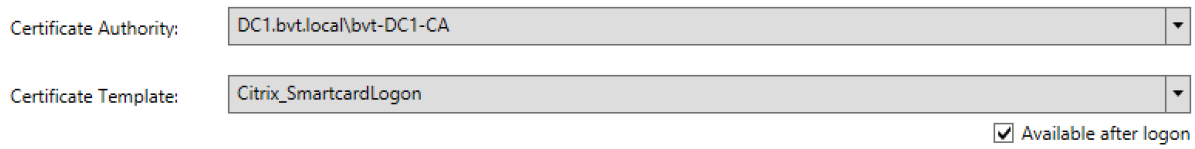


Um mehrere Zertifizierungsstellen im Feld für die Zertifizierungsstelle hinzuzufügen, müssen Sie die Zertifikatdefinition mit PowerShell konfigurieren. (Das Hinzufügen mehrerer Zertifizierungsstellen wird von der FAS-Verwaltungskonsole in dieser Version nicht unterstützt.)

Als Erstes benötigen Sie den Namen der Zertifikatdefinition. Der Name kann nicht mit der Verwaltungskonsole ermittelt werden. Verwenden Sie zur Ermittlung das Cmdlet Get-FASCertificateDefinition.

```
PS > Get-FasCertificateDefinition

Name                          : default_Definition
CertificateAuthorities        : {
 DC1.bvt.local\bvt-DC1-CA }

MsTemplate                    : Citrix_SmartcardLogon
AuthorizationCertificate      : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids                    : {
  }

InSession                     : True
```


Auf der Benutzeroberfläche sieht dies wie folgt aus:



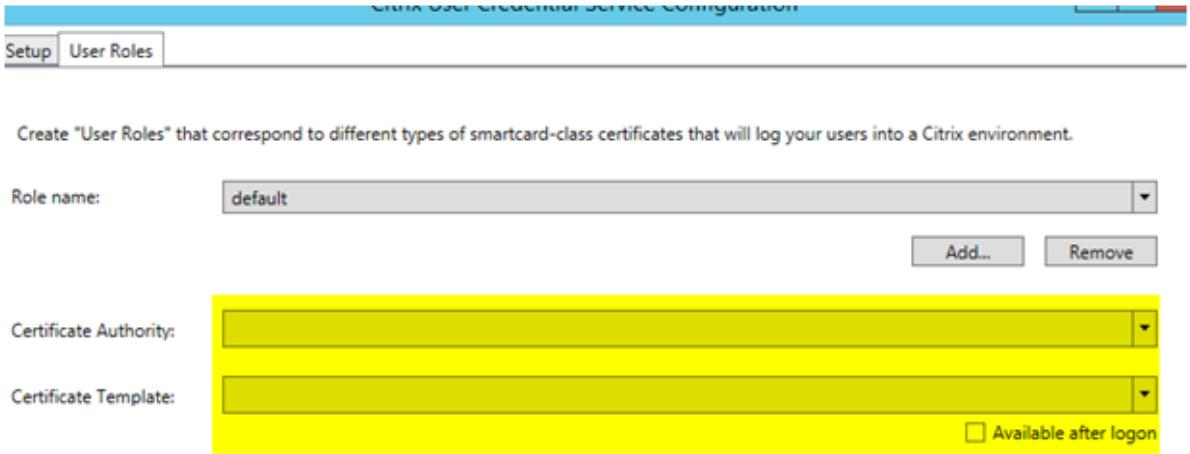
Wenn Sie den Namen der Zertifikatdefinition ermittelt haben, ändern Sie die Zertifikatdefinition, damit Sie eine Liste mit Zertifizierungsstellen haben:

```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```

Das Cmdlet Get-FASCertificateDefinition gibt nun Folgendes zurück:

```
PS > Get-FasCertificateDefinition
Name                        : default_Definition
CertificateAuthorities      : {
 DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\
    ca2.bvt.local }

MsTemplate                  : Citrix_SmartcardLogon
AuthorizationCertificate    : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids                  : {
  }

InSession                   : True
```

Nachdem Sie mehrere Zertifizierungsstellenserver konfiguriert haben, kann FAS nicht über die FAS-Verwaltungskonsole konfiguriert werden. Die Felder “Certificate Authority”und “Certificate Template”sind leer (siehe Abbildung):



> **Hinweis:**
>
> Wenn Sie mit der Konsole die Zugriffsregel ändern, wird Ihre Konfiguration mit mehreren Zertifizierungsstellen überschrieben. Wiederholen Sie Schritt 2, um alle Zertifizierungsstellen anzuzeigen.

Wenn Sie die Zugriffssteuerungslisten (ACL) in PowerShell neu konfigurieren möchten und unsicher bezüglich der Werte sind, empfehlen wir Folgendes:

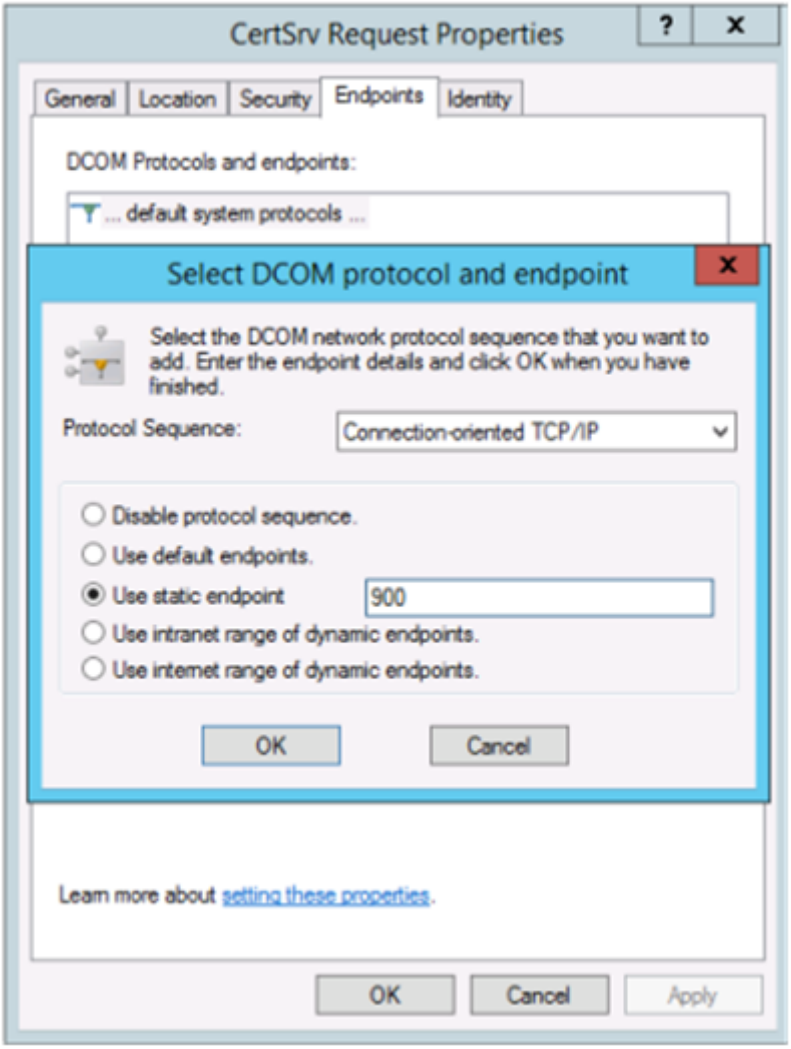
- Erstellen Sie eine zweite Regel (z. B. "test") mit einer einzelnen Zertifizierungsstelle.
- Konfigurieren Sie die ACLs je nach Bedarf in der Regel "test".
- Verwenden Sie PowerShell, um die ACL zu prüfen (Get-FasRule –name "test").
- Verwenden Sie PowerShell, um die ACL auf die ursprüngliche Regel anzuwenden (Set-FasRule).
- Löschen Sie die nicht mehr benötigte Regel "test".

Erwartete Verhaltensänderungen

Wenn Sie den FAS-Server mit mehreren Zertifizierungsstellenservern konfiguriert haben, wird die Generierung von Benutzerzertifikaten auf alle konfigurierten Zertifizierungsstellenserver verteilt. Wenn einer der konfigurierten Zertifizierungsstellenserver ausfällt, wechselt der FAS-Server zu einem anderen verfügbaren Zertifizierungsstellenserver.

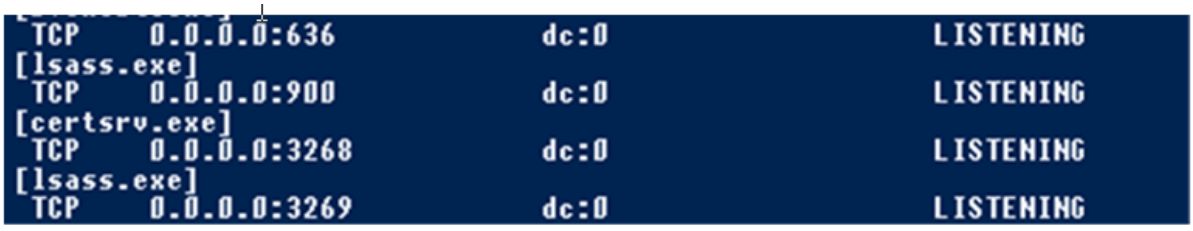
Konfigurieren der Microsoft-Zertifizierungsstelle für TCP-Zugriff

Standardmäßig verwendet die Microsoft-Zertifizierungsstelle für den Zugriff DCOM. Beim Implementieren von Firewallsicherheit kann dies sehr komplex sein, daher bietet Microsoft die Möglichkeit, zu einem statischen TCP-Port zu wechseln. Verwenden Sie in der Microsoft-Zertifizierungsstelle **Start > Ausführen > dcomcnfg.exe**, um das DCOM-Konfigurationsfenster zu öffnen. Erweitern Sie *Computer* > *Arbeitsplatz* > *DCOM-Konfiguration*, um den Knoten **CertSrv Request** anzuzeigen, und bearbeiten Sie dann die Eigenschaften der Anwendung "CertSrv Request DCOM":



Ändern Sie die Endpunkte, indem Sie einen statischen Endpunkt auswählen, und geben Sie eine TCP-Portnummer ein (900 in der Abbildung oben).

Starten Sie die Microsoft-Zertifizierungsstelle neu und senden Sie eine Zertifikatanforderung. Wenn Sie “netstat –a –n –b”ausführen, sollte certsrv zur Überwachung Port 900 verwenden:



Sie brauchen den FAS-Server (bzw. andere Maschinen, die die Zertifizierungsstelle verwenden) nicht zu konfigurieren, da DCOM durch Verwendung des RPC-Ports eine Aushandlungsphase hat. Wenn ein Client DCOM verwenden muss, stellt er eine Verbindung zum DCOM RPC-Dienst auf dem Zertifikatserver her und fordert Zugriff auf einen bestimmten DCOM-Server an. Dadurch wird Port 900 geöffnet

und der DCOM-Server gibt dem FAS-Server Anweisungen zum Herstellen der Verbindung.

Vorabgenerieren von Benutzerzertifikaten

Die Anmeldung erfolgt für Benutzer erheblich schneller, wenn Benutzerzertifikate im FAS-Server vorab generiert werden. In den folgenden Abschnitten wird die erforderliche Vorgehensweise für einen oder mehrere FAS-Server beschrieben.

Abrufen einer Liste der Active Directory-Benutzer

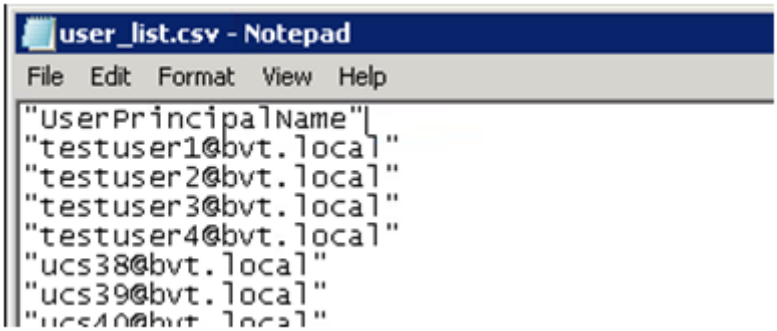
Sie können die Zertifikatgenerierung verbessern, indem Sie eine Liste der Benutzer von Active Directory abrufen und als Datei (z. B. als CSV-Datei) speichern, wie im folgenden Beispiel dargestellt.

```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for
    Users, leave it blank to search all
$filename = "user_list.csv" # Filename to save

if ($searchbase -ne ""){

    Get-ADUser -Filter {
 (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
  -SearchBase $searchbase -Properties UserPrincipalName | Select
      UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -
      delimiter "," $filename
 }
  else {

    Get-ADUser -Filter {
 (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
  -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv
      -NoTypeInformation -Encoding utf8 -delimiter "," $filename
 }

<!--NeedCopy-->
```

Get-ADUser ist ein Standardcmdlet zum Abrufen einer Liste der Benutzer. Das obige Beispiel enthält ein Filterargument, damit nur Benutzer mit einem UserPrincipalName aufgelistet werden, deren Kontostatus “enabled”ist.

Mit dem Argument SearchBase können Sie den Teil von Active Directory einschränken, der nach Benutzern durchsucht wird. Wenn Sie alle Benutzer in AD durchsuchen möchten, lassen Sie das Argument aus. **Hinweis:** Die Abfrage gibt u. U. eine große Anzahl Benutzer zurück.

Die CSV-Datei sieht wie folgt aus:



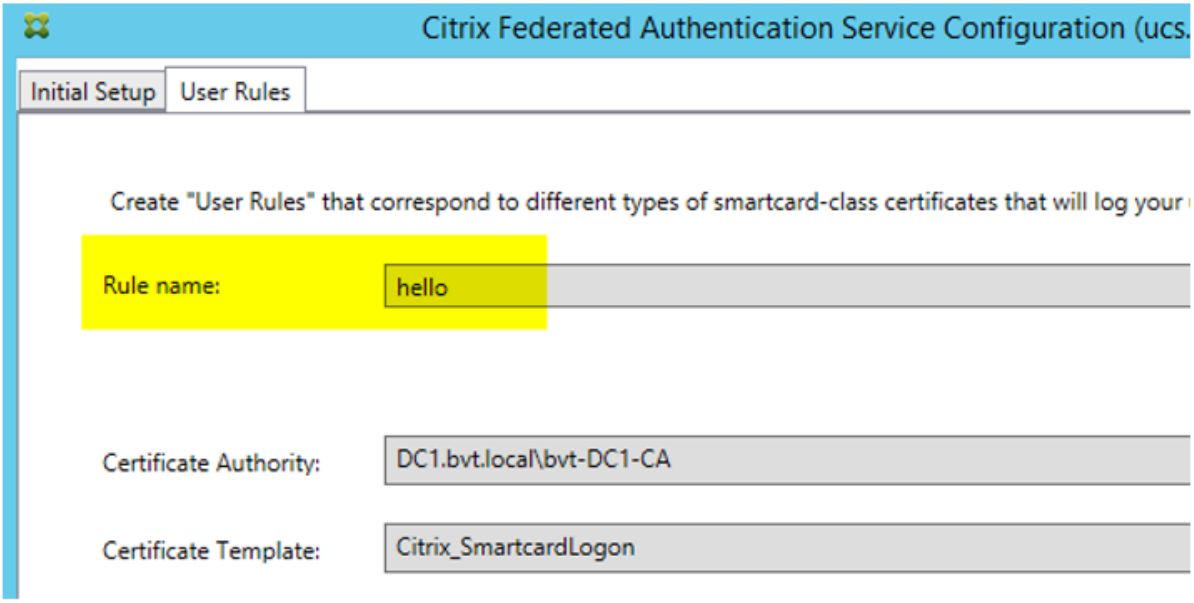
FAS-Server

Das folgende PowerShell-Skript erstellt mit der generierten Benutzerliste eine Liste mit Benutzerzertifikaten.

```
Add-PSSnapin Citrix.A*
$csv = "user_list.csv"
$rule = "default" # rule/role in your admin console
$users = Import-Csv -encoding utf8 $csv
foreach ( $user in $users )
{

    $server = Get-FasServerForUser -UserPrincipalNames $user.
       UserPrincipalName
    if( $server.Server -ne $NULL) {

        New-FasUserCertificate -Address $server.Server -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

    if( $server.Failover -ne $NULL) {

        New-FasUserCertificate -Address $server.Failover -
           UserPrincipalName $user.UserPrincipalName -
           CertificateDefinition $rule"_Definition" -Rule $rule
     }

 }

<!--NeedCopy-->
```

Wenn Sie mehr als einen FAS-Server haben, wird das Zertifikat für einen bestimmten Benutzer zweimal generiert: eins auf dem Hauptserver und das andere auf dem Failoverserver.

Das obige Skript wird durch die Regel “default”gesteuert. Wenn Ihre Regel einen anderen Namen hat (z. B. “hello”), ändern Sie im Skript die Variable $rule.



Erneuern von Registrierungsstellenzertifikaten

Wenn mehrere FAS-Server verwendet werden, können Sie ein FAS-Registrierungsstellenzertifikat erneuern, ohne dass es Auswirkungen auf angemeldete Benutzer hat. Hinweis: Sie können die Autorisierung von FAS auch mit der GUID aufheben und FAS neu autorisieren, jedoch werden dabei die FAS-Konfigurationsoptionen zurückgesetzt.

Führen Sie die folgenden Schritte aus:

1. Erstellen Sie ein neues Autorisierungszertifikat: `New-FasAuthorizationCertificate`
2. Notieren Sie die GUID des neuen Autorisierungszertifikats, das mit folgendem Befehl zurückgegeben wird: `Get-FasAuthorizationCertificate`
3. Versetzen Sie den FAS-Server in den Wartungsmodus: `Set-FasServer –Address <FAS server> -MaintenanceMode $true`
4. Wechseln Sie zum neuen Autorisierungszertifikat: `Set-FasCertificateDefinition –AuthorizationCertificate <GUID>`
5. Heben Sie den Wartungsmodus für den FAS-Server auf: `Set-FasServer –Address <FAS server> -MaintenanceMode $false`
6. Löschen Sie das alte Autorisierungszertifikat: `Remove-FasAuthorizationCertificate`

Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.

Schutz durch private Schlüssel beim Verbundauthentifizierungsdienst

August 18, 2021

Einführung

Zertifikate werden in der Registrierung auf dem FAS-Server gespeichert. Die zugehörigen privaten Schlüssel werden über das Netzwerkdienstkonto des FAS-Servers gespeichert und sind standardmäßig als nicht exportierbar markiert.

Es gibt zwei Arten privater Schlüssel:

- Der private Schlüssel des Registrierungsstellenzertifikats (RA-Zertifikat) der Zertifikatvorlage Citrix_RegistrationAuthority.
- Die privaten Schlüssel der Benutzerzertifikate der Zertifikatvorlage Citrix_SmartcardLogon.

Es gibt zwei RA-Zertifikate: Citrix_RegistrationAuthority_ManualAuthorization (24 Stunden gültig) und Citrix_RegistrationAuthority (zwei Jahre gültig).

Wenn der Administrator während der Ersteinrichtung auf der FAS-Verwaltungskonsole in Schritt 3 auf "Authorize"klickt, generiert der FAS-Server ein Schlüsselpaar und sendet eine Zertifikatsignieranforderung (CSR) für das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization an die Zertifizierungsstelle. Dies ist ein temporäres Zertifikat, das standardmäßig 24 Stunden lang gültig ist. Die Zertifizierungsstelle stellt dieses Zertifikat nicht automatisch aus. Die Ausstellung muss bei der Zertifizierungsstelle manuell von einem Administrator genehmigt werden. Wenn das Zertifikat für den FAS-Server ausgestellt wurde, verwendet der Verbundauthentifizierungsdienst das Zertifikat Citrix_RegistrationAuthority_ManualAuthorization, um automatisch das Zertifikat Citrix_RegistrationAuthority (zwei Jahre gültig) abzurufen. Der FAS-Server löscht das Zertifikat und den Schlüssel für Citrix_RegistrationAuthority_ManualAuthorization, sobald er das Zertifikat Citrix_RegistrationAuthority erhält.

Der private Schlüssel des RA-Zertifikates ist besonders vertraulich, da die RA-Zertifikatrichtlinie dem Besitzer des privaten Schlüssels das Ausstellen von Zertifikatanforderungen für die in der Vorlage konfigurierten Benutzer erlaubt. Wer also diesen Schlüssel hat, kann als einer der konfigurierten Benutzer eine Verbindung mit der Umgebung herstellen.

Mit einer der folgenden Optionen können Sie die Konfiguration des FAS-Servers so festlegen, dass private Schlüssel den Sicherheitsanforderungen Ihrer Organisation entsprechend geschützt sind:

- Microsoft Enhanced RSA und AES Cryptographic Provider oder Schlüsselspeicheranbieter für Microsoft-Software für die privaten Schlüssel von RA-Zertifikaten und von Benutzerzertifikaten.
- Schlüsselspeicheranbieter der Microsoft-Plattform mit einem Trusted Platform Module (TPM)-Chip für den privaten Schlüssel des RA-Zertifikats und Microsoft Enhanced RSA und AES Cryptographic Provider oder Schlüsselspeicheranbieter für Microsoft-Software für die privaten Schlüssel von Benutzern.
- Ein Hardwaresicherheitsmodul (HSM) mit dem Kryptografiedienst eines Anbieters oder ein Schlüsselspeicheranbieter mit dem HSM-Gerät für das RA-Zertifikat und die privaten Schlüssel der Benutzerzertifikate.

Konfigurationseinstellungen für private Schlüssel

Konfigurieren Sie den Verbundauthentifizierungsdienst, sodass er eine der drei Optionen verwendet. Bearbeiten Sie die Datei Citrix.Authentication.FederatedAuthenticationService.exe.config mit einem Text-Editor. Der Standardspeicherort der Datei ist unter Programme\Citrix\Federated Authentication Service auf dem FAS-Server.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Der Verbundauthentifizierungsdienst liest die Konfigurationsdatei nur, wenn der Dienst gestartet wird. Wenn Sie Werte ändern, muss der FAS neu gestartet werden, damit die neuen Einstellungen wirksam werden.

Legen Sie die relevanten Werte in der Datei Citrix.Authentication.FederatedAuthenticationService.exe.config wie folgt fest:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (Wechsel zwischen CAPI und CNG-APIs)

Wert	Kommentar
true	CAPI-APIs verwenden
false (Standardwert)	CNG-APIs verwenden

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (Name des zu verwendenden Anbieters)

Wert	Kommentar
Microsoft Enhanced RSA und AES Cryptographic Provider	CAPI-Standardanbieter
Schlüsselspeicheranbieter für Microsoft-Software	CNG-Standardanbieter
Schlüsselspeicheranbieter der Microsoft-Plattform	TPM-Standardanbieter TPM wird nicht für Benutzerschlüssel empfohlen. Verwenden Sie TPM nur für RA-Schlüssel. Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie die TPM- und Hypervisor-Hersteller, ob Virtualisierung unterstützt wird.
HSM_Vendor CSP/Schlüsselspeicheranbieter	Bereitstellung durch HSM-Hersteller. Der Wert unterscheidet sich je nach Hersteller. Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie den HSM-Hersteller, ob Virtualisierung unterstützt wird.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (nur bei CAPI-API erforderlich)

Wert	Kommentar
24	Standard. Bezieht sich auf Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Muss immer 24 lauten, es sei denn, Sie verwenden ein HSM mit CAPI und der HSM-Hersteller hat eine andere Spezifikation.

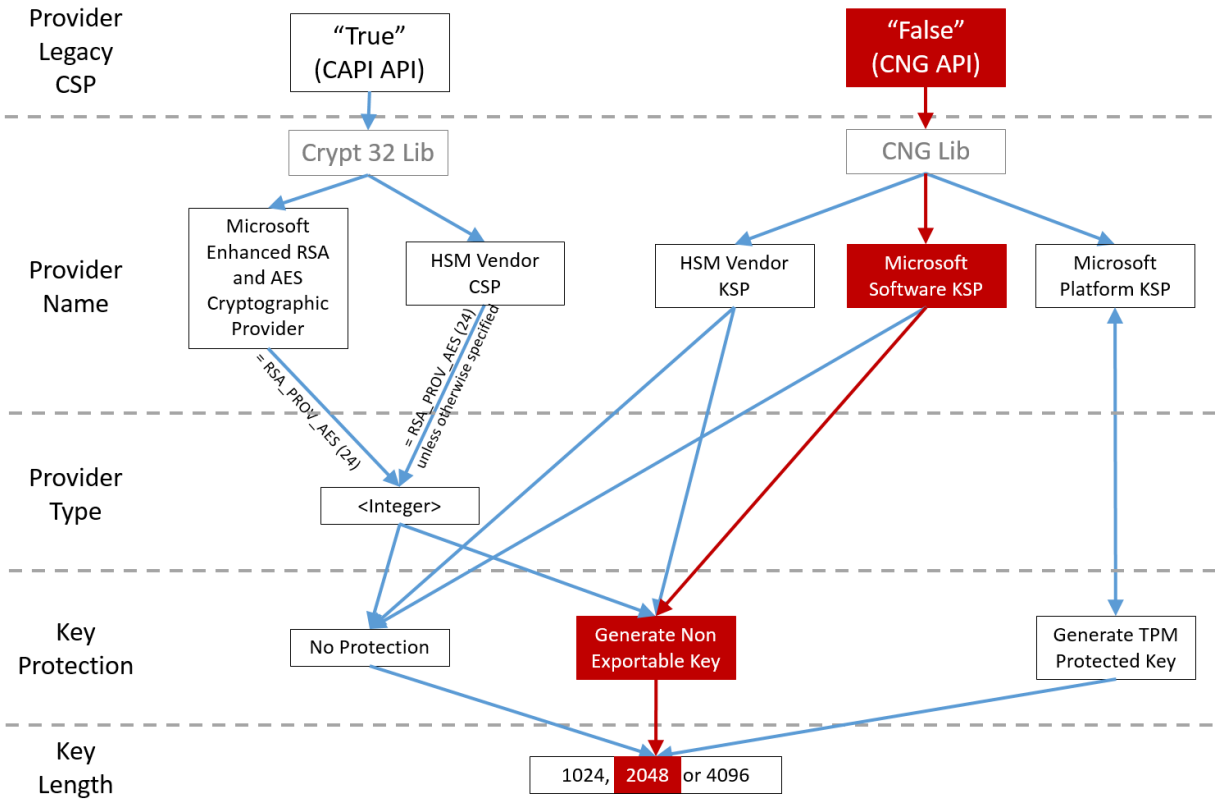
Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (wenn der FAS einen Privatschlüsselvorgang ausführen muss, wird der hier angegebene Wert verwendet) steuert das Flag "exportable"von privaten Schlüsseln. Ermöglicht außerdem die Verwendung eines TPM-Schlüsselspeichers, wenn die Hardware dies unterstützt.

Wert	Kommentar
NoProtection	Privater Schlüssel kann exportiert werden.
GenerateNonExportableKey	Standard. Privater Schlüssel kann nicht exportiert werden.
GenerateTPMProtectedKey	Privater Schlüssel wird mit dem TPM verwaltet. Der private Schlüssel wird von dem Anbieter gespeichert, den Sie in ProviderName angegeben haben (z. B. Schlüsselspeicheranbieter der Microsoft-Plattform)

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (Größe des privaten Schlüssels in Bit eingeben)

Wert	Kommentar
2048	1024 oder 4096 können auch verwendet werden.

Die Einstellungen für die Konfigurationsdatei werden grafisch wie folgt dargestellt (Installationsstandards sind rot markiert):



Beispiele für Konfigurationsszenarios

Beispiel 1

Dieses Beispiel gilt für den privaten Schlüssel des RA-Zertifikats und die privaten Schlüssel der Benutzerzertifikate, die mit dem Schlüsselspeicheranbieter für Microsoft-Software gespeichert wurden.

Dies ist die Standardkonfiguration nach der Installation. Eine zusätzliche Konfiguration des privaten Schlüssels ist nicht erforderlich.

Beispiel 2

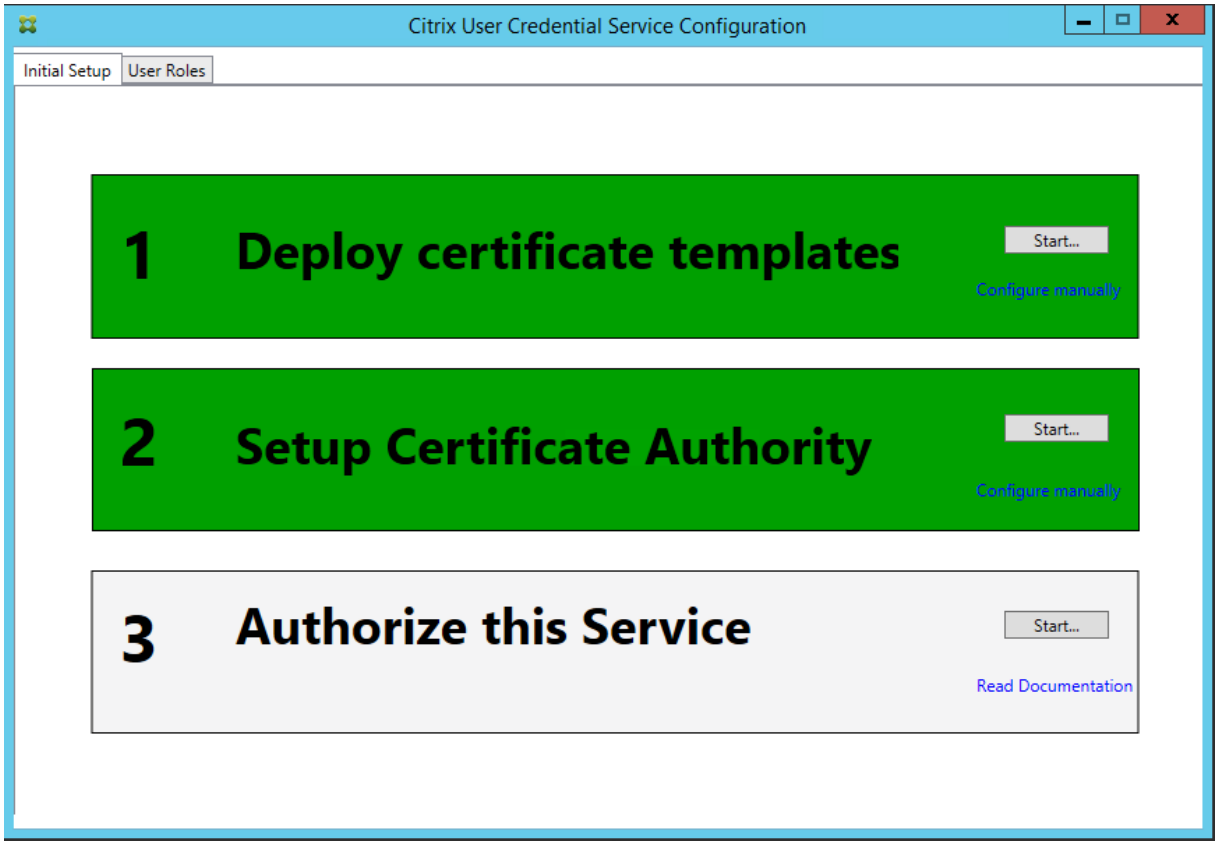
Dieses Beispiel zeigt den privaten Schlüssel des RA-Zertifikats, der im FAS-Server auf der Hauptplatine im Hardware-TPM vom Schlüsselspeicheranbieter der Microsoft-Plattform gespeichert wurde, sowie die privaten Schlüssel der Benutzerzertifikate, die vom Schlüsselspeicheranbieter für Microsoft-Software gespeichert wurden.

In diesem Szenario wird angenommen, dass das TPM auf der Hauptplatine des FAS-Servers im BIOS entsprechend der TPM-Herstellerdokumentation aktiviert und dann in Windows initialisiert wurde.

Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)?redirectedfrom=MSDN.

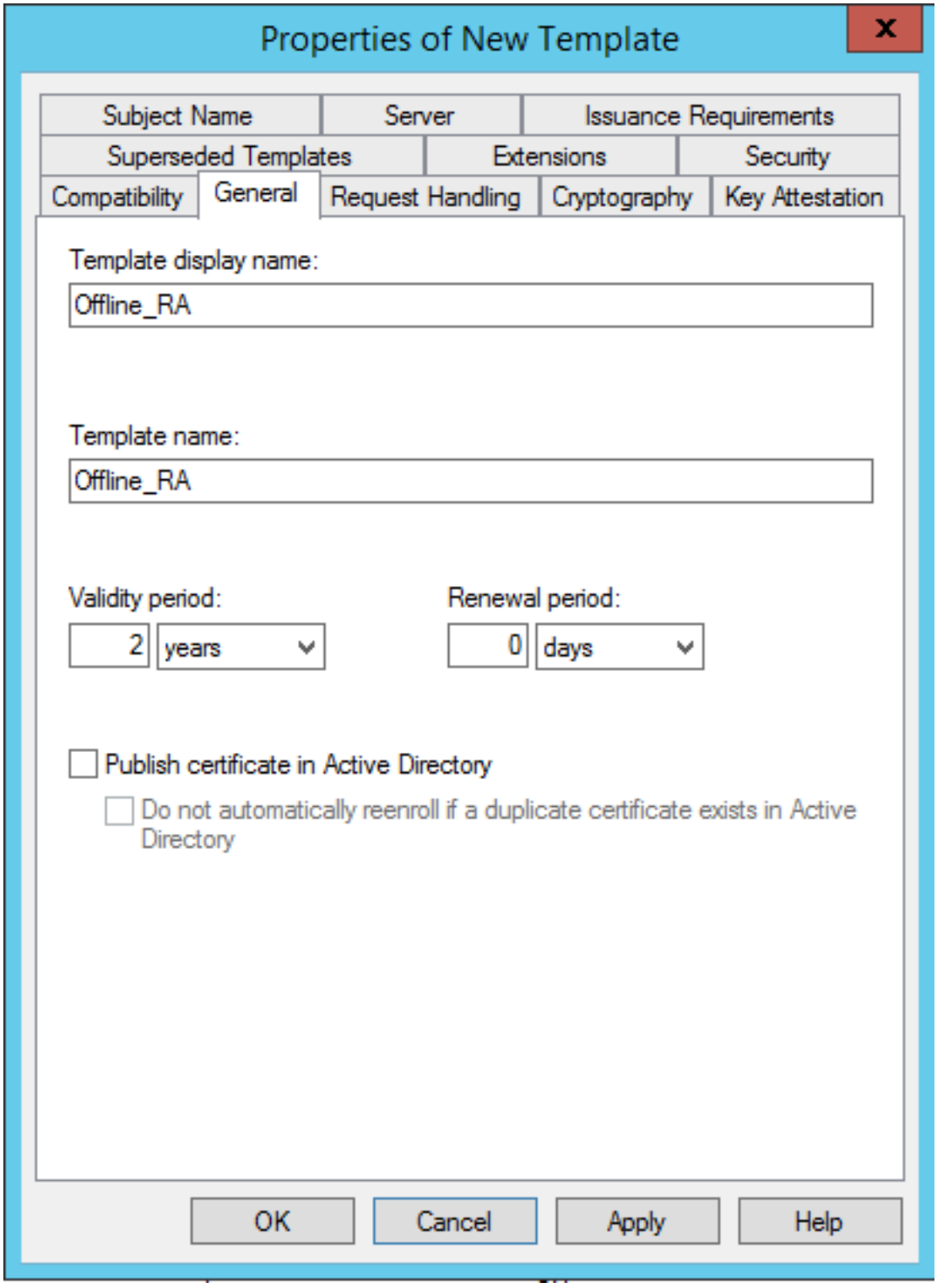
Verwenden von PowerShell (empfohlen) Das RA-Zertifikat kann offline mit PowerShell angefordert werden. Dies ist für Organisationen geeignet, wenn die Zertifizierungsstellen keine RA-Zertifikate über eine Online-Zertifikatsignieranforderung ausstellen dürfen. Eine Offline-Zertifikatsignieranforderung kann von einer Registrierungsstelle nicht über die FAS-Verwaltungskonsole ausgestellt werden.

Schritt 1: Führen Sie während der Ersteinrichtung der FAS-Konfiguration mit der Verwaltungskonsole nur die ersten zwei Schritte aus: "Deploy certificate templates"und "Setup Certificate Authority".



Schritt 2: Fügen Sie auf dem CA-Server das Zertifikatvorlagen-MMC-Snap-In hinzu. Klicken Sie mit der rechten Maustaste auf die Vorlage **Citrix_RegistrationAuthority_ManualAuthorization** und wählen Sie **Vorlage duplizieren**.

Wählen Sie die Registerkarte **Allgemein**. Ändern Sie den Namen und die Gültigkeitsdauer. In diesem Beispiel ist der Name Offline_RA und die Gültigkeitsdauer 2 Jahre:



Schritt 3: Fügen Sie auf dem CA-Server das Zertifizierungsstellen-MMC-Snap-In hinzu. Klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**. Wählen Sie **Neu** und klicken Sie dann auf **Auszustellende Zertifikatvorlage**. Wählen Sie die Vorlage aus, die Sie soeben erstellt haben.

Schritt 4: Laden Sie die folgenden PowerShell-Cmdlets auf dem FAS-Server:

Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

Schritt 5: Erstellen Sie das RSA-Schlüsselpaar im TPM des FAS-Servers und erstellen Sie die Zertifikatsignieranforderung durch Eingabe des folgenden PowerShell-Cmdlets auf dem FAS-Server. **Hinweis:** Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge ist 2048 Bit. Geben Sie eine Schlüssellänge an, die Ihre Hardware unterstützt.

New-FasAuthorizationCertificateRequest -UseTPM $true -address <FQDN des FAS-Servers>

Beispiel:

New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net

Folgendes wird angezeigt:

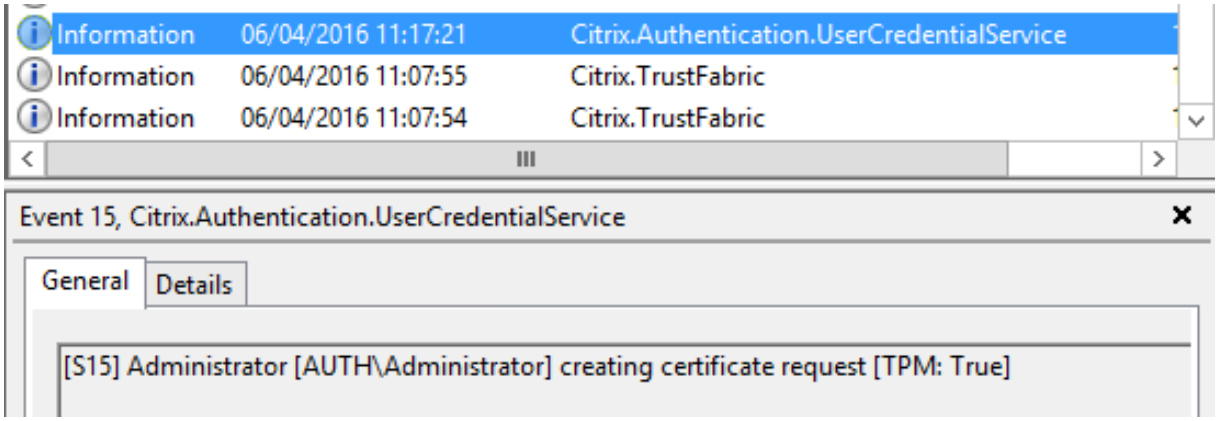
```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      1hCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPRgcq9XBwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      Y1ITHOtmcHFKt4Loz5O5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4XQvr1F+TO15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWOjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

Hinweise:

- Die ID GUID (in diesem Beispiel "5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39") ist in einem der folgenden Schritte erforderlich.
- Betrachten Sie das PowerShell-Cmdlet als einmalige "Überschreibungsmethode"zum Generieren des privaten Schlüssels für das RA-Zertifikat.
- Wenn dieses Cmdlet ausgeführt wird, wird die zu verwendende Schlüssellänge anhand der Werte bestimmt, die beim Start des FAS-Diensts aus der Konfigurationsdatei gelesen wurden (der Standardwert ist 2048).
- Da -UseTPM in diesem manuellen, mit PowerShell initiierten Privatschlüsselvorgang für das RA-Zertifikat auf $true festgelegt ist, ignoriert das System Werte aus der Datei, die nicht mit den Einstellungen übereinstimmen, die zur Verwendung eines TPM erforderlich sind.
- Durch das Ausführen des Cmdlets ändern sich keine Einstellungen in der Konfigurationsdatei.
- Bei nachfolgenden automatischen, vom FAS initiierten Privatschlüsselvorgängen für Benutzerzertifikate werden die Werte verwendet, die beim Starten des FAS-Diensts aus der Datei gelesen wurden.
- Es ist auch möglich, den Wert KeyProtection in der Konfigurationsdatei auf GenerateTPMProtectedKey festzulegen, wenn der FAS-Server Benutzerzertifikate festlegt, damit durch das TPM

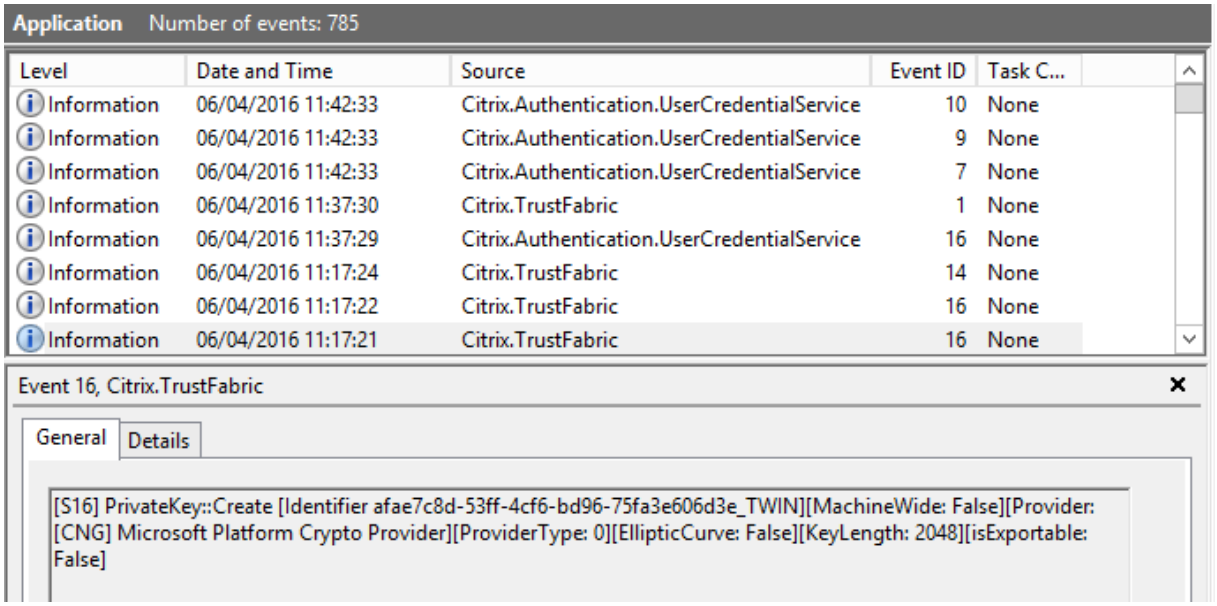
geschützte private Schlüssel für Benutzerzertifikate generiert werden.

Um sicherzustellen, dass das TPM zum Generieren des Schlüsselpaars verwendet wurde, überprüfen Sie das Anwendungsprotokoll in der Windows-Ereignisanzeige auf dem FAS-Server auf die Zeit, zu der das Schlüsselpaar generiert wurde.



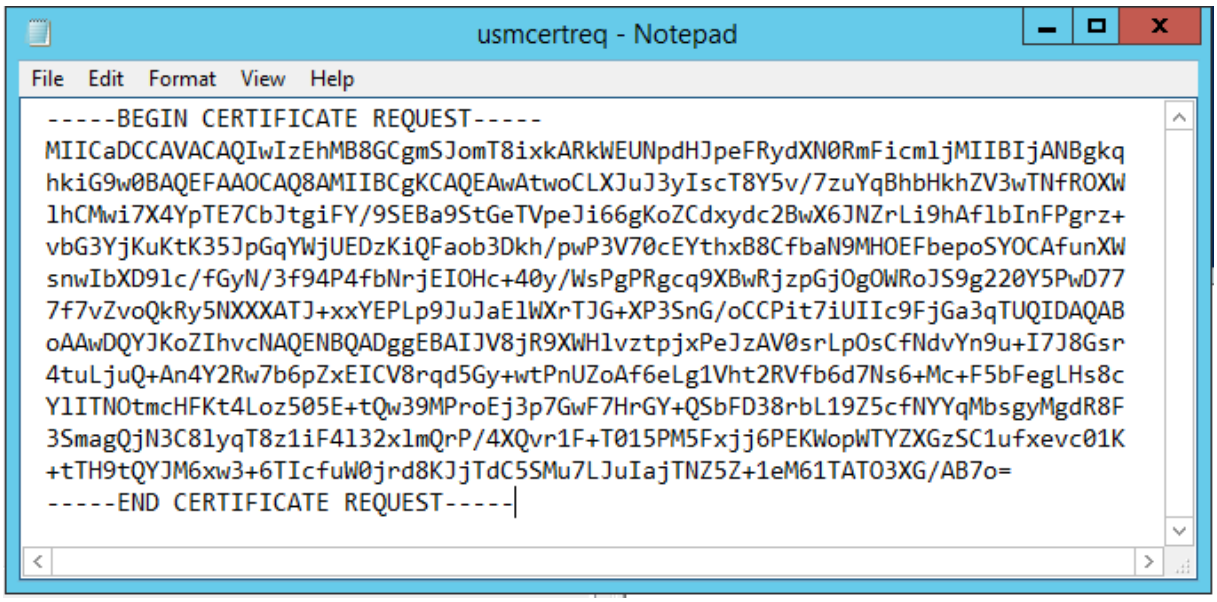
Folgendes sollte angezeigt werden: [TPM: True]

Gefolgt von:



Folgendes sollte angezeigt werden: “Provider: [CNG] Microsoft Platform Crypto Provider”

Schritt 6: Kopieren Sie den Zertifikatanforderungsabschnitt in einen Texteditor und speichern Sie ihn als Textdatei.



Schritt 7: Senden Sie die CSR an die Zertifizierungsstelle, indem Sie Folgendes in PowerShell auf dem FAS-Server eingeben:

certreq -submit -attrib “certificatetemplate:<Zertifikatvorlage aus Schritt 2>”<Zertifikatanforderungs-datei aus Schritt 6>

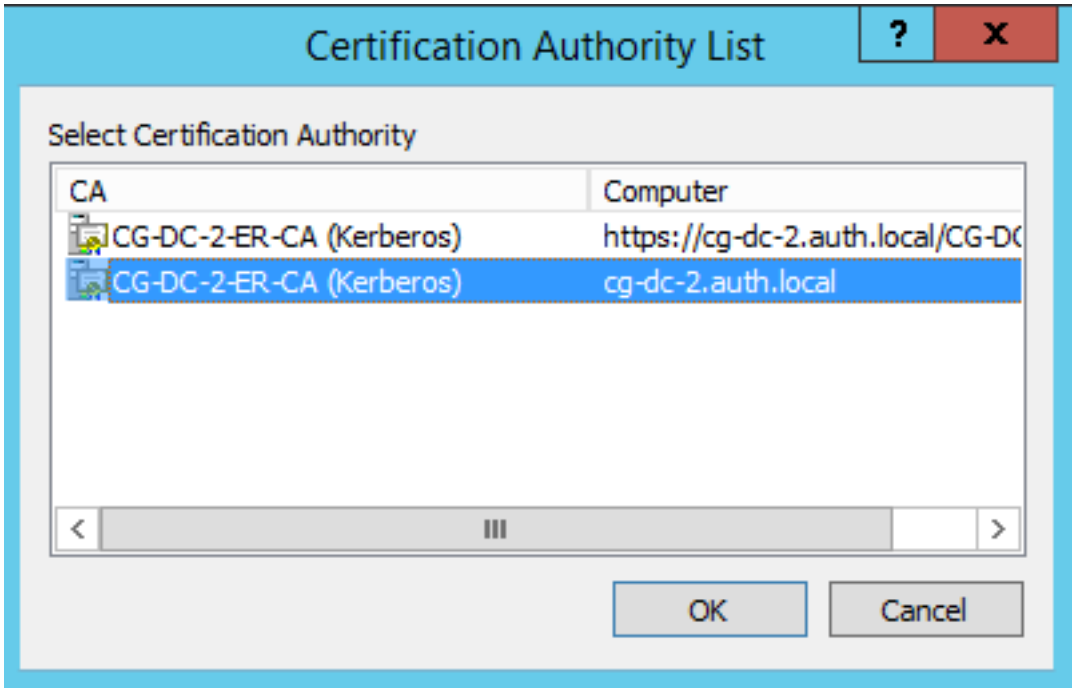
Beispiel:

certreq -submit -attrib “certificatetemplate:Offline_RA”C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt

Folgendes wird angezeigt:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
```

An dieser Stelle wird u. U. ein Fenster mit einer Liste der Zertifizierungsstellen angezeigt. Für die Zertifizierungsstelle in diesem Beispiel sind http- (oben) und DCOM-Registrierung (unten) aktiviert. Wählen Sie ggf. die DCOM-Option:

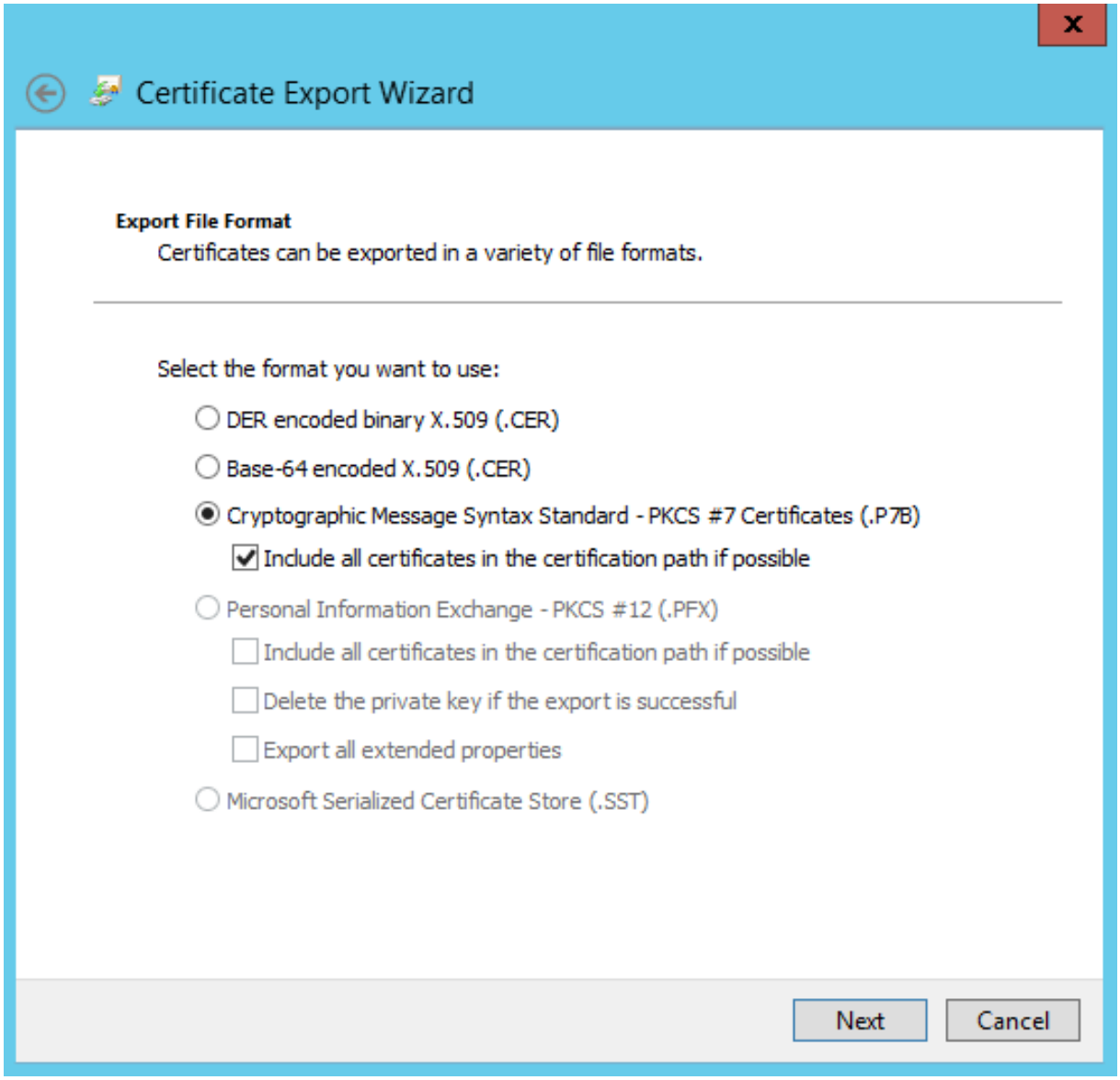


Nachdem die Zertifizierungsstelle angegeben wurde, zeigt PowerShell die RequestID an:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH> _
```

Schritt 8: Klicken Sie auf dem CA-Server im CA-MMC-Snap-In auf **Ausstehende Anforderungen**. Suchen Sie die Anforderungs-ID (RequestID). Klicken Sie mit der rechten Maustaste auf die Anforderung und wählen Sie **Ausstellen**.

Schritt 9: Wählen Sie den Knoten **Ausgestellte Zertifikate**. Suchen Sie das Zertifikat, das soeben ausgestellt wurde (die Anforderungs-ID muss übereinstimmen). Doppelklicken Sie auf das Zertifikat, um es zu öffnen. Wählen Sie die Registerkarte **Details**. Klicken Sie auf **In Datei kopieren**. Der Zertifikatexportassistent wird gestartet. Klicken Sie auf **Weiter**. Wählen Sie die folgenden Optionen für das Dateiformat:



Format: **Cryptographic Message Syntax Standard –PKCS #7 Certificates (.P7B)** und **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen muss** ausgewählt werden.

Schritt 10: Kopieren Sie die exportierte Zertifikatdatei auf den FAS-Server.

Schritt 11: Importieren Sie das RA-Zertifikat in die Registrierung des FAS-Servers, indem Sie das folgende PowerShell-Cmdlet auf dem FAS-Server eingeben:

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

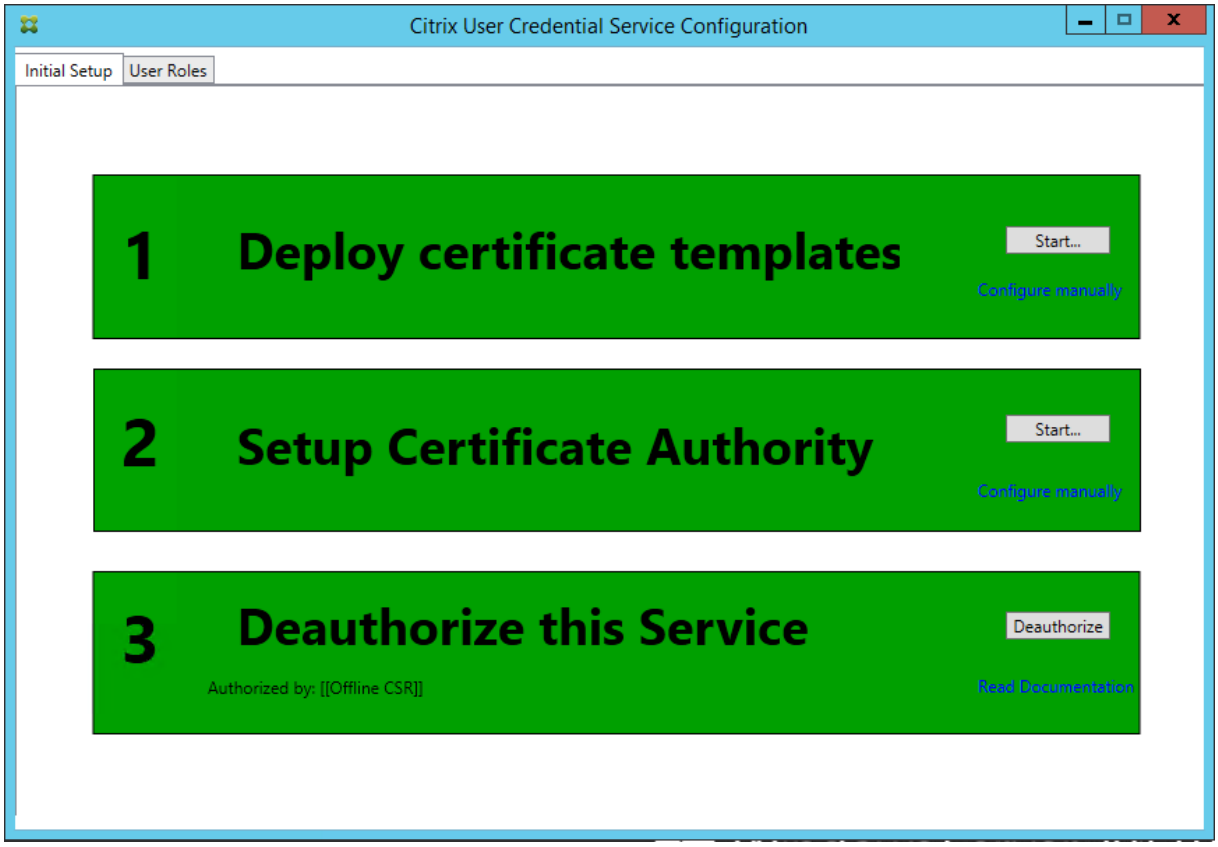
Beispiel:

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```


Folgendes wird angezeigt:

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec31102Dfc
CertificateRequest :
Status              : Ok
```

Schritt 12: Schließen Sie die FAS-Verwaltungskonsole und starten Sie sie neu.



Der Schritt “Authorize this Service”ist nun grün und der Text lautet nun “Deauthorize this Service”. Der Eintrag unten gibt “Authorized by: Offline CSR”an.

Schritt 13: Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte **User Roles** und bearbeiten Sie die Einstellungen entsprechend den Anleitungen im FAS-Hauptartikel.

Hinweis: Wenn Sie die Autorisierung des FAS über die Verwaltungskonsole aufheben, wird die Benutzerregel gelöscht.

Verwenden der FAS-Verwaltungskonsole

Die FAS-Verwaltungskonsole kann keine Offline-Zertifikatsignieranforderung ausstellen, daher wird die Verwendung nicht empfohlen, es sei denn, Ihre Organisation erlaubt Online-Zertifikatsignieranforderungen für RA-Zertifikate.

Führen Sie bei der Ersteinrichtung des Verbundauthentifizierungsdiensts die folgenden Schritte aus, und zwar nach der Bereitstellung der Zertifikatvorlagen und der Einrichtung der Zertifizierungsstelle, aber bevor Sie den Dienst autorisieren (Schritt 3 in der Konfigurationsreihenfolge):

Schritt 1: Ändern Sie in der Config-Datei die u. a. Zeile wie folgt:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

Daraufhin sollte die Datei wie folgt aussehen:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Einige TPMs beschränken die Schlüssellänge. Die Standardschlüssellänge ist 2048 Bit. Geben Sie eine Schlüssellänge an, die Ihre Hardware unterstützt.

Schritt 2: Autorisieren Sie den Dienst.

Schritt 3: Stellen Sie die ausstehende Zertifikatsanforderung manuell über den CA-Server aus. Nachdem Sie das RA-Zertifikat erhalten haben, wird Schritt 3 der Einrichtungsreihenfolge in der Verwaltungskonsole grün angezeigt. Der private Schlüssel für das RA-Zertifikat wurde nun im TPM generiert. Das Zertifikat gilt standardmäßig 2 Jahre.

Schritt 4: Ändern Sie die Config-Datei folgendermaßen zurück:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

Hinweis: Obwohl der Verbundauthentifizierungsdienst Benutzerzertifikate mit TPM-geschützten Schlüsseln generieren kann, ist die TPM-Hardware möglicherweise zu langsam für große Bereitstellungen.

Schritt 5: Starten Sie den Citrix Verbundauthentifizierungsdienst neu. Dadurch wird der Dienst gezwungen, die Konfigurationsdatei erneut zu lesen und die geänderten Werte werden wirksam. Die

nachfolgenden automatischen Privatschlüsselvorgänge wirken sich auf Benutzerzertifikatschlüssel aus. Bei diesen Vorgängen werden die privaten Schlüssel nicht im TPM, sondern mit dem Schlüsselspeicheranbieter für Microsoft-Software gespeichert.

Schritt 6: Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte "User Roles"und bearbeiten Sie die Einstellungen wie im FAS-Hauptartikel beschrieben.

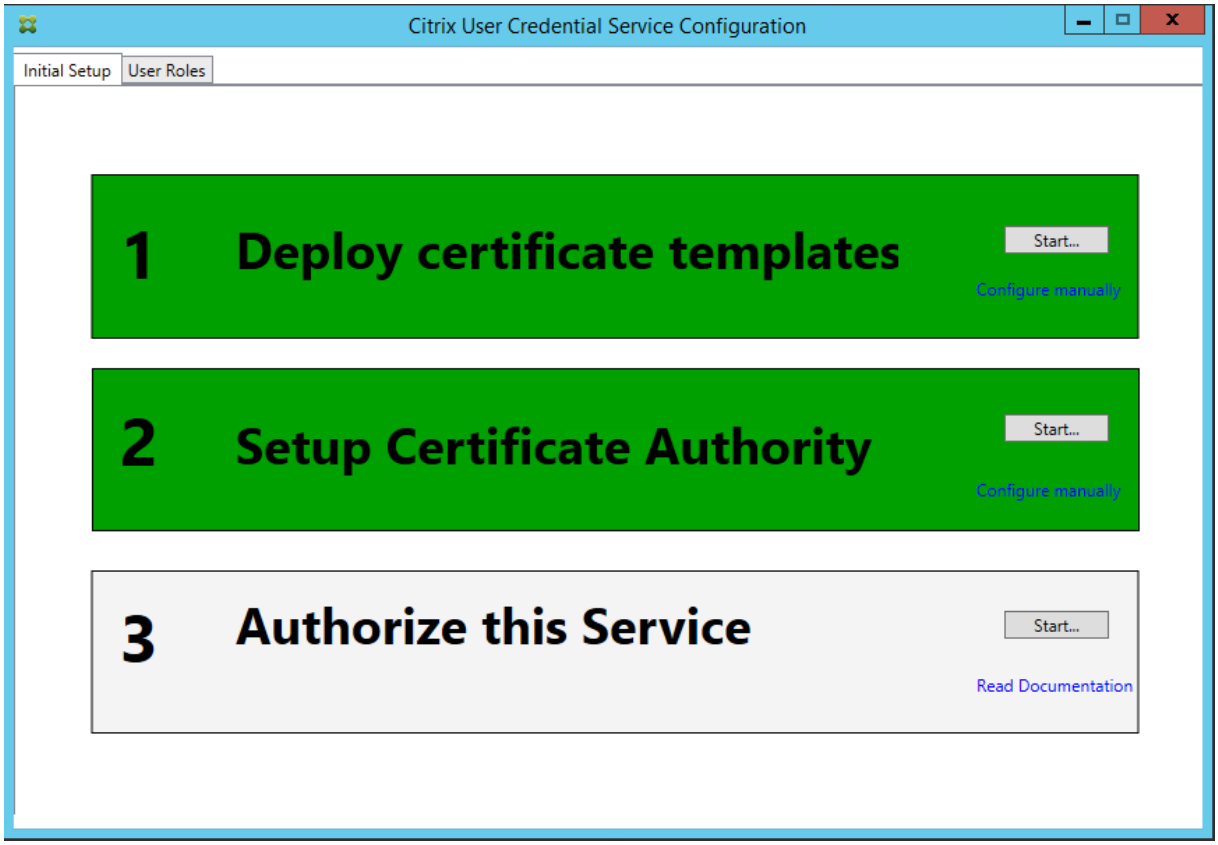
Hinweis: Wenn Sie die Autorisierung des FAS über die Verwaltungskonsole aufheben, wird die Benutzerregel gelöscht.

Beispiel 3

Dieses Beispiel gilt für einen privaten Schlüssel des RA-Zertifikats und die privaten Schlüssel der Benutzerzertifikate, die in einem HSM gespeichert wurden. In diesem Beispiel wird ein konfiguriertes HSM vorausgesetzt. Das HSM hat einen Anbieternamen, z. B. "HSM_Vendor's Key Storage Provider" .

Wenn Sie beabsichtigen, den FAS-Server in einer virtualisierten Umgebung auszuführen, fragen Sie den HSM-Hersteller nach Hypervisor-Unterstützung.

Schritt 1. Führen Sie während der Ersteinrichtung der FAS-Konfiguration mit der Verwaltungskonsole nur die ersten zwei Schritte aus: "Deploy certificate templates"und "Setup Certificate Authority".



Schritt 2: Aus der Dokumentation Ihres HSM erfahren Sie, welchen Wert der ProviderName Ihres HSM haben sollte. Wenn das HSM CAPI verwendet, wird der Anbieter in der Dokumentation möglicherweise als Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) bezeichnet. Wenn das HSM CNG verwendet, wird der Anbieter möglicherweise als Schlüsselspeicheranbieter (Key Storage Provider, KSP) bezeichnet.

Schritt 3: Bearbeiten Sie die Config-Datei wie folgt:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

Daraufhin sollte die Datei wie folgt aussehen:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

In diesem Szenario wird angenommen, dass Ihr HSM CNG verwendet, daher ist der Wert von ProviderLegacyCsp “false”. Wenn das HSM CAPI verwendet, sollte der Wert für ProviderLegacyCsp auf “true” festgelegt sein. Sie erfahren aus der Dokumentation des HSM-Herstellers, ob das HSM CAPI oder CNG verwendet. Außerdem erfahren Sie aus der Dokumentation, welche Schlüssellängen für die Generierung eines asymmetrischen RSA-Schlüssels das HSM unterstützt. In diesem Beispiel ist die Schlüssellänge auf den Standardwert von 2048 Bit festgelegt. Stellen Sie sicher, dass die von Ihnen festgelegte Schlüssellänge von der Hardware unterstützt wird.

Schritt 4: Starten Sie den Citrix Verbundauthentifizierungsdienst neu, damit die Werte aus der Config-Datei gelesen werden.

Schritt 5: Generieren Sie das RSA-Schlüsselpaar im HSM und erstellen Sie die CSR, indem Sie auf der Registerkarte “Initial Setup”der FAS-Verwaltungskonsole auf **Authorize** klicken.

Schritt 6: Um zu überprüfen, ob das Schlüsselpaar im HSM generiert wurde, überprüfen Sie die Anwendungseinträge im Windows-Ereignisprotokoll:


```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG]
HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

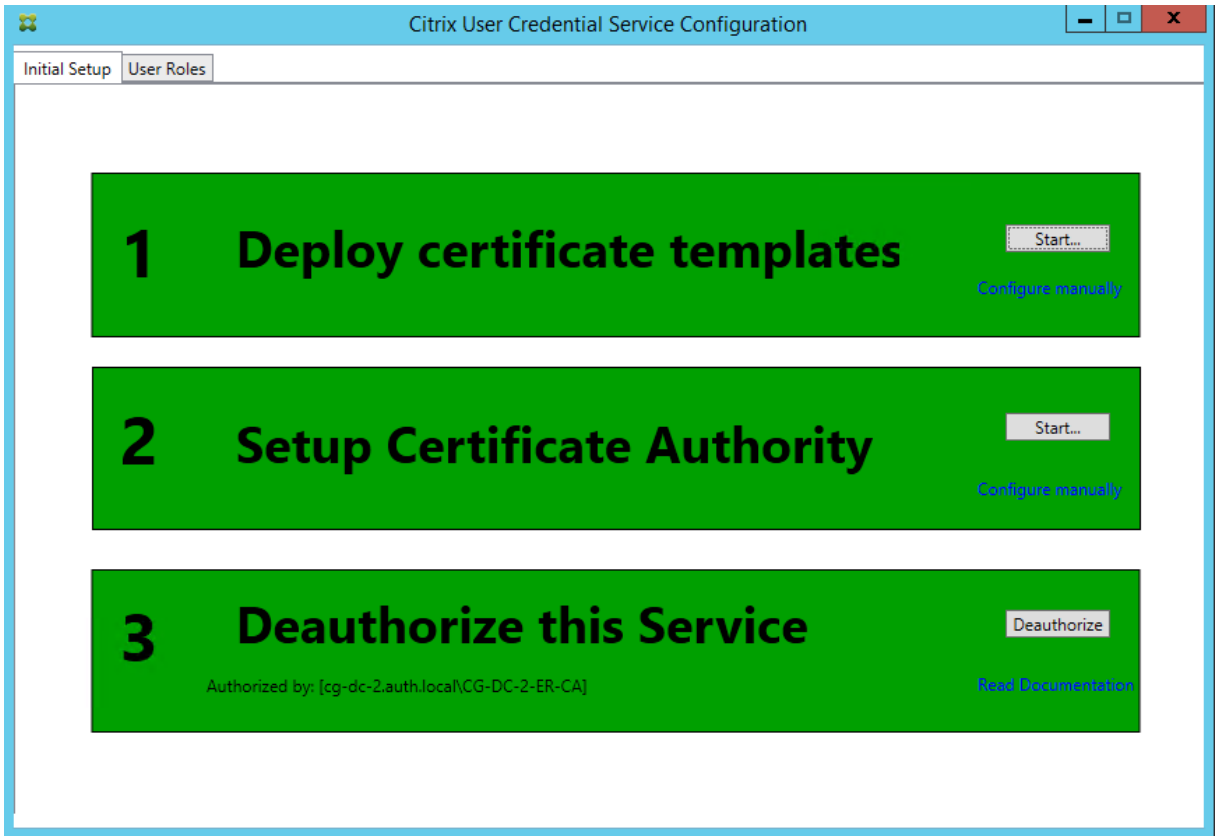
Hinweis: Folgendes sollte angezeigt werden: Provider: [CNG HSM_Vendor's Key Storage Provider]

Schritt 7: Wählen Sie auf dem CA-Server in der CA MMC den Knoten **Ausstehende Anforderungen**:

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

Klicken Sie mit der rechten Maustaste auf die Anforderung und wählen Sie **Ausstellen**.

Der Schritt "Authorize this Service"ist nun grün und der Text lautet nun "Deauthorize this Service". Der Eintrag unten gibt "Authorized by: [<CA-Name>]"an.



Schritt 8: Wählen Sie in der FAS-Verwaltungskonsole die Registerkarte **User Roles** und bearbeiten Sie die Einstellungen wie im FAS-Hauptartikel beschrieben.

Hinweis: Wenn Sie die Autorisierung des FAS über die Verwaltungskonsole aufheben, wird die Benutzerregel gelöscht.

FAS-Zertifikatspeicher

Der Verbundauthentifizierungsdienst verwendet nicht den Microsoft Zertifikatspeicher auf dem FAS-Server, um Zertifikate zu speichern. Stattdessen wird die Registrierung verwendet.

Hinweis: Wenn Sie ein HSM zum Speichern der privaten Schlüssel verwenden, werden die HSM-Container durch GUIDs identifiziert. Die GUID für den privaten Schlüssel im HSM stimmt mit der GUID für das entsprechende Zertifikat in der Registrierung überein.

Um die GUID für das RA-Zertifikat zu ermitteln, geben Sie die folgenden PowerShell-Cmdlets auf dem FAS-Server ein:

Add-pssnapin Citrix.a*

Get-FasAuthorizationCertificate –address <FAS server FQDN>

Beispiel:

Get-FasAuthorizationCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                 : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address            : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea          : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest :
Status             : MaintenanceDue

Id                 : fcb185f9-5069-4e34-8625-a333ac126535
Address            : [Offline CSR]
TrustArea          :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
                     MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                     hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                     Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORholV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                     zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                     ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                     3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                     oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                     bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                     PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                     GlO/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                     H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                     -----END CERTIFICATE REQUEST-----
Status             : WaitingForApproval
```

Geben Sie zum Abrufen einer Liste mit Benutzerzertifikaten Folgendes ein:

Get-FasUserCertificate –address <FAS server FQDN>

Beispiel:

Get-FasUserCertificate –address cg-fas-2.auth.net

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.

- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Übersicht über die gebräuchlichen FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.

Sicherheits- und Netzwerkkonfiguration für den Verbundauthentifizierungsdienst

August 18, 2021

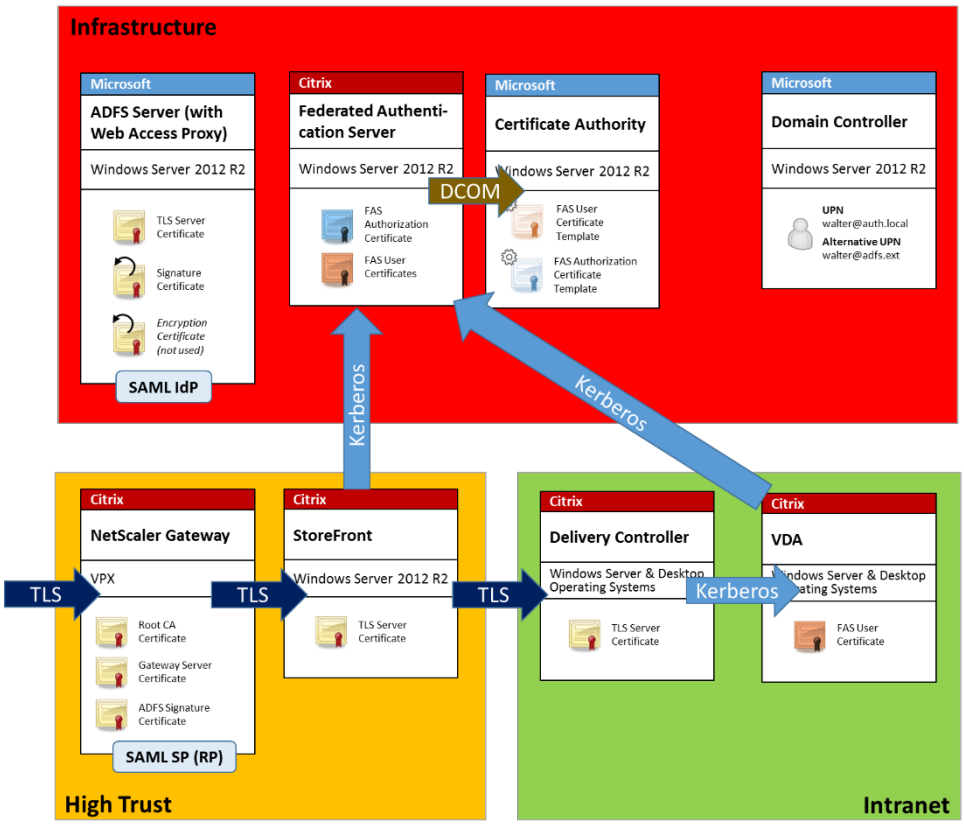
Der Citrix Verbundauthentifizierungsdienst (Federated Authentication Service, FAS) ist eng in Microsoft Active Directory und die Microsoft-Zertifizierungsstelle integriert. Es ist wichtig, das System richtig zu verwalten und zu schützen. Hierfür muss, wie bei Domänencontrollern oder anderen wichtigen Infrastrukturkomponenten auch, eine geeignete Sicherheitsrichtlinie entwickelt werden.

Dieses Dokument enthält eine Übersicht über die Sicherheitsfragen, die Sie bei der FAS-Bereitstellung berücksichtigen sollten. Außerdem finden Sie hier eine Übersicht über die Features, die Ihnen beim Schutz der Infrastruktur helfen können.

Netzwerkarchitektur

Die folgende Abbildung zeigt die wichtigsten Komponenten und Sicherheitsgrenzen einer FAS-Bereitstellung.

Der FAS-Server gilt zusammen mit der Zertifizierungsstelle und dem Domänencontroller als Teil der sicherheitskritischen Infrastruktur. In einer Verbundumgebung haben Citrix NetScaler und Citrix StoreFront eine Vertrauensstellung zur Durchführung der Benutzerauthentifizierung. Andere XenApp- und XenDesktop-Komponenten werden von einer FAS-Implementierung nicht betroffen.



Firewall und Netzwerksicherheit

Die Kommunikation zwischen NetScaler, StoreFront und den Delivery Controller-Komponenten muss durch TLS über Port 443 geschützt werden. Der StoreFront-Server führt nur ausgehende Verbindungen durch und NetScaler Gateway darf nur Verbindungen über das Internet mit HTTPS-Port 443 akzeptieren.

Der StoreFront-Server kontaktiert den FAS-Server über Port 80 unter Verwendung von beidseitig authentifiziertem Kerberos. Bei der Authentifizierung werden die Kerberos-HOST/fqdn-Identität des FAS-Servers und die Kerberos-Computerkontoidentität des StoreFront-Servers verwendet. Dadurch wird ein Anmeldehandle für die einmalige Verwendung erstellt, das der Citrix Virtual Delivery Agent (VDA) zur Anmeldung des Benutzers benötigt.

Wenn eine HDX-Sitzung mit dem VDA verbunden wird, kontaktiert der VDA außerdem den FAS-Server über Port 80. Bei der Authentifizierung werden die Kerberos-HOST/fqdn-Identität des FAS-Servers und die Kerberos-Computeridentität des VDAs verwendet. Außerdem muss der VDA das Anmeldeinformations-Handle übergeben, um auf Zertifikat und privaten Schlüssel zugreifen zu können.

Die Microsoft-Zertifizierungsstelle akzeptiert Kommunikation mit einem Kerberos-authentifizierten DCOM, das zur Verwendung eines festen TCP-Ports konfiguriert werden kann. Die Zertifizierungsstelle

erfordert außerdem, dass der FAS-Server ein durch ein vertrauenswürdiges Enrollment Agent-Zertifikat signiertes CMC-Paket übergibt.

Server	Firewallports
Verbundauthentifizierungsdienst	[eingehend] Kerberos über HTTP von StoreFront und VDAs, [ausgehend] DCOM zur Microsoft-ZS
NetScaler	[eingehend] HTTPS von Clientmaschinen, [eingehend/ausgehend] HTTPS zum/vom StoreFront-Server, [ausgehend] HDX zum VDA
StoreFront	[eingehend] HTTPS von NetScaler, [ausgehend] HTTPS an Delivery Controller, [ausgehend] Kerberos über HTTP an FAS
Delivery Controller	[eingehend] HTTPS vom StoreFront-Server, [eingehend/ausgehend] Kerberos über HTTP von VDAs
VDA	[eingehend/ausgehend] Kerberos über HTTP vom Delivery Controller, [eingehend] HDX von NetScaler Gateway, [ausgehend] Kerberos HTTP an FAS
Microsoft-Zertifizierungsstelle	[eingehend] DCOM und signiert von FAS

Verwaltungsaufgaben

Die Verwaltung der Umgebung lässt sich in folgende Zuständigkeiten aufgliedern:

Name	Aufgaben
Unternehmensadministrator	Installation und Schutz von Zertifikatvorlagen in der Gesamtstruktur
Domänenadministrator	Konfiguration der Gruppenrichtlinieneinstellungen
Zertifizierungsstellenadministrator	Konfigurieren der Zertifizierungsstelle
FAS-Administrator	Installieren und konfigurieren des FAS-Servers
StoreFront-/NetScaler-Administrator	Konfigurieren der Benutzerauthentifizierung
XenDesktop-Administrator	Konfigurieren von VDAs und Controllern

Jeder Administrator ist für verschiedene Aspekte des allgemeinen Sicherheitsmodells zuständig, sodass ein Defense-in-Depth-Schutz des Systems möglich ist.

Gruppenrichtlinieneinstellungen

Vertrauenswürdige FAS-Maschinen werden anhand einer über die Gruppenrichtlinie konfigurierten Nachschlagetabelle mit Indexnummer -> FQDN identifiziert. Beim Herstellen einer Verbindung mit dem FAS-Server prüfen Clients dessen HOST\<fqdn> Kerberos-Identität. Alle Server, die auf den FAS-Server zugreifen, müssen die gleiche FQDN-Konfiguration für denselben Index haben, ansonsten stellen StoreFront und VDAs möglicherweise eine Verbindung mit verschiedenen FAS-Servern her.

Zur Vermeidung von Konfigurationsfehlern empfiehlt Citrix die Anwendung einer einzelnen Richtlinie auf alle Maschinen in der Umgebung. Vorsicht beim Bearbeiten der Liste der FAS-Server, insbesondere wenn Sie Einträge entfernen oder umsortieren.

Die Steuerung dieses Gruppenrichtlinienobjekts sollte auf FAS-Administratoren (und/oder Domänenadministratoren) beschränkt werden, die FAS-Server installieren und außer Betrieb nehmen. Die Wiederverwendung von Maschinen-FQDNs kurz nach der Außerbetriebnahme eines FAS-Servers ist zu vermeiden.

Zertifikatvorlagen

Wenn Sie die mit dem FAS gelieferte Zertifikatvorlage "Citrix_SmartcardLogon"nicht verwenden möchten, können Sie eine Kopie davon modifizieren. Die folgenden Änderungen werden unterstützt:

Umbenennen der Zertifikatvorlage

Wenn Sie die Zertifikatvorlage "Citrix_SmartcardLogon"entsprechend dem Benennungsstandard Ihres Unternehmens umbenennen möchten, müssen Sie folgende Schritte ausführen:

- Erstellen Sie eine Kopie der Zertifikatvorlage und benennen Sie sie gemäß Ihrem Benennungsstandard.
- Verwenden Sie zum Verwalten von FAS nicht die Verwaltungsbenutzeroberfläche, sondern die FAS-PowerShell-Befehle. (Die Verwaltungsbenutzeroberfläche ist nur zur Verwendung mit den Citrix Standardvorlagennamen vorgesehen.)
  - Veröffentlichen Sie die Vorlage mit dem Microsoft MMC-Zertifikatvorlagen-Snap-In oder mit dem Befehl "Publish-FasMsTemplate".
  - Konfigurieren Sie FAS mit dem Befehl "New-FasCertificateDefinition"für den Namen der Vorlage.

Ändern allgemeiner Eigenschaften

Sie können die Gültigkeitsdauer der Zertifikatvorlage ändern.

Ändern Sie nicht den Verlängerungszeitraum. FAS ignoriert diese Einstellung in der Zertifikatvorlage. FAS aktualisiert das Zertifikat automatisch nach Ablauf der halben Gültigkeitsdauer.

Ändern der Anforderungsverarbeitung

Ändern Sie diese Eigenschaften nicht. FAS ignoriert diese Einstellungen in der Zertifikatvorlage. FAS deaktiviert immer die Einstellungen **Exportieren von privatem Schlüssel zulassen** und **Mit gleichem Schlüssel erneuern**.

Ändern der Kryptographieeigenschaften

Ändern Sie diese Eigenschaften nicht. FAS ignoriert diese Einstellungen in der Zertifikatvorlage.

Informationen zu gleichwertigen Einstellungen in FAS finden Sie unter Schutz durch private Schlüssel beim Verbundauthentifizierungsdienst.

Ändern der Schlüsselnachweiseigenschaften

Ändern Sie diese Eigenschaften nicht. FAS unterstützt keinen Schlüsselnachweis.

Ändern der Eigenschaften für abgelöste Vorlagen

Ändern Sie diese Eigenschaften nicht. FAS unterstützt keine Vorlagenablösung.

Ändern der Erweiterungseigenschaften

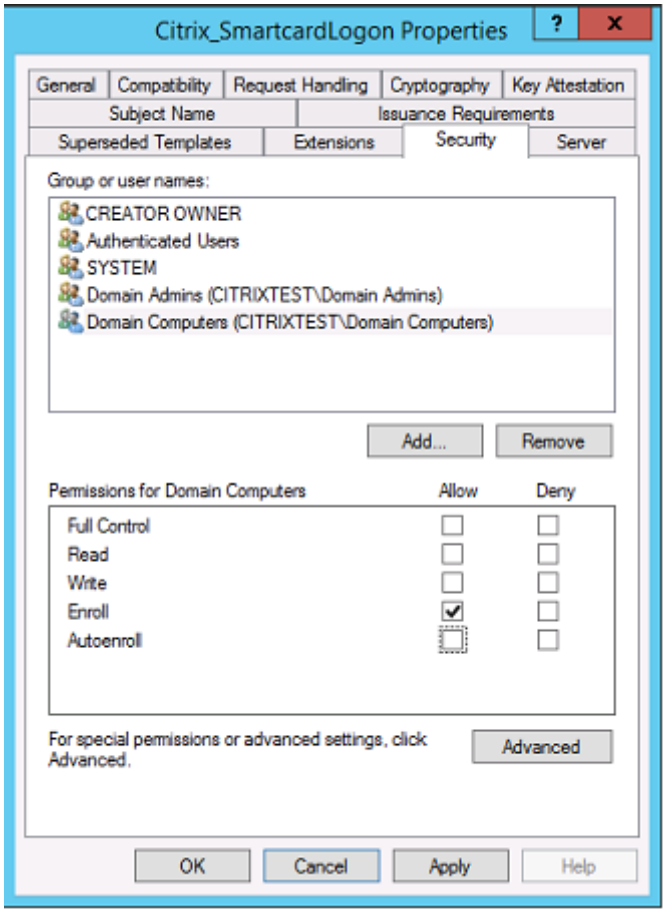
Sie können diese Einstellungen entsprechend den Richtlinien Ihres Unternehmens ändern.

Hinweis: Ungeeignete Erweiterungseinstellungen können Sicherheitsprobleme verursachen oder zur Unbrauchbarkeit von Zertifikaten führen.

Ändern der Sicherheitseigenschaften

Citrix empfiehlt die Änderung dieser Einstellungen, sodass die Berechtigungen **Lesen** und **Registrieren** ausschließlich für Maschinenkonten der FAS-Server zugelassen werden. Für den Verbundauthentifizierungsdienst sind keine weiteren Berechtigungen erforderlich. Wie bei anderen Zertifikatvorlagen sollten Sie jedoch Folgendes tun:

- Administratoren erlauben, die Vorlage zu lesen und schreiben
- Authentifizierten Benutzern erlauben, die Vorlage zu lesen



Ändern der Eigenschaften des Antragstellernamens

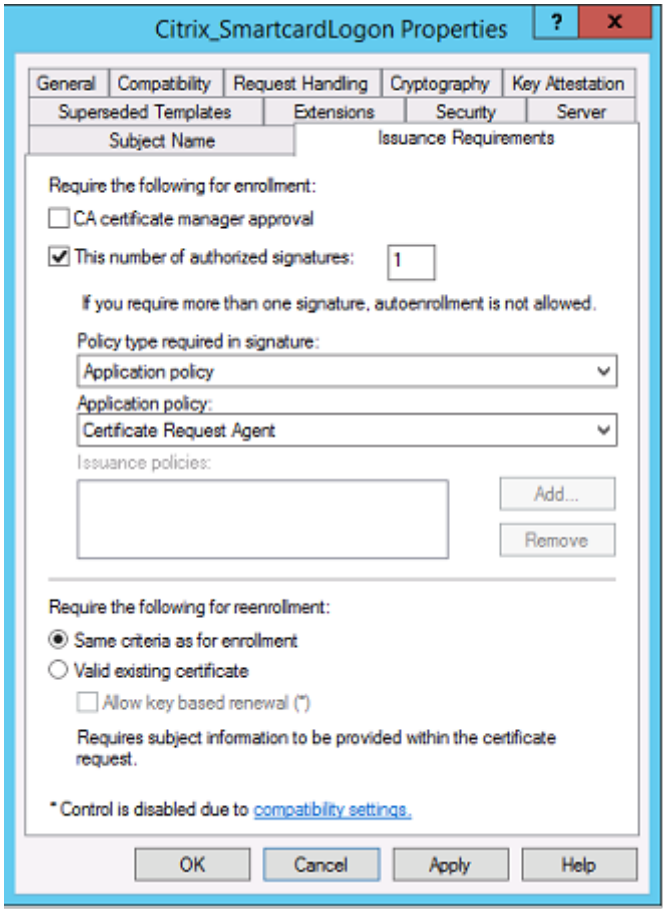
Falls erforderlich, können Sie diese Einstellung entsprechend den Richtlinien Ihres Unternehmens ändern.

Ändern von Servereigenschaften

Falls erforderlich, können Sie diese Einstellung entsprechend den Richtlinien Ihres Unternehmens ändern. Citrix rät davon ab.

Ändern der Ausstellungsvoraussetzungen

Ändern Sie diese Einstellungen nicht. Diese Einstellungen müssen immer folgendermaßen festgelegt sein:



Ändern der Kompatibilitätseigenschaften

Sie können diese Einstellungen ändern. Die Mindesteinstellung ist **Windows Server 2003 CAs** (Schemaversion 2). FAS unterstützt jedoch nur Zertifizierungsstellen für Windows Server 2008 und höher. Wie oben erläutert ignoriert FAS außerdem die zusätzlichen Einstellungen für **Windows Server 2008 CAs** (Schemaversion 3) und **Windows Server 2012 CAs** (Schemaversion 4).

Zertifizierungsstellenverwaltung

Der ZS-Administrator ist für die Konfiguration des ZS-Servers und des von diesem für das Ausstellerzertifikat verwendeten privaten Schlüssels verantwortlich.

Veröffentlichen von Vorlagen

Damit eine Zertifizierungsstelle Zertifikate basierend auf einer vom Unternehmensadministrator bereitgestellten Vorlage ausstellen kann, muss der ZS-Administrator die Vorlage veröffentlichen.

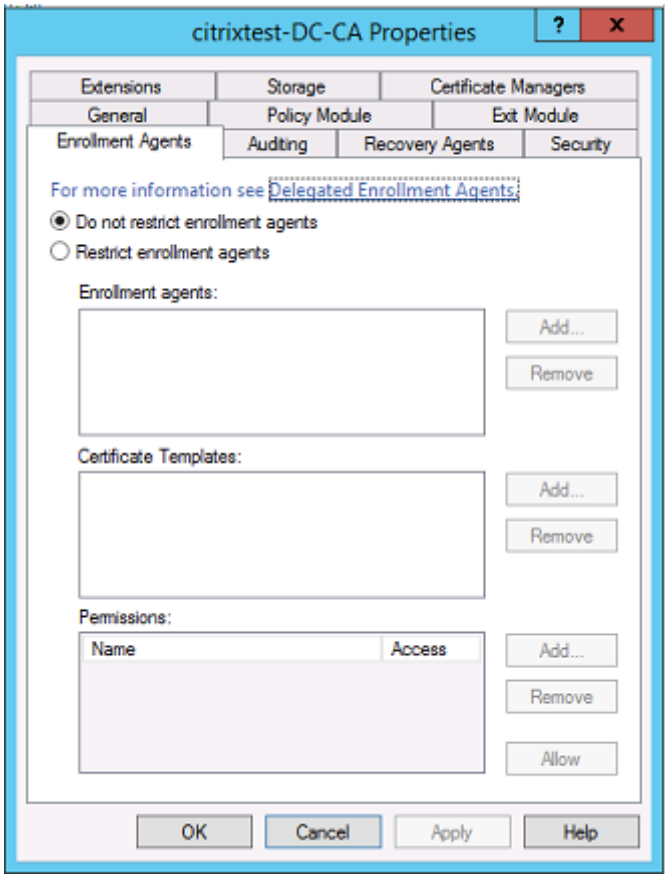
Eine einfache Sicherheitsmaßnahme besteht darin, die Registrierungsstellenzertifikate nur zu veröffentlichen, wenn die FAS-Server installiert werden, oder ein Ausstellungsverfahren vorzuschreiben, das komplett offline ist. In beiden Fällen darf nur der ZS-Administrator Registrierungsstellenzertifikate autorisieren und er muss eine Richtlinie für die Autorisierung von FAS-Servern haben.

Firewalleinstellungen

Im Allgemeinen kann der ZS-Administrator auch die Firewalleinstellungen der Zertifizierungsstelle festlegen und somit eingehende Verbindungen steuern. Der ZS-Administrator kann DCOM TCP- und Firewallregeln so konfigurieren, dass nur FAS-Server Zertifikate anfordern können.

Eingeschränkte Registrierung

Standardmäßig kann jeder Eigentümer eines Registrierungsstellenzertifikats beliebigen Benutzern ein Zertifikat auf der Basis einer Zertifikatvorlage, die Zugriff ermöglicht, ausstellen. Dies sollte auf eine Gruppe von Benutzern ohne Privilegien über die Zertifizierungsstelleneigenschaft “Restrict enrollment agents”eingeschränkt werden.



Richtlinienmodule und Überwachung

In komplexeren Bereitstellungen können benutzerdefinierte Sicherheitsmodule verwendet werden, um die Zertifikatausstellung zu verfolgen und zu unterbinden.

FAS-Verwaltung

Der FAS hat mehrere Sicherheitsfeatures.

Beschränken von StoreFront, Benutzern und VDAs über eine ACL

Im Zentrum des FAS-Sicherheitsmodells liegt die Steuerung des Zugriffs auf Funktionen durch Kerberos-Konten:

Zugriffsvektor	Beschreibung
StoreFront [IdP]	Diese Kerberos-Konten können deklarieren, dass ein Benutzer korrekt authentifiziert wurde. Bei Gefährdung eines dieser Konten können Zertifikate erstellt und für durch die FAS-Konfiguration zugelassene Benutzer verwendet werden.
VDAs [vertrauende Seite]	Dies sind die Maschinen, die auf Zertifikate und private Schlüssel zugreifen dürfen. Zusätzlich ist ein vom IdP abgerufenes Anmelde-Handle erforderlich, sodass ein gefährdetes VDA-Konto in dieser Gruppe nur geringe Möglichkeiten für einen Angriff auf das System hat.
Benutzer	Hierdurch wird gesteuert, welche Benutzer vom IdP bestätigt werden können. Es besteht eine Überschneidung mit den Zertifizierungsstellenoptionen “Restrict enrollment agents”. Im Allgemeinen sollten nur nicht-privilegierte Benutzerkonten in diese Liste aufgenommen werden. Dies verhindert, dass ein gefährdetes StoreFront-Konto Privilegien auf eine höhere Verwaltungsebene übertragen kann. Vor allem Domänenadministratorkonten dürfen keine Berechtigung durch diese ACL erhalten.

Konfigurieren von Regeln

Regeln sind nützlich, wenn mehrere eigenständige XenApp- oder XenDesktop-Bereitstellungen die gleiche FAS-Serverinfrastruktur verwenden. Jede Regel hat eigene Konfigurationsoptionen, wobei insbesondere separate Zugriffssteuerungslisten konfiguriert werden können.

Konfigurieren von Zertifizierungsstelle und Vorlagen

Für verschiedene Zugriffsrechte können verschiedene Zertifikatvorlagen und Zertifizierungsstellen konfiguriert werden. In komplexen Konfigurationen werden ggf. abhängig von der Umgebung weniger oder leistungsfähigere Zertifikate verwendet. Beispiel: Als extern identifizierte Benutzer können ein Zertifikat mit weniger Berechtigungen als interne Benutzer haben.

Sitzungsinterne und Authentifizierungszertifikate

Der FAS-Administrator kann festlegen, ob das für die Authentifizierung verwendete Zertifikat in der Sitzung eines Benutzers verwendet werden kann. Damit kann beispielsweise festgelegt werden, dass nur Signaturzertifikate sitzungsintern zur Verfügung stehen und die leistungsfähigeren Anmeldezertifikate nur bei der Anmeldung.

Schutz privater Schlüssel und Schlüssellänge

Der FAS-Administrator kann den FAS so konfigurieren, dass private Schlüssel in einem Hardwaresicherheitsmodul (HSM) oder einem Trusted Platform Module (TPM) gespeichert werden. Citrix empfiehlt, zumindest den privaten Schlüssel des Registrierungsstellenzertifikats durch Speicherung in einem TPM zu schützen. Diese Option kann im Offline-Verfahren für die Zertifikatanforderung gewählt werden.

Auch die privaten Schlüssel für Benutzerzertifikate können in einem TPM oder HSM gespeichert werden. Alle Schlüssel müssen als nicht exportierbar generiert werden und eine Länge von mindestens 2048 Bit haben.

Ereignisprotokolle

Der FAS-Server bietet detaillierte Konfigurations- und Laufzeit-Ereignisprotokolle, die für die Überwachung und Angriffserkennung verwendet werden können.

Verwaltungszugriff und Verwaltungstools

Der FAS umfasst Features und Tools zur Remoteverwaltung (unter gegenseitiger Kerberos-Authentifizierung). Mitglieder der lokalen Administratorgruppe haben Vollzugriff auf die FAS-Konfiguration. Diese Liste muss sorgfältig gepflegt werden.

XenApp-, XenDesktop- und VDA-Administratoren

Generell ändert die Verwendung des FAS nichts am Sicherheitsmodell für Delivery Controller- und VDA-Administratoren, da das FAS-Anmeldeinformations-Handle direkt das Active Directory-Kennwort ersetzt. Controller- und VDA-Administratorgruppen dürfen nur vertrauenswürdige Benutzer enthalten. Es müssen Überwachungs- und Ereignisprotokolle geführt werden.

Allgemeine Windows-Serversicherheit

Für alle Server müssen sämtliche Patches installiert sein und Standardfirewall- und Antivirensoftware zur Verfügung stehen. Sicherheitskritische Infrastrukturserver müssen an einem sicheren physischen Standort sein, Optionen für Datenträgerverschlüsselung und die Wartung virtueller Maschinen müssen sorgfältig gewählt werden.

Überwachungs- und Ereignisprotokolle müssen sicher auf einem Remotecomputer gespeichert werden.

Der RDP-Zugriff muss auf autorisierte Administratoren beschränkt werden. Soweit möglich sollten Benutzerkonten eine Smartcard-Anmeldung erfordern. Dies gilt insbesondere für Zertifizierungsstellen- und Domänenadministratorkonten.

Verwandte Informationen

- Der Artikel Verbundauthentifizierungsdienst ist die primäre Referenz für die Installation und Konfiguration dieser Komponente.
- Der Artikel Übersicht über die Architekturen des Verbundauthentifizierungsdiensts enthält eine Einführung zu den FAS-Architekturen.
- Der Artikel Anleitung: Konfigurieren und Verwalten des Verbundauthentifizierungsdiensts enthält Links zu weiteren Anleitungen.

Problembehandlung von Windows-Anmeldeproblemen mit dem Verbundauthentifizierungsdienst

August 18, 2021

In diesem Artikel werden die Protokolle und Fehlermeldungen beschrieben, die in Windows verfügbar sind, wenn sich Benutzer mit Zertifikaten und/oder Smartcards anmelden. Die Protokolle enthalten Informationen, die bei der Problembehandlung von Authentifizierungsfehlern hilfreich sein können.

Zertifikate und Public Key-Infrastruktur

Windows Active Directory unterhält mehrere Zertifikatspeicher, in denen Zertifikate für Benutzer verwaltet werden, die sich anmelden.

- **NTAuth-Zertifikatspeicher:** Für die Authentifizierung bei Windows muss die Zertifizierungsstelle, die Benutzerzertifikate sofort ausstellt (Verkettung wird nicht unterstützt), im NTAuth-Speicher platziert werden. Geben Sie zum Anzeigen dieser Zertifikate im certutil-Programm Folgendes ein: certutil –viewstore –enterprise NTAuth.
- **Speicher für Stamm- und Zwischenzertifikate:** Normalerweise können Zertifikatanmeldesysteme nur ein einzelnes Zertifikat zur Verfügung stellen. Wenn eine Kette verwendet wird, muss daher der Zwischenzertifikatspeicher auf allen Maschinen diese Zertifikate enthalten. Das Stammzertifikat muss im vertrauenswürdigen Stammspeicher und das vorletzte Zertifikat muss im NTAuth-Speicher sein.
- **Anmeldezertifikat-Erweiterungen und Gruppenrichtlinie:** Windows kann so konfiguriert werden, dass die Überprüfung von EKUs und anderen Zertifikatrichtlinien erzwungen wird. Informationen finden Sie in der Microsoft-Dokumentation auf https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)?redirectedfrom=MSDN.

Registrierungsrichtlinie	Beschreibung
AllowCertificatesWithNoEKU	Wenn deaktiviert, müssen Zertifikate die Smartcard-Anmeldung “Erweiterte Schlüsselverwendung”(Enhanced Key Usage, EKU) enthalten.

Registrierungsrichtlinie	Beschreibung
AllowSignatureOnlyKeys	Standardmäßig filtert Windows die privaten Schlüssel aus Zertifikaten heraus, die RSA-Entschlüsselung nicht zulassen. Diese Option setzt den Filter außer Kraft.
AllowTimeInvalidCertificates	Standardmäßig filtert Windows abgelaufene Zertifikate heraus. Diese Option setzt den Filter außer Kraft.
EnumerateECCCerts	Aktiviert die Authentifizierung mit elliptischen Kurven.
X509HintsNeeded	Mit dieser Option können Benutzer ihr Windows-Anmeldekonto manuell angeben, wenn ein Zertifikat keinen eindeutigen Benutzerprinzipalnamen (UPN) enthält oder der Name mehrdeutig ist.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Deaktiviert die Überprüfung von Sperrlisten (normalerweise auf dem Domänencontroller festgelegt).

- **Domänencontrollerzertifikate:** Zum Authentifizieren von Kerberos-Verbindungen müssen alle Server entsprechende Domänencontrollerzertifikate haben. Diese können mit dem MMC-Snap-In-Menü "Local Computer Certificate Personal Store"angefordert werden.

Zuordnung von UPN-Namen und Zertifikaten

Es wird empfohlen, dass die Erweiterung des alternativen Antragstellernamens in Benutzerzertifikaten einen eindeutigen UPN (Benutzerprinzipalname) enthält.

UPN-Namen in Active Directory

Standardmäßig hat jeder Benutzer in Active Directory eine implizite UPN entsprechend den Mustern <samUsername>@<domainNetBios> und <samUsername>@<domainFQDN>. Die verfügbaren Domänen und FQDNs sind im RootDSE-Eintrag für die Gesamtstruktur enthalten. Für eine einzelne Domäne können mehrere FQDN-Adressen im RootDSE registriert sein.

Darüber hinaus hat jeder Benutzer in Active Directory eine explizite UPN und altUserPrincipalNames. Dies sind LDAP-Einträge, die den UPN für den Benutzer angeben.

Wenn Benutzer anhand der UPN gesucht werden, sucht Windows zuerst in der aktuellen Domäne (basierend auf der Identität des Prozesses bei der Suche nach der UPN) nach expliziten UPNs und dann

nach alternativen UPNs. Wenn keine Übereinstimmungen gefunden werden, wird nach der impliziten UPN gesucht, die möglicherweise in anderen Domänen in der Gesamtstruktur aufgelöst wird.

Zertifikatszuordnungsdienst

Wenn ein Zertifikat keine explizite UPN enthält, kann Active Directory für jede Verwendung ein genaues öffentliches Zertifikat in einem "x509certificate"-Attribut speichern. Um ein solches Zertifikat in einen Benutzer aufzulösen, kann ein Computer eine direkte Abfrage für dieses Attribut durchführen (standardmäßig in einer einzelnen Domäne).

Der Benutzer hat die Option, ein Benutzerkonto anzugeben, das die Suche beschleunigt. Dieses Feature kann außerdem in einer domänenübergreifenden Umgebung verwendet werden.

Wenn die Gesamtstruktur mehrere Domänen enthält und der Benutzer eine Domäne nicht explizit angibt, kann der Speicherort des Zertifikatzuordnungsdiensts mit Active Directory rootDSE angegeben werden. Dies ist normalerweise auf einer Maschine des globalen Katalogs und umfasst die zwischengespeicherte Anzeige aller x509certificate-Attribute in der Gesamtstruktur. Mit diesem Computer kann ein Benutzerkonto basierend auf dem Zertifikat effizient in jeder Domäne gesucht werden.

Steuern der Domänencontrollerauswahl für die Anmeldung

Wenn eine Umgebung mehrere Domänencontroller umfasst, ist es sinnvoll einzuschränken, welcher Domänencontroller für die Authentifizierung verwendet wird, damit Protokolle aktiviert und abgerufen werden können.

Steuern der Domänencontrollerauswahl

Sie können Windows zur Verwendung eines bestimmten Windows-Domänencontrollers für die Anmeldung zwingen, indem Sie durch Konfigurieren der Datei lmhosts eine explizite Liste mit Domänencontrollern festlegen, die eine Windows-Maschine verwendet: \Windows\System32\drivers\etc\lmhosts.

In diesem Speicherort ist normalerweise eine Beispieldatei namens "lmhosts.sam". Fügen Sie einfach eine Zeile hinzu:

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

"1.2.3.4"ist die IP-Adresse des Domänencontrollers "dcnetbiosname"in der Domäne "mydomain".

Nach einem Neustart verwendet die Windows-Maschine diese Informationen, um sich bei "mydomain"anzumelden. Diese Konfiguration muss zurückgesetzt werden, wenn das Debuggen abgeschlossen ist.

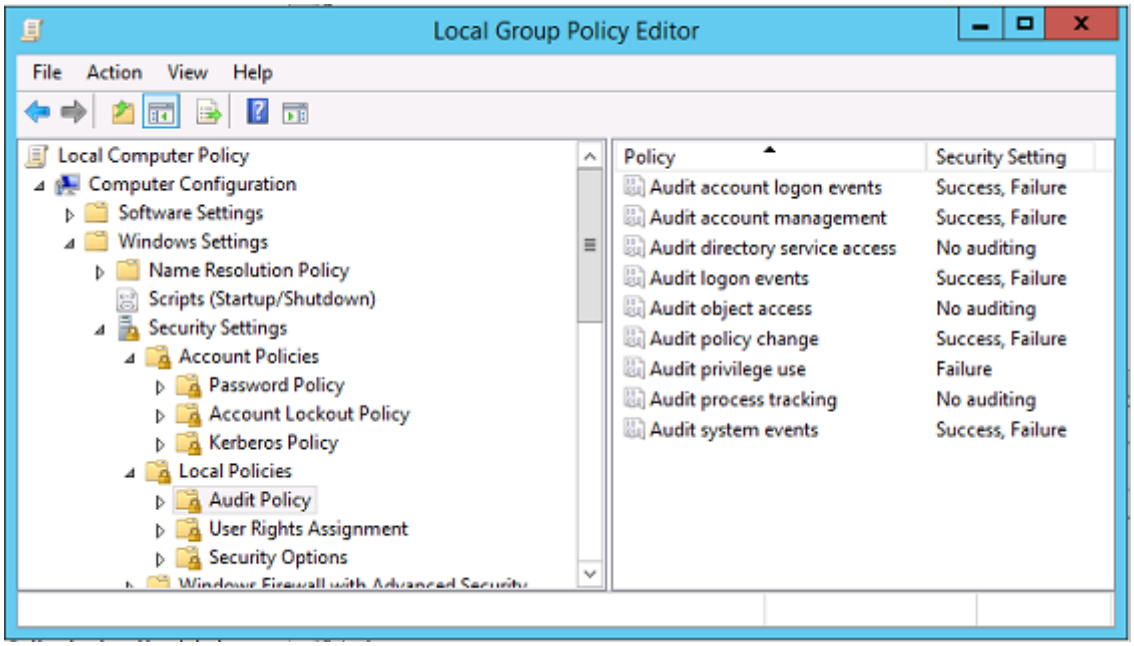
Identifizieren des verwendeten Domänencontrollers

Bei der Anmeldung platziert Windows eine MSDOS-Umgebungsvariable in dem Domänencontroller, der den Benutzer angemeldet hat. Zum Anzeigen starten Sie die Befehlszeile mit dem folgenden Befehl: **echo %LOGONSERVER%**.

Authentifizierungsprotokolle werden auf dem Computer gespeichert, den dieser Befehl zurückgibt.

Aktivieren von Kontoüberwachungsereignissen

Standardmäßig aktivieren Windows-Domänencontroller keine vollständigen Überwachungsprotokolle für Konten. Überwachungsprotokolle können mit Überwachungsrichtlinien in den Sicherheitseinstellungen im Gruppenrichtlinien-Editor gesteuert werden. Wenn sie aktiviert sind, schreibt der Domänencontroller zusätzliche Ereignisprotokollinformationen in die Protokolldatei.



Zertifikatüberprüfungsprotokolle

Überprüfen der Zertifikatgültigkeit

Wenn ein Smartcardzertifikat als DER-Zertifikat (kein privater Schlüssel erforderlich) exportiert wird, können Sie es mit folgendem Befehl überprüfen: certutil –verify user.cer

Aktivieren der CAPI-Protokollierung

Öffnen Sie auf dem Domänencontroller und den Benutzermaschinen die Ereignisanzeige und aktivieren Sie die Protokollierung für Microsoft/Windows/CAPI2/Operational Logs.

Sie können die CAPI-Protokollierung mit den Registrierungsschlüsseln hier steuern: CurrentControlSet\Services\crypt32.

Wert	Beschreibung
DiagLevel (DWORD)	Ausführlichkeitsgrad (0 bis 5)
DiagMatchAnyMask (QUADWORD)	Ereignisfilter (0xffffff für alle)
DiagProcessName (MULTI_SZ)	Nach Prozessname filtern (z. B. LSASS.exe)

CAPI-Protokolle

Meldung	Beschreibung
Build Chain	LSA-Aufruf: CertGetCertificateChain (einschließlich Ergebnis)
Verify Revocation	LSA-Aufruf: CertVerifyRevocation (einschließlich Ergebnis)
X509 Objects	Im ausführlichen Modus werden Zertifikate und Zertifikatsperrlisten (CRLs) im Verzeichnis \AppData\LocalLow Microsoft\X509Objects ausgegeben
Verify Chain Policy	LSA-Aufruf: CertVerifyChainPolicy (einschließlich Parameter)

Fehlermeldungen

Fehlercode	Beschreibung
Zertifikat ist nicht vertrauenswürdig	Das Smartcardzertifikat konnte nicht mit Zertifikaten aus den Speichern für Zwischenzertifikate und vertrauenswürdige Stammzertifikate erstellt werden.

Fehlercode	Beschreibung
Certificate revocation check error	Die Zertifikatsperrliste für die Smartcard konnte nicht von der Adresse heruntergeladen werden, die vom Zertifikatsperrlisten-Verteilungspunkt angegeben wurde. Wenn die Zertifikatsperrüberprüfung obligatorisch ist, schlagen Anmeldungen fehl. Weitere Informationen finden Sie im Abschnitt Zertifikate und Public Key-Infrastruktur.
Certificate Usage errors	Das Zertifikat ist nicht für Anmeldungen geeignet. Es ist möglicherweise ein Serverzertifikat oder ein Signaturzertifikat.

Kerberos-Protokolle

Erstellen Sie folgende Registrierungswerte, um Kerberos-Protokollierung auf dem Domänencontroller und der Maschine des Endbenutzers zu aktivieren:

Struktur	Wertname	Wert [DWORD]
CurrentControlSet\Control\Lsa\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebugLevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Die Kerberos-Protokollierung wird im Systemereignisprotokoll aufgezeichnet.

- Meldungen wie “untrusted certificate”sind in der Regel einfach zu diagnostizieren.
- Zwei Fehlercodes sind nur zur Information und können ignoriert werden:
  - KDC_ERR_PREAUTH_REQUIRED (für die Abwärtskompatibilität bei älteren Domänencontrollern)
  - Unknown error 0x4b

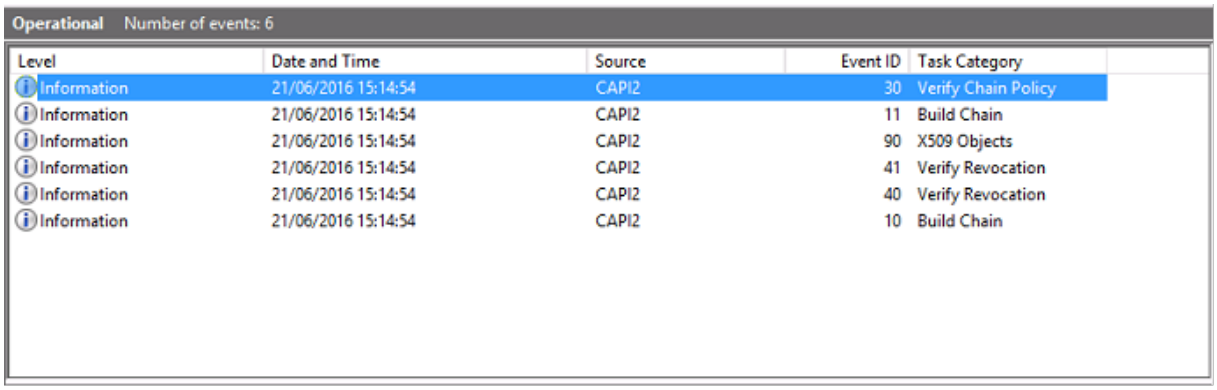
Ereignisprotokollmeldungen

Dieser Abschnitt beschreibt die auf dem Domänencontroller und der Arbeitsstation erwarteten Protokolleinträge, wenn Benutzer sich mit einem Zertifikat anmelden.

- CAPI2-Protokoll des Domänencontrollers
- Sicherheitsprotokoll des Domänencontrollers
- VDA-Sicherheitsprotokoll
- VDA-CAPI-Protokoll
- VDA-Systemprotokoll

CAPI2-Protokoll des Domänencontrollers

Bei einer Anmeldung überprüft der Domänencontroller das Zertifikat des Aufrufenden, wodurch eine Sequenz von Protokolleinträgen wie nachfolgend dargestellt erstellt wird.



Operational Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain Policy
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	10	Build Chain

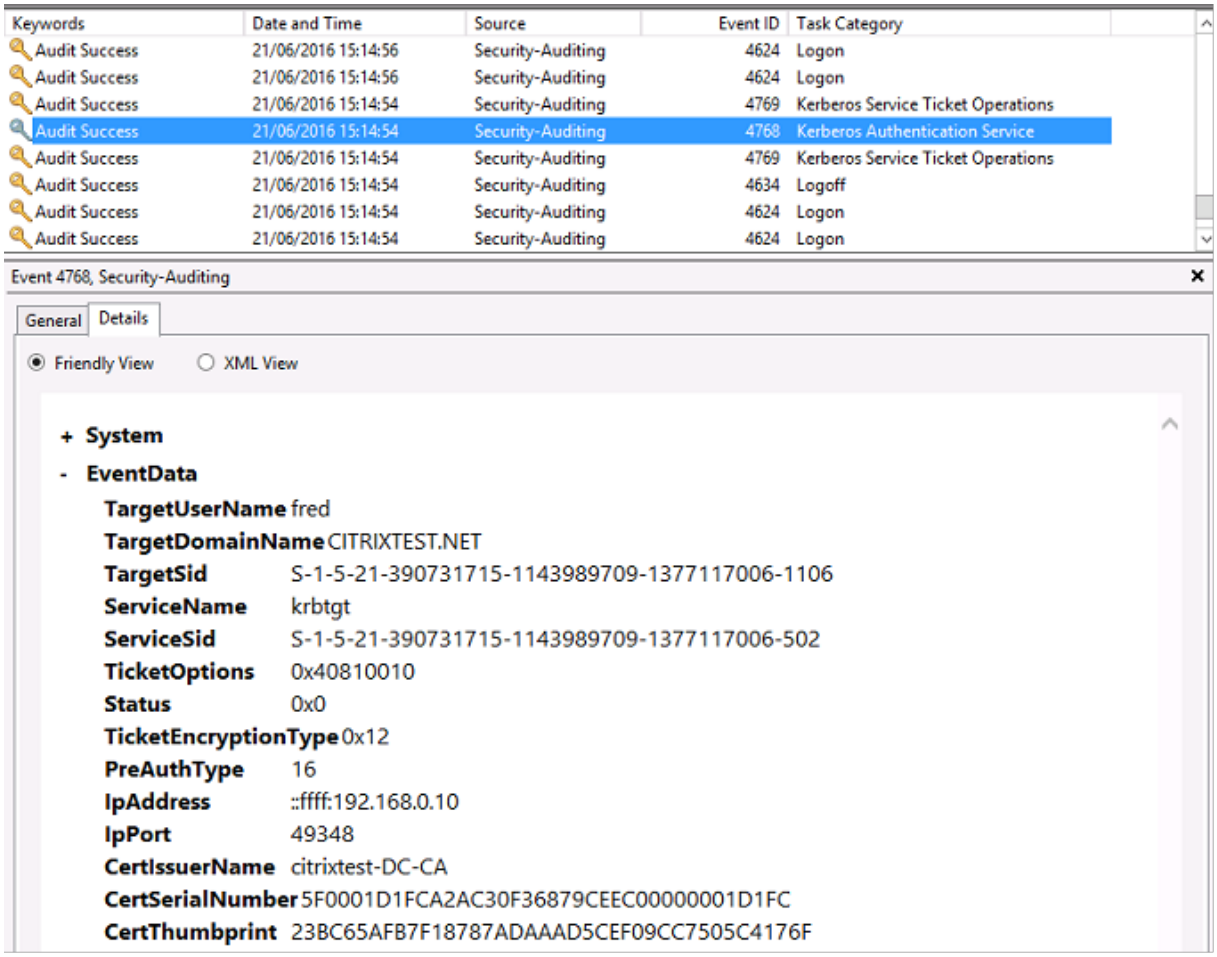
Die letzte Meldung zeigt, dass lsass.exe auf dem Domänencontroller basierend auf dem vom VDA bereitgestellten Zertifikat eine Kette erstellt und sie auf Gültigkeit überprüft (einschließlich Sperrung). Das zurückgegebene Ergebnis ist “ERROR_SUCCESS”.

- **CertVerifyCertificateChainPolicy**
  - **Policy**
    [**type**] CERT_CHAIN_POLICY_NT_AUTH
    [**constant**] 6
  - **Certificate**
    [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    [**subjectName**] fred
  - **CertificateChain**
    [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    [**value**] 0
  - **Status**
    [**chainIndex**] -1
    [**elementIndex**] -1
  - **EventAuxInfo**
    [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    [**SeqNumber**] 1
  - **Result**
    [**value**] 0

Sicherheitsprotokoll des Domänencontrollers

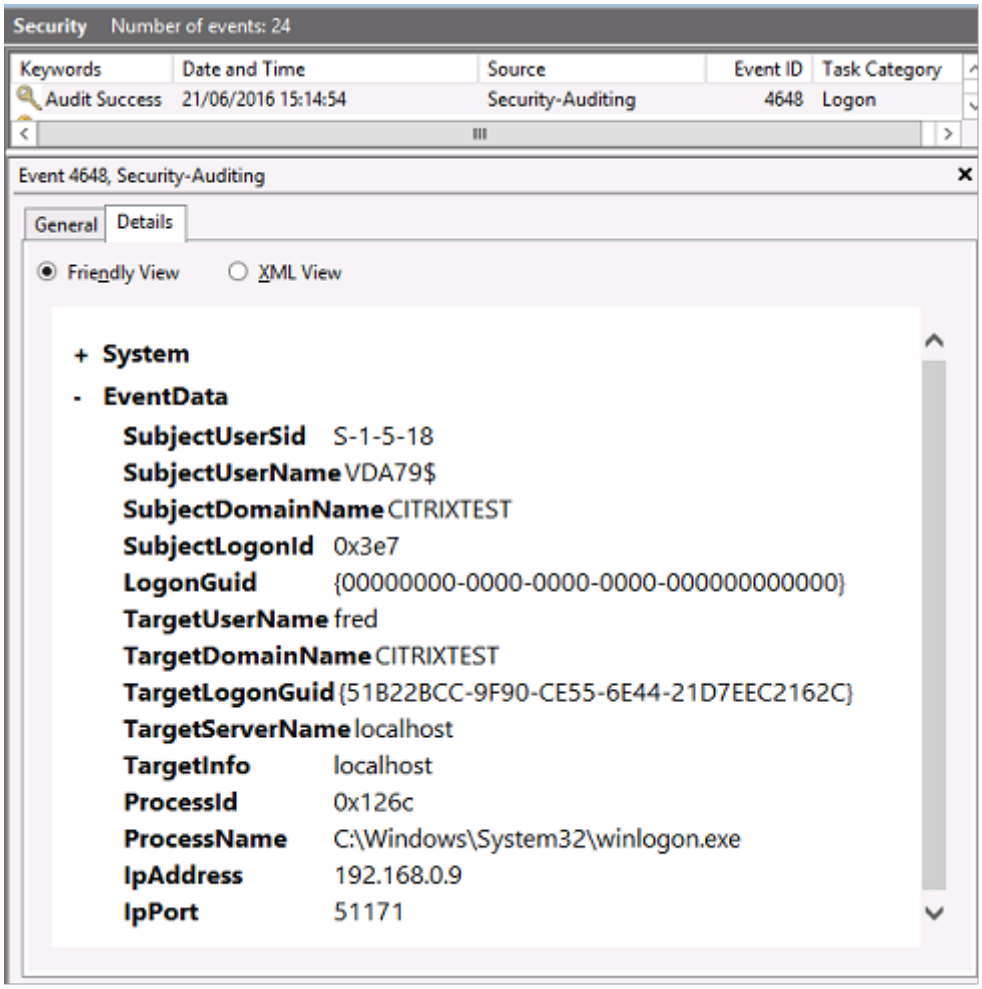
Der Domänencontroller zeigt eine Reihe von Anmeldeereignissen an, wobei das Ereignis 4768, die Verwendung des Zertifikats zum Ausstellen des Kerberos Ticket Granting Ticket (krbtgt), das wichtigste ist.

Die vorhergehenden Meldungen zeigen, wie sich das Maschinenkonto des Servers beim Domänencontroller authentifiziert. Die darauffolgenden Meldungen zeigen, wie mit dem Benutzerkonto, das nun zum neuen krbtgt gehört, die Authentifizierung beim Domänencontroller durchgeführt wird.



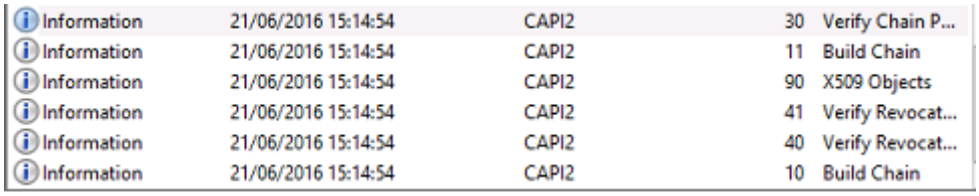
VDA-Sicherheitsprotokoll

Das VDA-Sicherheitsüberwachungsprotokoll, das der Anmeldung entspricht, ist der Eintrag mit der Ereignis-ID 4648, der von winlogon.exe verursacht wurde.



VDA-CAPI-Protokoll

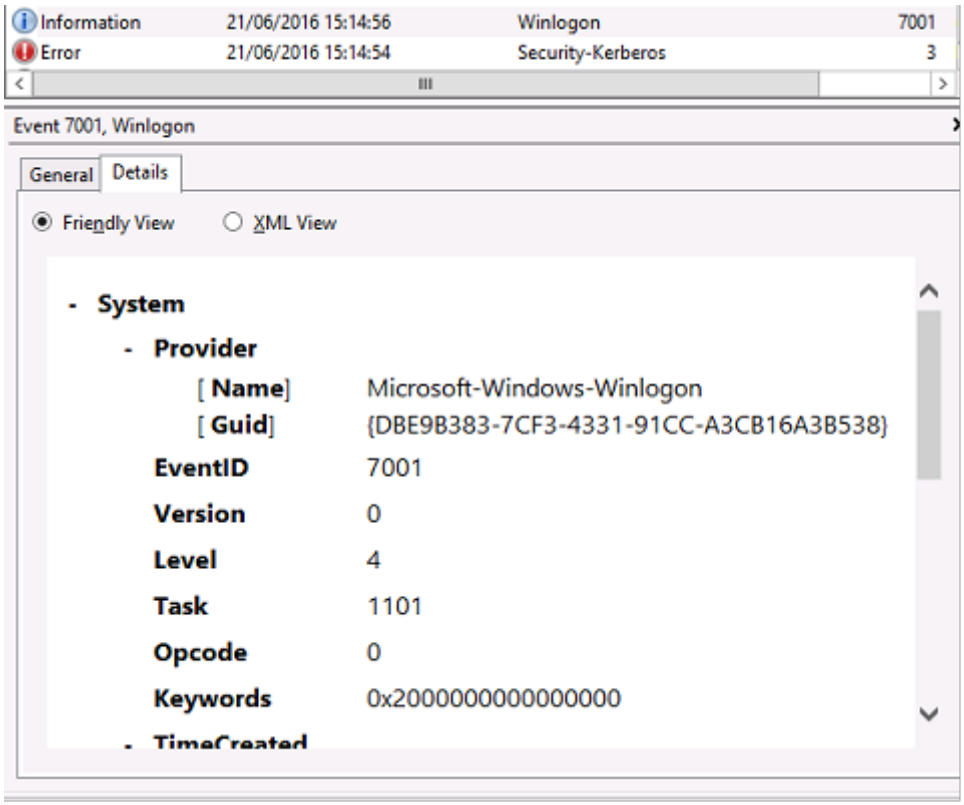
Dieses VDA-CAPI-Beispielprotokoll zeigt eine erstellte Kette und eine Überprüfungssequenz von lsass.exe, mit der das Domänencontrollerzertifikat (dc.citrixtest.net) überprüft wurde.



- **UserData**
  - **CertVerifyCertificateChainPolicy**
    - **Policy**
      - [**type**] CERT_CHAIN_POLICY_NT_AUTH
      - [**constant**] 6
    - **Certificate**
      - [**fileRef**] 813C6D12E1E1800E61B8DB071E186EB912B7
      - [**subjectName**] dc.citrixtest.net
    - **CertificateChain**
      - [**chainRef**] {84E0B3D1-A4D4-4AC7-BA99-5291415B343
    - **Flags**
      - [**value**] 0
    - **Status**
      - [**chainIndex**] -1

VDA-Systemprotokoll

Wenn die Kerberos-Protokollierung aktiviert ist, enthält das Systemprotokoll die Fehlermeldung KDC_ERR_PREAUTH_REQUIRED, die ignoriert werden kann, und einen Eintrag von Winlogon zur erfolgreichen Kerberos-Anmeldung.



Endbenutzerfehlermeldungen

In diesem Abschnitt finden Sie allgemeine Fehlermeldungen, die Benutzern auf der Windows-Anmeldeseite angezeigt werden.

Angezeigte Fehlermeldung	Beschreibung und Referenz
Ungültiger Benutzername oder Kennwort	Der Computer glaubt, dass Sie ein gültiges Zertifikat und einen gültigen privaten Schlüssel haben, aber der Kerberos-Domänencontroller hat die Verbindung zurückgewiesen. Weitere Informationen finden unter *Kerberos-Protokolle*.
Sie konnten nicht angemeldet werden. Ihre Anmeldeinformationen konnten nicht überprüft werden.	Es kann kein Kontakt zum Domänencontroller hergestellt werden oder auf dem Domänencontroller sind nicht die entsprechenden Zertifikate installiert.
Die Anforderung wird nicht unterstützt.	Registrieren Sie die Zertifikate "Domain Controller"und "Domain Controller Authentication"auf dem Domänencontroller neu, wie in CTX206156 beschrieben. Dies ist einen Versuch wert, selbst wenn die vorhandenen Zertifikate anscheinend gültig sind.
Sie konnten nicht angemeldet werden. Das für die Authentifizierung verwendete Smartcardzertifikat ist nicht vertrauenswürdig.	Die Zwischen- und Stammzertifikate sind nicht auf dem lokalen Computer installiert. Informationen zum Installieren von Smartcardzertifikaten auf nicht in Domänen eingebundenen Computern finden Sie unter CTX206156. Weitere Informationen finden Sie im Abschnitt *Zertifikate und Public Key-Infrastruktur* in diesem Artikel.
Sie können sich nicht anmelden, da die Smartcard-Anmeldung für Ihr Konto nicht unterstützt wird.	Ein Arbeitsgruppenbenutzerkonto wurde für die Smartcard-Anmeldung nicht vollständig konfiguriert.
Der angeforderte Schlüssel ist nicht vorhanden.	Ein Zertifikat verweist auf einen privaten Schlüssel, auf den nicht zugegriffen werden kann. Dieser Fall kann eintreten, wenn eine PIV-Karte nicht vollständig konfiguriert ist und die CHUID oder CCC-Datei fehlt.

Angezeigte Fehlermeldung	Beschreibung und Referenz
Fehler beim Verwenden der Smartcard	Die Smartcard-Middleware ist nicht ordnungsgemäß installiert. Smartcard-Installationsanweisungen finden Sie unter CTX206156.
Smartcard einlegen	Die Smartcard oder der Smartcardleser wurde nicht erkannt. Wenn die Smartcard eingelegt ist, weist diese Meldung auf ein Problem mit der Hardware oder Middleware hin. Smartcard-Installationsanweisungen finden Sie unter CTX206156.
Die PIN ist falsch.	Die Smartcard hat die vom Benutzer eingegebene PIN nicht akzeptiert.
Es wurde kein gültiges Smartcardzertifikat gefunden.	Die Erweiterungen des Zertifikats sind möglicherweise nicht richtig festgelegt worden oder der RSA-Schlüssel ist zu kurz. (<2048 Bits). Informationen zum Erstellen von gültigen Smartcardzertifikaten finden Sie unter CTX206901.
Die Smartcard ist blockiert.	Eine Smartcard wurde gesperrt, z. B. weil der Benutzer mehrmals eine falsche PIN eingegeben hat. Ein Administrator hat möglicherweise Zugriff auf den PIN-Entsperrcode (PUK) für die Smartcard und kann die PIN mit einem Tool zurücksetzen, das beim Smartcardhersteller erhältlich ist. Wenn der Entsperrcode nicht verfügbar ist oder die Sperrung nicht aufgehoben werden kann, muss die Smartcard auf die Werkseinstellungen zurückgesetzt werden.

Angezeigte Fehlermeldung	Beschreibung und Referenz
Ungültige Anforderung	Der private Schlüssel einer Smartcard unterstützt die Kryptografie nicht, die der Domänencontroller erfordert. Beispielsweise fordert der Domänencontroller möglicherweise die Entschlüsselung des privaten Schlüssels, aber die Smartcard unterstützt nur das Signieren. Dies weist meist darauf hin, dass die Erweiterungen des Zertifikats nicht ordnungsgemäß festgelegt sind oder dass der RSA-Schlüssel zu kurz ist. (<2048 Bits). Informationen zum Erstellen von gültigen Smartcardzertifikaten finden Sie unter CTX206901.

Verwandte Informationen

- Konfigurieren einer Domäne für die Smartcard-Anmeldung: https://support.citrix.com/article/CTX206156
- Smartcard-Anmelderichtlinien: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)?redirectedfrom=MSDN
- Aktivieren der CAPI-Protokollierung: https://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Aktivieren der Kerberos-Protokollierung: https://support.microsoft.com/en-us/kb/262177
- Richtlinien für die Aktivierung der Smartcard-Anmeldung mit Drittanbieter-Zertifizierungsstellen: https://support.microsoft.com/en-us/kb/281245

PowerShell-Cmdlets für den Verbundauthentifizierungsdienst

August 18, 2021

Die Verwaltungskonsole des Verbundauthentifizierungsdiensts eignet sich für einfache Bereitstellungen, während die PowerShell-Oberfläche erweiterte Optionen bietet. Wenn Sie Optionen verwenden möchten, die in der Konsole nicht verfügbar sind, empfiehlt Citrix, ausschließlich PowerShell für die Konfiguration zu verwenden.

Mit dem folgenden Befehl werden die FAS-PowerShell-Cmdlets hinzugefügt:


```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

In einem PowerShell-Fenster können Sie Get-Help <*cmdlet-name*> verwenden um die Cmdlet-Hilfe anzuzeigen.

Die unter dem Link unten verfügbare ZIP-Datei enthält Hilfedateien für alle Cmdlets des PowerShell SDKs für FAS. Klicken Sie auf den Link, um die ZIP-Datei herunterzuladen. Extrahieren Sie den Inhalt in einen lokalen Ordner. Die Datei index.html enthält eine Liste aller Cmdlets mit Links zu den individuellen Cmdlet-Hilfedateien.

Hilfedateien für PowerShell-Cmdlets für den Verbundauthentifizierungsdienst

Grafik

August 18, 2021

Citrix HDX umfasst vielfältige Technologien zur Grafikbeschleunigung und -codierung, die die Bereitstellung reichhaltiger Grafikanwendungen über XenApp und XenDesktop optimieren. Die Grafiktechnologien bieten bei der Remotearbeit mit grafikintensiven virtuellen Anwendungen die gleiche Benutzererfahrung wie ein physischer Desktop.

Sie können für das Grafikrendering Software oder Hardware verwenden. Softwarerendering erfordert eine Drittanbieter-Bibliothek ("Softwarerasterizer"). Windows enthält beispielsweise den WARP-Rasterizer für DirectX-basierte Grafiken. Unter Umständen wird ein anderer Softwarerenderer bevorzugt (z. B. OpenGL Software Accelerator). Hardwarerendering (Hardwarebeschleunigung) erfordert einen Grafikprozessor (GPU).

HDX bietet eine Standardcodierungskonfiguration, die für die häufigsten Anwendungsfälle optimiert ist. Über Citrix Richtlinien können IT-Administratoren grafikbezogene Einstellungen zur Erfüllung verschiedener Anforderungen und Bereitstellung der gewünschten Benutzererfahrung konfigurieren.

Thinwire

ThinWire ist die in XenApp und XenDesktop verwendete Standardtechnologie von Citrix für das Anzeigeremoting.

Per Anzeigeremoting können auf einer Maschine erzeugte Grafiken (normalerweise über ein Netzwerk) auf eine andere Maschine für die Anzeige übertragen werden. Grafiken werden als Ergebnis von Benutzereingaben, z. B. Tastenanschläge und Mausaktionen, erzeugt.

HDX 3D Pro

Mit der HDX 3D Pro-Funktion von XenApp und XenDesktop können Desktops und Anwendungen bereitgestellt werden, die mit einem Grafikprozessor (GPU) für die Hardwarebeschleunigung

am besten funktionieren. Dazu gehören professionelle, auf OpenGL und DirectX basierende 3D-Grafikanwendungen. Der Standard-VDA unterstützt die GPU-Beschleunigung nur für DirectX.

GPU-Beschleunigung für Windows-Desktopbetriebssysteme

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Desktopbetriebssystemmaschinen bereitstellen. HDX 3D Pro unterstützt physische Hostcomputer (einschließlich Desktop-, Blade- und Rack-Arbeitsstationen) und die Virtualisierungstechnologien der Hypervisors XenServer, vSphere und Hyper-V (nur Passthrough).

Mit GPU-Passthrough können Sie VMs mit exklusivem Zugriff auf dedizierte Hardware für die Grafikverarbeitung erstellen. Sie können mehrere GPUs auf dem Hypervisor installieren und VMs jeder dieser GPUs einzeln zuweisen.

Mit GPU-Virtualisierung können mehrere virtuelle Maschinen die Grafikverarbeitungsleistung eines einzelnen physischen GPU direkt nutzen.

GPU-Beschleunigung für Windows-Serverbetriebssysteme

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Windows-Serverbetriebssystemsitzungen ausgeführt werden, auf der GPU des Servers gerendert werden. Beim Verlagern der Wiedergabe von OpenGL, DirectX, Direct3D und Windows Presentation Foundation (WPF) auf den GPU des Servers wird die CPU des Servers nicht durch die Grafikwiedergabe verlangsamt. Außerdem kann der Server so mehr Grafiken verarbeiten, weil die Arbeitslast zwischen Prozessor und Grafikprozessor aufgeteilt wird.

Framehawk

Framehawk ist eine Technologie für das Anzeigeremoting für mobile Mitarbeiter mit drahtlosen Breitbandverbindungen (WiFi und 4G/LTE-Mobilfunknetze). Framehawk überwindet die Herausforderungen der spektralen Interferenz und des Mehrwegeempfangs und liefert eine flüssige, interaktive Benutzererfahrung für virtuelle Apps und Desktops.

OpenGL Software Accelerator

OpenGL Software Accelerator ist ein Softwarerasterizer für OpenGL-Anwendungen wie ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD und CAM. Manchmal bietet OpenGL Software Accelerator auch ohne die Verwendung einer Grafikkarte eine gute Benutzererfahrung mit OpenGL-Anwendungen.

Verwandte Informationen

- Thinwire
- HDX 3D Pro
- GPU-Beschleunigung für Windows-Desktopbetriebssysteme
- GPU-Beschleunigung für Windows-Serverbetriebssysteme
- Framehawk

- OpenGL Software Accelerator

Framehawk

August 15, 2023

Framehawk ist eine Technologie für das Anzeigeremoting für mobile Mitarbeiter mit drahtlosen Breitbandverbindungen (WiFi und 4G/LTE-Mobilfunknetze). Framehawk überwindet die Herausforderungen der spektralen Interferenz und des Mehrwegeempfangs und liefert eine flüssige, interaktive Benutzererfahrung für virtuelle Apps und Desktops. Framehawk kann in Langstrecken-Breitbandnetzwerken mit hoher Latenz eingesetzt werden, bei denen geringfügige Paketverluste die Benutzererfahrung verschlechtern können. Citrix empfiehlt die Verwendung des adaptiven Transports für diesen Anwendungsfall. Weitere Informationen finden Sie unter Adaptiver Transport.

Sie können Framehawk mit Citrix Richtlinienvorlagen für Benutzergruppen und Zugriffsszenarios in einer für Ihr Unternehmen geeigneten Weise implementieren. Framehawk ist für mobile Einzelbildschirm-Anwendungsfälle (Laptops, Tablets usw.) vorgesehen. Verwenden Sie Framehawk, wenn der geschäftliche Wert einer Echtzeit-Interaktivität die Kosten zusätzlicher Serverressourcen und das Erfordernis einer Breitbandverbindung rechtfertigt.

Wirkungsweise von Framehawk

Bei der Betrachtung des Inhalts des Framepuffers und der Unterscheidung verschiedener Inhaltsarten auf dem Bildschirm wirkt Framehawk wie das menschliche Auge. Was ist dem Benutzer wichtig? In Bildschirmbereichen mit schnellen Änderungen (Video, Animationen etc.) spielt es für das menschliche Auge keine Rolle, wenn einige Pixel verloren gehen, da sie schnell durch neue Daten überschrieben werden.

Bei statischen Bereichen, z. B. Symbolleisten oder Text kurz nach Ausführen eines Bildlaufs, den der Benutzer direkt lesen möchte, ist das menschliche Auge sehr anspruchsvoll. Diese Bereiche müssen pixelgenau sein. Im Gegensatz zu Protokollen, bei denen die technische Präzision im Sinne von **Nullen und Einsen** im Vordergrund steht, ist Framehawk stärker auf die menschlichen Nutzer von Technik ausgelegt.

Framehawk umfasst einen völlig neuen QoS-Signalverstärker sowie eine zeitabhängige Heatmap zur exakteren und effizienten Arbeitslasterkennung. Zusätzlich zur Datenkomprimierung werden in Framehawk autonome, selbstkorrigierende Transformationen verwendet, die erneute Übertragung von Daten wird zur Gewährleistung von Klickantwort, Linearität und konsistenter Kadenz vermieden. In einem verlustreichen Netzwerk kann Framehawk Verluste durch Interpolation ausgleichen, sodass der Benutzer die Bildqualität weiterhin als gut empfindet und die Benutzererfahrung sogar flüssiger

wird. Darüber hinaus unterscheiden die Algorithmen von Framehawk zwischen verschiedenen Paketverlusttypen. Etwa den regellosen Verlust (weitere Daten zur Kompensierung senden) und den Verlust durch Engpässe (keine weiteren Daten senden, da der Kanal bereits blockiert ist).

Die Framehawk Intent Engine in Citrix Receiver unterscheidet Bildlauf nach oben oder unten, Vergrößern, Verschieben nach links oder rechts, Lesen, Eingeben und weitere übliche Aktionen. Die Engine steuert zudem die Antwort an den Virtual Delivery Agent (VDA) mit einem gemeinsamen Wörterbuch. Wenn der Benutzer lesen möchte, muss die visuelle Qualität des Texts hervorragend sein. Führt er einen Bildlauf durch, muss dieser schnell und gleichmäßig sein. Er muss außerdem unterbrochen werden können, damit der Benutzer die Interaktion mit der Anwendung oder dem Desktop jederzeit unter Kontrolle hat.

Durch die Messung der Kadenz der Netzwerkverbindung (**Gearing**, analog zur Spannung einer Fahrradkette) reagiert die Framehawk-Logik schneller und bei Verbindungen mit hoher Latenz wird eine bessere Benutzererfahrung ermöglicht. Dieses einzigartige, patentierte Verfahren liefert kontinuierlich aktuelle Rückmeldungen zu Netzwerkbedingungen, sodass Framehawk auf Änderungen bei Bandbreite, Latenz und Verlust sofort reagieren kann.

Thinwire und Framehawk –Überlegungen zur Auslegung

ThinWire ist branchenweit erste Wahl in puncto Bandbreiteneffizienz und eignet sich gut für viele Zugriffsszenarien und Netzwerkbedingungen. Allerdings wird zur Gewährleistung einer zuverlässigen Datenkommunikation bei ThinWire TCP verwendet. Aus diesem Grund ist in verlustreichen oder überlasteten Netzwerken eine Paketneuübertragung erforderlich, was zu Verzögerungen beim Endbenutzer führt. ThinWire steht über eine neue Enlightened Data Transport-Ebene zur Verfügung, die die Probleme von TCP bei Netzwerkverbindungen mit hoher Latenz ausräumen soll.

In Framehawk wird eine auf UDP (User Datagram Protocol) aufbauende Datentransportschicht verwendet. UDP hat einen kleinen Anteil an der Überwindung von Paketverlusten bei Framehawk im Vergleich mit dessen Leistung mit anderen UDP-basierten Protokollen. UDP bildet eine wichtige Grundlage für die menschenorientierte Technik, die Framehawk von anderen Lösungen abhebt.

Wie viel Bandbreite benötigt Framehawk?

Die Bezeichnung Breitband-WLAN hängt von verschiedenen Faktoren ab, etwa der Zahl der Benutzer, die eine Verbindung teilen, der Qualität der Verbindung und der verwendeten Apps. Zur Erzielung einer optimalen Leistung empfiehlt Citrix einen Grundwert von 4 oder 5 MBit/s plus ca. 150 KBit/s pro gleichzeitig verbundenem Benutzer.

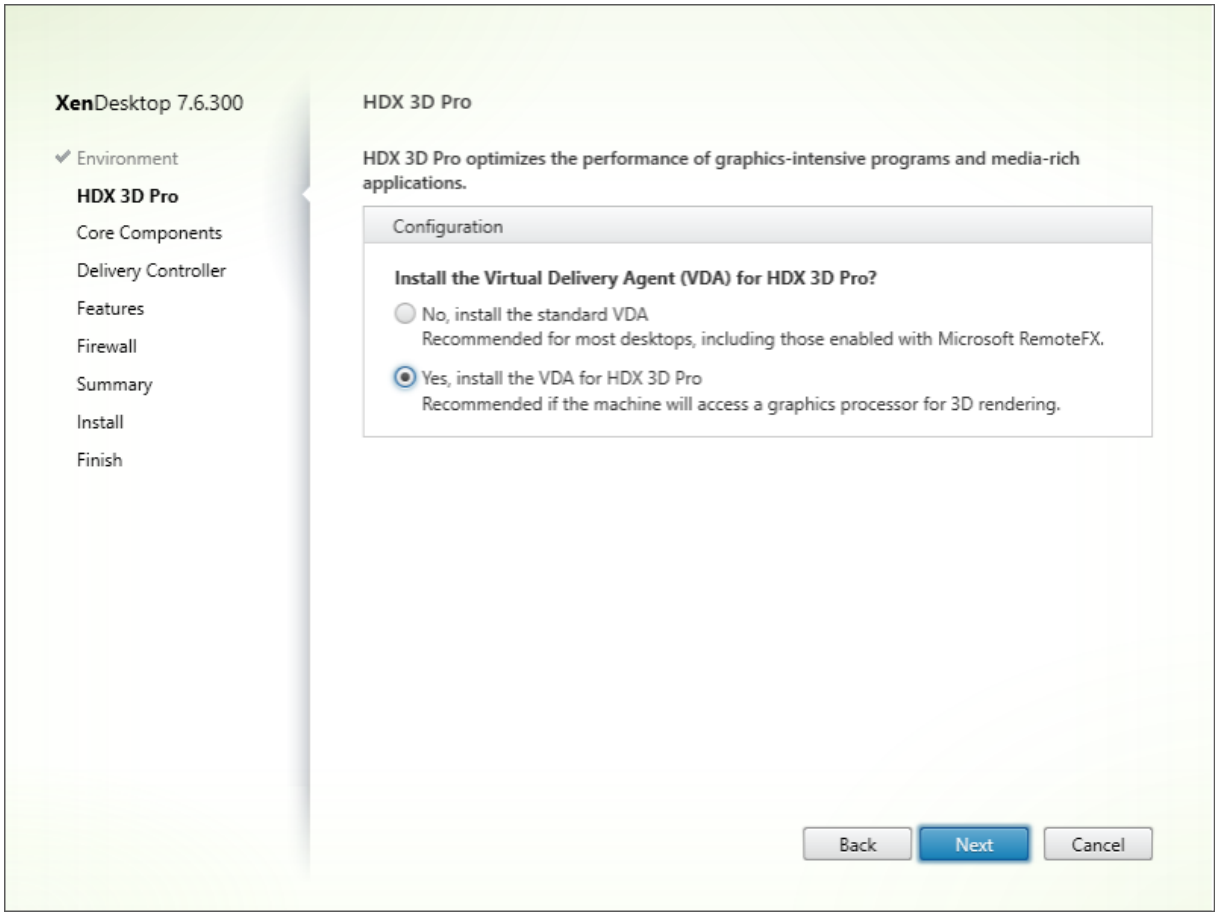
Für Thinwire wird generell eine Bandbreite von 1,5 MBit/s plus 150 KBit/s pro Benutzer empfohlen. Details siehe Blog zu XenApp- und XenDesktop-Bandbreite. Bei einem Paketverlust von 3 % benötigt Thinwire viel mehr Bandbreite als Framehawk, um eine gute Benutzererfahrung zu gewährleisten.

Thinwire ist weiterhin der Primärkanal für das Anzeigen-Remoting des ICA-Protokolls. Framehawk ist standardmäßig deaktiviert. Citrix empfiehlt die selektive Aktivierung für spezifische Breitband-WLAN-Szenarios in Ihrer Organisation. Denken Sie daran, dass Framehawk erheblich mehr Serverressourcen (CPU und Speicher) erfordert als Thinwire.

Framehawk und HDX 3D Pro

Framehawk unterstützt alle Anwendungsfälle von HDX 3D Pro für XenApp-Apps (Serverbetriebssystem) und XenDesktop-Apps (Desktopbetriebssystem). Es wurde in Kundenumgebungen bei Latenzen von 400–500 ms und Paketverlusten von 1–2 % validiert. Bei gebräuchlichen Anwendungen zur 3D-Modellierung (z. B. AutoCAD, Siemens NX) wird eine gute Interaktivität erzielt. Diese Unterstützung ermöglicht nun auch die Anzeige von und Arbeit an großen CAD-Modellen im mobilen Einsatz oder an entfernten Standorten mit schlechten Netzwerkverbindungen. (Organisationen, die 3D-Anwendungen über Langstrecken-Netzwerkverbindungen bereitstellen müssen, sollten den adaptiven Transport verwenden. Weitere Informationen finden Sie unter Adaptiver Transport.)

Zur Aktivierung dieser Funktion ist keine gesonderte Konfiguration erforderlich. Beim Installieren des VDAs wählen Sie die 3DPro-Option zu Beginn der Installation aus:



Mit dieser Auswahl wird von HDX der Videotreiber des GPU-Herstellers anstelle des Citrix Videotreibers verwendet. Standardmäßig wird dann eine Vollbild-H.264-Codierung über ThinWire anstatt der normalerweise verwendeten Standardeinstellung (adaptive Anzeige mit selektiver H.264-Codierung) verwendet.

Anforderungen und Überlegungen

Framehawk erfordert mindestens VDA 7.6.300 und Gruppenrichtlinienverwaltung 7.6.300.

Auf dem Endpunkt muss mindestens Citrix Receiver für Windows 4.3.100 oder Citrix Receiver für iOS 6.0.1 ausgeführt werden.

Standardmäßig verwendet Framehawk einen Bereich bidirektionaler UDP-Ports (3224–3324) zum Austausch von Framehawk-Anzeigekanaldaten mit Citrix Receiver. Dieser Bereich kann über die Richtlinieneinstellung **Portbereich für Framehawk-Anzeigekanal** angepasst werden. Jede einzelne Verbindung zwischen dem Client und dem virtuellen Desktop erfordert einen eigenen Port. Definieren Sie in Betriebssystemumgebungen mit mehreren Benutzern (z. B. XenApp-Server) ausreichend Ports für die maximale Zahl gleichzeitiger Benutzersitzungen. Bei Einzelbenutzer-Betriebssystemen wie etwa VDI-Desktops reicht ein UDP-Port. Framehawk versucht die Verwendung der Ports beginnend vom ersten bis zum letzten im angegebenen Bereich. Dies gilt sowohl für Verbindungen über NetScaler Gateway als auch für direkte interne Verbindungen mit dem StoreFront-Server.

Für den Remotezugriff muss NetScaler Gateway bereitgestellt sein. Standardmäßig verwendet NetScaler UDP-Port 443 für die verschlüsselte Kommunikation zwischen Citrix Receiver auf dem Client und dem Gateway. Dieser Port muss in allen externen Firewalls geöffnet sein, damit eine sichere Kommunikation in beide Richtungen möglich ist. Das Feature wird als "Datagram Transport Security"(DTLS) bezeichnet.

> **Hinweis:**
>
> Framehawk-/DTLS-Verbindungen werden auf FIPS-Geräten nicht unterstützt.

Verschlüsselte Framehawk-Verbindungen werden unter NetScaler Gateway ab Version 11.0.62 und unter NetScaler Unified Gateway ab Version 11.0.64.34 unterstützt.

NetScaler mit hoher Verfügbarkeit wird von XenApp und XenDesktop 7.12 unterstützt.

Bei der Implementierung von Framehawk empfehlen sich folgende bewährte Methoden:

- Vergewissern Sie sich beim Sicherheitsadministrator, dass die für Framehawk definierten UDP-Ports in der Firewall geöffnet sind. Die Firewall wird bei der Installation nicht automatisch konfiguriert.
- Oft ist NetScaler Gateway in der DMZ umgeben von einer externen und einer internen Firewall installiert. UDP-Port 443 muss in der externen Firewall geöffnet sein. Wenn die Standardportbere-

iche verwendet werden, muss der UDP-Portbereich 3224–3324 in der internen Firewall geöffnet sein.

Konfiguration

> **Achtung:**
>
> Citrix empfiehlt, Framehawk nur für Benutzer zu aktivieren, bei denen ein hoher Paketverlust wahrscheinlich ist. Citrix empfiehlt außerdem, Framehawk nicht als universelle Richtlinie für alle Objekte der Site zu aktivieren.

Framehawk ist standardmäßig deaktiviert. Wenn das Feature aktiviert ist, versucht der Server, Framehawk für die Grafiken und Eingaben der Benutzer zu verwenden. Sind die Voraussetzungen nicht erfüllt, wird die Verbindung im Standardmodus (Thinwire) hergestellt.

Die folgenden Richtlinieneinstellungen wirken sich auf Framehawk aus:

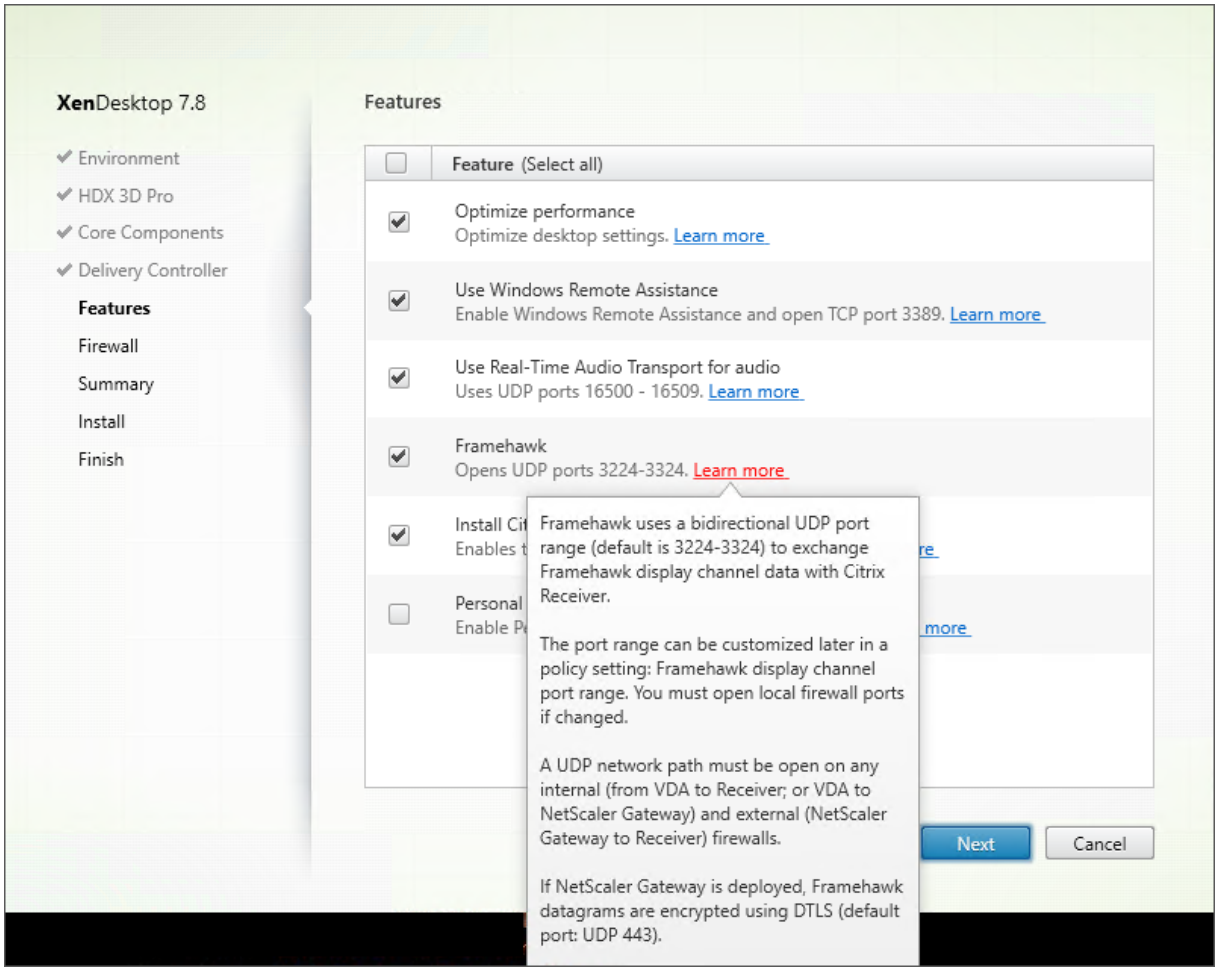
- Framehawk-Anzeigekanal: aktiviert oder deaktiviert das Feature.
- Portbereich für Framehawk-Anzeigekanal: Bereich der UDP-Portnummern (niedrigste bis höchste Portnummer), die der VDA für den Austausch von Framehawk-Anzeigekanaldaten mit dem Benutzergerät verwendet. Der VDA versucht die Verwendung eines Ports, beginnend bei dem Port mit der niedrigsten Nummer und geht dann ggf. zu dem Port mit der nächsthöheren Nummer über. Über den Port erfolgen eingehende und ausgehende Datenübertragungen.

Öffnen von Ports für den Framehawk-Anzeigekanal

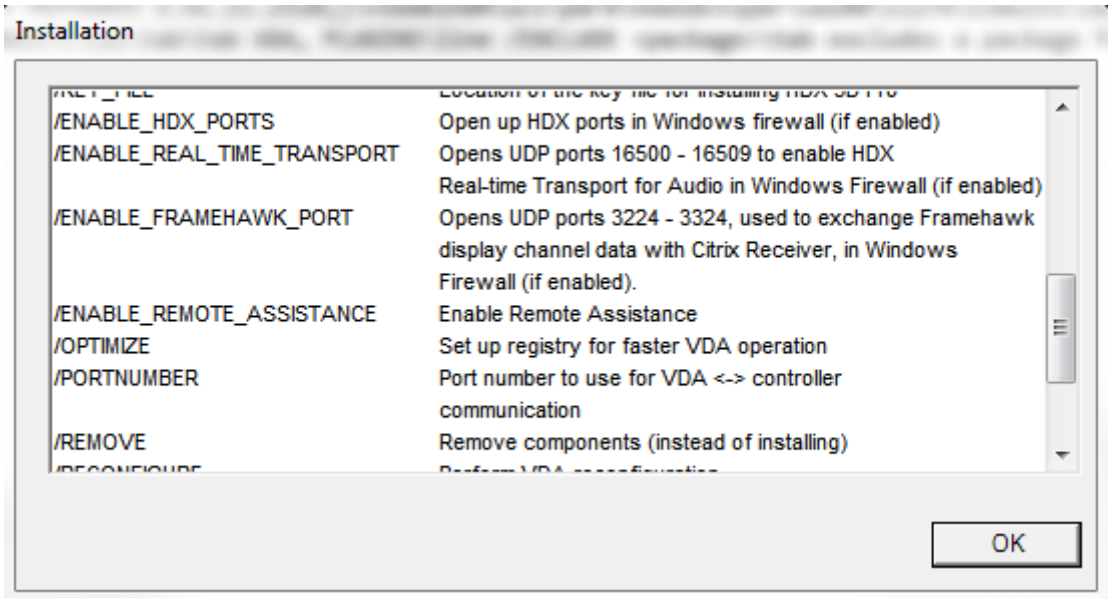
In XenApp und XenDesktop 7.8 gibt es eine Option zum Umkonfigurieren der Firewall im Schritt **Features** des VDA-Installationsprogramms. Über das zugehörige Kontrollkästchen werden die UDP-Ports 3224–3324 in der Windows-Firewall geöffnet. In folgenden Fällen ist eine manuelle Firewallkonfiguration erforderlich:

- Es handelt sich um eine Netzwerkfirewall.
  oder
- Der Standardportbereich wurde angepasst.

Zum Öffnen der UDP-Ports aktivieren Sie das Kontrollkästchen **Framehawk**:

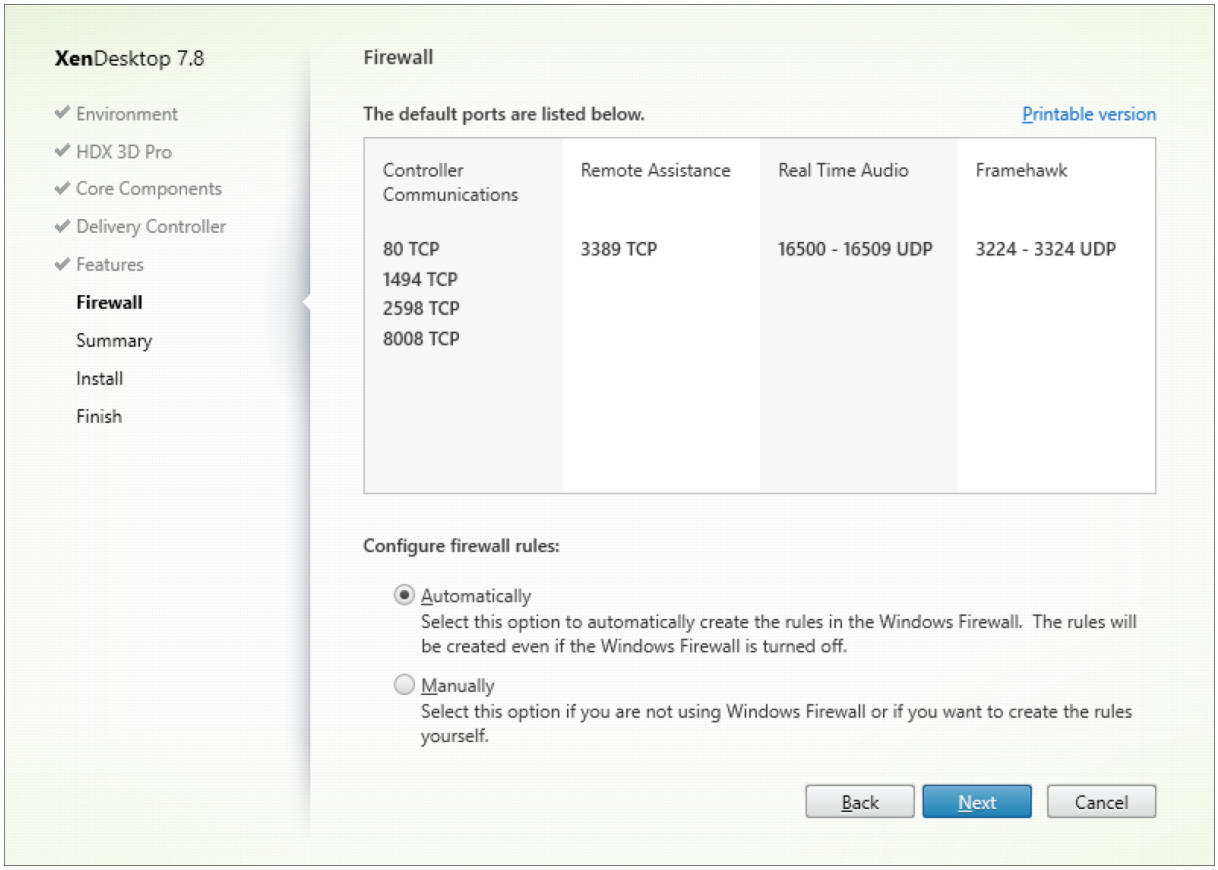


Sie können die UDP-Ports für Framehawk auch über die Befehlszeile mit **/ENABLE_FRAMEHAWK_PORT** öffnen:

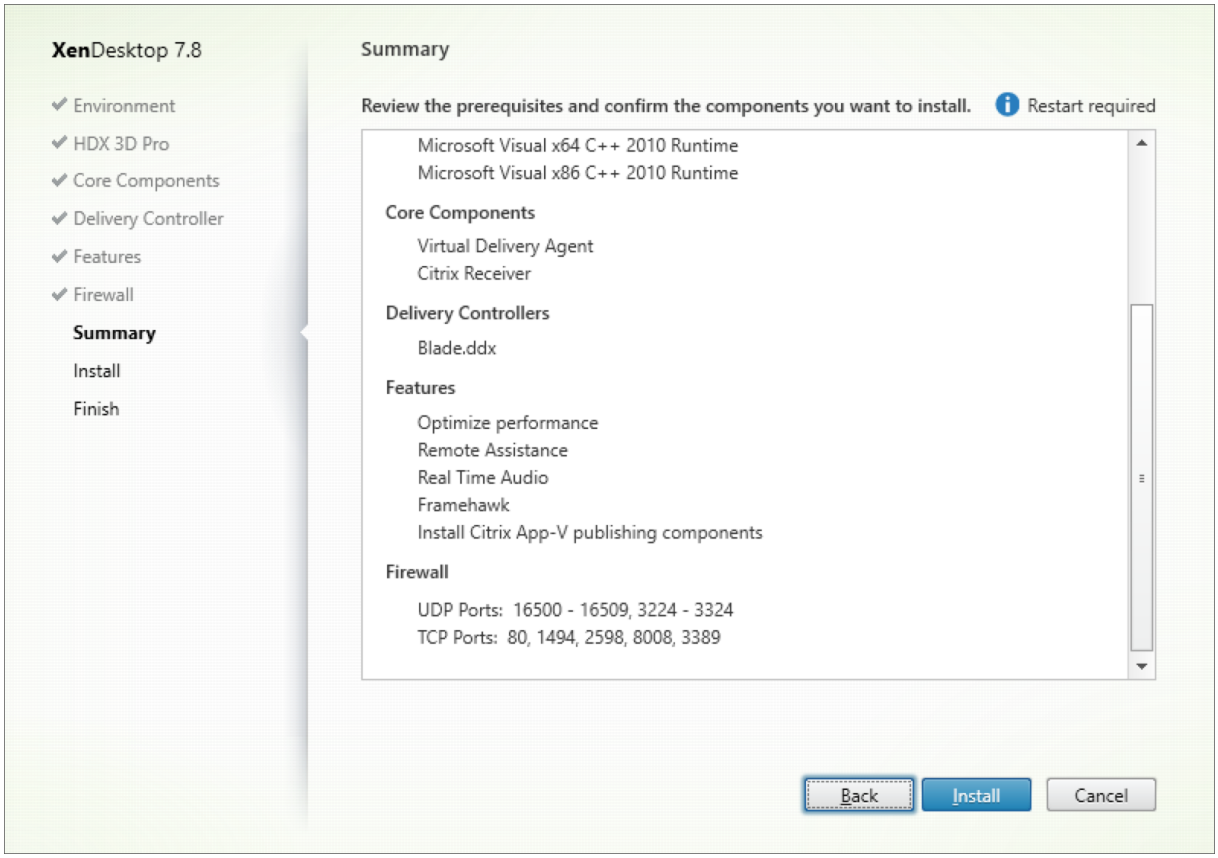


Überprüfen der UDP-Portzuweisungen für Framehawk

Während der Installation können Sie die Framehawk zugewiesenen UDP-Ports im Bildschirm **Firewall** überprüfen:



Auf der Registerkarte **Zusammenfassung** wird angezeigt, ob Framehawk aktiviert ist:



NetScaler Gateway-Unterstützung für Framehawk

Verschlüsselter Framehawk-Datenverkehr wird unter NetScaler Gateway ab Version 11.0.62.10 und unter NetScaler Unified Gateway ab Version 11.0.64.34 unterstützt.

- NetScaler Gateway bezieht sich auf eine Bereitstellungsarchitektur, in der der virtuelle Gateway-VPN-Server direkt für das Gerät des Endbenutzers zugänglich ist. Das bedeutet, dass der virtuelle VPN-Server eine öffentliche IP-Adresse hat und der Benutzer direkt eine Verbindung mit dieser IP-Adresse herstellt.
- NetScaler Unified Gateway bezieht sich auf eine Bereitstellung, in der der virtuelle Gateway-VPN-Server als Ziel an den virtuellen Content Switching-Server (CS) gebunden ist. In einer solchen Bereitstellung hat der virtuelle CS-Server die öffentliche IP-Adresse und der virtuelle Gateway-VPN-Server eine Pseudo-IP-Adresse.

Zum Aktivieren der Framehawk-Unterstützung unter NetScaler Gateway muss der DTLS-Parameter auf der Ebene des virtuellen Gateway-VPN-Servers aktiviert sein. Wenn der Parameter aktiviert ist und die Komponenten in XenApp bzw. XenDesktop ordnungsgemäß aktualisiert wurden, wird der Audio-, Video- und Interaktionsdatenverkehr von Framehawk zwischen dem virtuellen Gateway-VPN–Server und dem Benutzergerät verschlüsselt.

NetScaler Gateway, Unified Gateway und NetScaler Gateway + Global Server Load Balancing werden mit Framehawk unterstützt.

Folgendes wird mit Framehawk nicht unterstützt:

- HDX Insight
- NetScaler Gateway im IPv6-Modus
- NetScaler Gateway-Double-Hop
- NetScaler Gateway im Cluster

Szenario	Unterstützung für Framehawk
NetScaler Gateway	Ja
NetScaler und Global Server Load Balancing	Ja
NetScaler mit Unified Gateway	Ja. **Hinweis:** Unified Gateway wird ab Version 11.0.64.34 unterstützt.
HDX Insight	Nein
NetScaler Gateway im IPv6-Modus	Nein
NetScaler Gateway-Double-Hop	Nein
Mehrere Secure Ticket Authoritys für NetScaler Gateway	Ja
NetScaler Gateway mit hoher Verfügbarkeit	Ja
NetScaler Gateway und Clustereinrichtung	Nein

Konfigurieren der NetScaler-Unterstützung für Framehawk

Zum Aktivieren der Framehawk-Unterstützung unter NetScaler Gateway aktivieren Sie den DTLS-Parameter auf der Ebene des virtuellen Gateway-VPN-Servers. Wenn der Parameter aktiviert ist und die Komponenten in XenApp bzw. XenDesktop ordnungsgemäß aktualisiert wurden, wird der Audio-, Video- und Interaktionsdatenverkehr von Framehawk zwischen dem virtuellen Gateway-VPN–Server und dem Benutzergerät verschlüsselt.

Diese Konfiguration ist erforderlich, wenn Sie die UDP-Verschlüsselung unter NetScaler Gateway für den Remotezugriff aktivieren.

NetScaler-Unterstützung für Framehawk erfordert Folgendes:

- UDP-Port 443 muss in der externen Firewall geöffnet sein.
- CGP-Standardport 2598 muss in der externen Firewall geöffnet sein.
- DTLS muss in den Einstellungen des virtuellen VPN-Servers aktiviert sein.

- Lösen Sie die Bindung des SSL-Zertifikatschlüsselpaars und binden Sie es erneut. Dies ist nicht erforderlich, wenn Sie NetScaler ab Version 11.0.64.34 verwenden.

Konfigurieren der NetScaler Gateway-Unterstützung für Framehawk

1. Stellen Sie NetScaler Gateway bereit und konfigurieren Sie es für die Kommunikation mit StoreFront und zur Authentifizierung der Benutzer von XenApp und XenDesktop.
2. Erweitern Sie auf der Registerkarte "Configuration"von NetScaler die Option "NetScaler Gateway"und wählen Sie **Virtual Servers**.
3. Klicken Sie auf **Edit**, um die Grundeinstellungen des virtuellen VPN-Servers anzuzeigen und prüfen Sie die DTLS-Einstellung.
4. Klicken Sie auf **More**, um weitere Konfigurationsoptionen aufzurufen:
5. Wählen Sie **DTLS**, um die Sicherheit für Datagramm-Protokolle wie Framehawk zu aktivieren. Klicken Sie auf **OK**. Der Bereich "Basic Settings"für den virtuellen VPN-Server zeigt, dass das DTLS-Flag auf **True** festgelegt ist.
6. Öffnen Sie den Bildschirm "Server Certificate Binding"neu und klicken Sie auf **+**, um das Zertifikatschlüsselpaar zu binden.
7. Wählen Sie das Zertifikatschlüsselpaar (siehe oben) und klicken Sie auf **Select**.
8. Speichern Sie die Änderungen an der Serverzertifikatbindung.
9. Nach dem Speichern wird das Zertifikatschlüsselpaar angezeigt. Klicken Sie auf **Bind**.
10. Ignorieren Sie Meldung **No usable ciphers configured on the SSL vserver/service**, sofern sie angezeigt wird.

Schritte bei älteren NetScaler Gateway-Versionen

Wenn Sie eine ältere Version als NetScaler Gateway 11.0.64.34 verwenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Bildschirm "Server Certificate Binding"neu und klicken Sie auf +, um das Zertifikatschlüsselpaar zu binden.
2. Wählen Sie das Zertifikatschlüsselpaar (siehe oben) und klicken Sie auf **Select**.
3. Speichern Sie die Änderungen an der Serverzertifikatbindung.
4. Nach dem Speichern wird das Zertifikatschlüsselpaar angezeigt. Klicken Sie auf **Bind**.
5. Ignorieren Sie Meldung **No usable ciphers configured on the SSL vserver/service**, sofern sie angezeigt wird.

Konfigurieren der Unified Gateway-Unterstützung für Framehawk

1. Vergewissern Sie sich, dass Unified Gateway installiert und richtig konfiguriert ist. Weitere Informationen finden Sie auf der Website mit der Citrix Produktdokumentation unter Unified Gateway.

2. Aktivieren Sie DTLS im virtuellen VPN-Server, der an den *virtuellen CS-Server* als *virtueller Zielserver* gebunden ist.

Einschränkungen

Wenn veraltete DNS-Einträge für den virtuellen NetScaler Gateway-Server, auf einem Clientgerät vorliegen, erfolgt für den adaptiven Transport und Framehawk möglicherweise ein Fallback auf TCP anstelle von UDP. Bei einem Fallback auf TCP leeren Sie als Workaround den DNS-Cache auf dem Client und stellen Sie wieder eine Verbindung her, um die Sitzung mit UDP zu starten.

Unterstützung für andere VPN-Produkte

NetScaler Gateway ist das einzige SSL VPN-Produkt, das die von Framehawk benötigte UDP-Verschlüsselung unterstützt. Wenn ein anderes SSL-VPN oder eine falsche Version von NetScaler Gateway verwendet wird, wird die Framehawk-Richtlinie möglicherweise nicht angewendet. Konventionelle IPsec-VPN-Produkte unterstützen Framehawk, ohne dass eine Modifizierung erforderlich ist.

Konfigurieren von Citrix Receiver für iOS zur Framehawk-Unterstützung

Zum Konfigurieren älterer Versionen von Citrix Receiver für iOS zur Framehawk-Unterstützung müssen Sie die Datei default.ica manuell bearbeiten.

1. Öffnen Sie auf dem StoreFront-Server das App_Data-Verzeichnis im Pfad c:\inetpub\wwwroot\.
2. Öffnen Sie die Datei default.ica und fügen Sie im Abschnitt "WFClient"die Zeile "Framehawk=On"hinzu.
3. Speichern Sie die Änderung.

Damit können Framehawk-Sitzungen von kompatiblen Citrix Receiver-Instanzen auf iOS-Geräten hergestellt werden. Dieser Schritt ist nicht erforderlich, wenn Sie Citrix Receiver für Windows verwenden.

> **Hinweis:**
>
> Ab Citrix Receiver für iOS 7.0 müssen Sie der Datei default.ica den Parameter **Framehawk=On** nicht explizit hinzufügen.

Überwachen von Framehawk

Sie können die Verwendung und Leistung von Framehawk über Citrix Director überwachen. Die Detailansicht für den virtuellen HDX-Kanal enthält nützliche Informationen zur Überwachung und Prob-

lembehandlung von Framehawk in jeder Sitzung. Zum Anzeigen von Zahlen für Framehawk wählen Sie **Grafiken - Framehawk**.

Wenn die Framehawk-Verbindung steht, wird auf der Detailseite **Anbieter = VD3D** und **Verbunden = True** angezeigt. Der Status "Im Leerlauf"des virtuellen Kanals ist normal, da er den Signalkanal überwacht, der nur beim ersten Handshake verwendet wird. Die Seite bietet auch andere nützliche Statistiken zu der Verbindung.

Wenn Probleme auftreten, besuchen Sie den Blog Framehawk troubleshooting.

HDX 3D Pro

August 18, 2021

Mit der HDX 3D Pro-Funktion von XenApp und XenDesktop können Desktops und Anwendungen bereitgestellt werden, die mit einem Grafikprozessor (GPU) für die Hardwarebeschleunigung am besten funktionieren. Dazu gehören professionelle, auf OpenGL und DirectX basierende 3D-Grafikanwendungen. Der Standard-VDA unterstützt die GPU-Beschleunigung nur für DirectX. Weitere Informationen zur Auswahl von Standard- oder HDX 3D Pro-VDA finden Sie unter "Schritt 5. Auswählen, ob HDX 3D Pro verwendet werden soll"im Artikel Installieren von VDAs.

Alle unterstützten Citrix Receiver-Versionen können mit 3D-Grafiken verwendet werden. Zur Erzielung der optimalen Leistung in Umgebungen mit komplexen 3D-Anwendungen, hochauflösenden Monitoren, Multimonitorkonfigurationen und Anwendungen mit hohen Framerates empfiehlt Citrix die Verwendung der aktuellen Version von Citrix Receiver für Windows bzw. Citrix Receiver für Linux. Informationen zu den unterstützten Versionen von Citrix Receiver finden Sie unter Lifecycle Milestones for Citrix Receiver.

Beispiele für professionelle 3D-Anwendungen:

- CAD-, CAM- und CAE-Anwendungen
- Geografische Informationssystemsoftware (GIS)
- Bildarchivierungskommunikationssystem (PACS) für bildgebende Diagnostik
- Anwendungen, die die aktuellen Versionen von OpenGL, DirectX, NVIDIA, CUDA, OpenCL und WebGL verwenden
- Rechenintensive Nichtgrafik-Anwendungen, die NVIDIA CUDA-GPUs (Compute Unified Device Architecture) für paralleles Computing verwenden

HDX 3D Pro bietet die beste bandbreitenunabhängige Benutzererfahrung:

- WAN-Verbindungen: Bieten Sie eine interaktive Benutzererfahrung über WAN-Verbindungen mit geringen Bandbreiten bis zu 1,5 MBit/s.

- LAN-Verbindungen: Bieten Sie eine Benutzererfahrung wie bei einem lokalen Desktop bei LAN-Verbindungen.

  Sie können komplexe und teure Arbeitsstationen durch einfache Benutzergeräte ersetzen, da die Grafikverarbeitung in das Datencenter für eine zentralisierte Verwaltung verschoben wird.

HDX 3D Pro stellt Windows-Desktopbetriebssystemmaschinen und Windows-Serverbetriebssystemmaschinen die GPU-Beschleunigung bereit. Weitere Informationen finden Sie unter GPU-Beschleunigung für Windows-Desktopbetriebssysteme sowie GPU-Beschleunigung für Windows-Serverbetriebssysteme.

HDX 3D Pro ist mit GPU-Passthrough und der GPU-Virtualisierung folgender Hypervisors und in Bare-Metal-Umgebungen kompatibel:

- Citrix XenServer
  - GPU-Passthrough mit NVIDIA GRID und Intel GVT-d
  - GPU-Virtualisierung mit NVIDIA GRID und Intel GVT-g
- Microsoft Hyper-V
  - GPU-Passthrough (Discrete Device Assignment) mit NVIDIA GRID und AMD
- VMware vSphere
  - GPU-Passthrough (vDGA) mit NVIDIA GRID, Intel und AMD IOMMU
  - GPU-Virtualisierung mit NVIDIA GRID und AMD MxGPU

Informationen zu den unterstützten XenServer-Versionen finden Sie unter Citrix XenServer Hardware Compatibility List.

Mit dem HDX Monitor können Sie den Betrieb und die Konfiguration von HDX-Visualisierungstechnologien überprüfen und HDX-Probleme diagnostizieren und beheben. Das Tool und weitere Informationen stehen unter https://taas.citrix.com/hdx/download/ zur Verfügung.

GPU-Beschleunigung für Windows-Serverbetriebssysteme

August 18, 2021

Mit HDX 3D Pro können grafikintensive Anwendungen, die in Windows-Serverbetriebssystemsitzungen ausgeführt werden, auf der GPU des Servers wiedergegeben werden. Beim Verlagern der Wiedergabe von OpenGL, DirectX, Direct3D und Windows Presentation Foundation (WPF) auf den GPU des Servers wird die CPU des Servers nicht durch die Grafikwiedergabe verlangsamt. Zusätzlich kann der Server so mehr Grafiken verarbeiten, weil die Arbeitslast zwischen Prozessor und Grafikprozessor aufgeteilt wird.

Da Windows Server ein Mehrbenutzer-Betriebssystem ist, kann ein von XenApp verwendeter GPU ohne GPU-Virtualisierung (vGPU) von mehreren Benutzern verwendet werden.

Vorsicht beim Bearbeiten der Registrierung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

GPU Sharing

GPU Sharing ermöglicht die GPU-Hardwarewiedergabe von OpenGL- und DirectX-Anwendungen in Remotedesktopsitzungen und hat die folgenden Merkmale:

- Verwenden auf Bare-Metal- oder virtuellen Maschinen, um die Anwendungsskalierbarkeit und -leistung zu steigern.
- Mehrere gleichzeitige Sitzungen können GPU-Ressourcen gemeinsam verwenden. (Die meisten Benutzer benötigen nicht die Wiedergabeleistung eines dedizierten GPU).
- Erfordert keine besonderen Einstellungen.

Sie können mehrere GPUs auf einem Hypervisor installieren und jedem GPU eine VM zuordnen: entweder durch Installation einer Grafikkarte mit mehreren GPUs oder durch Installation mehrerer Grafikkarten mit einem oder mehreren GPUs. Eine Mischung heterogener Grafikkarten auf einem Server wird nicht empfohlen.

Virtuelle Maschinen benötigen einen direkten Passthrough-Zugriff auf einen GPU; dies ist bei Citrix XenServer, VMware vSphere vDGA und Intel GVT-d möglich. Wenn HDX 3D Pro mit GPU-Passthrough verwendet wird, unterstützt jeder GPU des Servers eine virtuelle Maschine mit mehreren Benutzern.

GPU Sharing hängt nicht von einer bestimmten Grafikkarte ab.

- Wählen Sie bei Ausführung auf einem Hypervisor eine Hardwareplattform und Grafikkarten aus, die mit der Implementierung von GPU-Passthrough des Hypervisors kompatibel sind. Die Liste der Hardware, die Zertifizierungstests mit XenServer GPU-Passthrough bestanden hat, finden Sie unter GPU-Passthroughgeräte.
- Bei Ausführung auf Bare-Metal sollte eine Grafikkarte vom Betriebssystem aktiviert sein. Wenn mehrere GPUs auf der Hardware installiert sind, deaktivieren Sie mit dem Device Manager alle außer einem.

Die Skalierbarkeit mit GPU Sharing hängt von folgenden Faktoren ab:

- Ausgeführte Anwendungen

- Verbrauchter Videospeicher
- Verarbeitungsleistung der Grafikkarte

Einige Anwendungen handhaben fehlenden Videospeicher besser als andere. Wenn die Hardware stark überlastet wird, kann der Grafikkartentreiber instabil werden oder abstürzen. Schränken Sie die Anzahl der gleichzeitigen Benutzer ein, um diese Probleme zu vermeiden.

Sie können die GPU-Beschleunigung mit einem Tool von Drittanbietern bestätigen, z. B. GPU-Z. GPU-Z ist hier verfügbar: https://www.techpowerup.com/gpuz/.

Wiedergabe von DirectX, Direct3D und WPF

Die Wiedergabe von DirectX, Direct3D und WPF steht nur auf Servern zur Verfügung, die einen Grafikprozessor haben, der eine Anzeigetreiberschnittstelle (DDI) der Version 9ex, 10 oder 11 unterstützt.

- Unter Windows Server 2008 R2 sind für DirectX und Direct3D keine Sondereinstellungen erforderlich, um einen einzelnen GPU zu verwenden.
- Unter Windows Server 2016 und Windows Server 2012 verwenden Remotedesktopdienste-Sitzungen auf dem RD-Sitzungshostserver als Standardadapter Microsoft Basic Render Driver. Um den GPU in RDS-Sitzungen unter Windows Server 2012 zu verwenden, aktivieren Sie die Einstellung Use the hardware default graphics adapter for all Remote Desktop Services sessions in der Gruppenrichtlinie Lokale Computerrichtlinie > Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung.
- Um die Wiedergabe von WPF-Anwendungen mit der GPU des Servers zu aktivieren, müssen Sie in der Registrierung des Servers, der die Windows-Serverbetriebssystemsitzungen ausführt, die folgenden Einstellungen erstellen:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] “EnableWPFHook”=dword:00000001

GPU-Beschleunigung für CUDA- oder OpenCL-Anwendungen

Die GPU-Beschleunigung von CUDA- und OpenCL-Anwendungen, die in einer Benutzersitzung ausgeführt werden, ist standardmäßig deaktiviert.

Aktivieren Sie die folgenden Registrierungseinstellungen, um die im Rahmen der Machbarkeitsstudie verfügbaren CUDA-Beschleunigungsfeatures zu verwenden:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA" =dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "CUDA"=dword:00000001

Aktivieren Sie die folgenden Registrierungseinstellungen, um die im Rahmen der Machbarkeitsstudie verfügbaren OpenCL-Beschleunigungsfeatures zu verwenden:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL" =dword:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

GPU-Beschleunigung für Windows-Desktopbetriebssysteme

August 18, 2021

Mit HDX 3D Pro können Sie grafikintensive Anwendungen als Teil gehosteter Desktops oder Anwendungen auf Desktopbetriebssystemmaschinen bereitstellen. HDX 3D Pro unterstützt physische Hostcomputer (einschließlich Desktop-, Blade- und Rack-Arbeitsstationen) und die Virtualisierungstechnologien der Hypervisors XenServer, vSphere und Hyper-V (nur Passthrough).

Mit GPU-Passthrough können Sie VMs mit exklusivem Zugriff auf dedizierte Hardware für die Grafikverarbeitung erstellen. Sie können mehrere GPUs auf dem Hypervisor installieren und VMs jeder dieser GPUs einzeln zuweisen.

Mit GPU-Virtualisierung können mehrere virtuelle Maschinen die Grafikverarbeitungsleistung eines einzelnen physischen GPU direkt nutzen. Die echte gemeinsame Hardware-GPU-Nutzung bietet Desktops, die für Benutzer mit komplexen und anspruchsvollen Designanforderungen geeignet sind. Für die GPU-Virtualisierung für NVIDIA GRID-Karten werden die gleichen NVIDIA-Grafiktreiber verwendet, die auf nicht-virtualisierten Betriebssystemen bereitgestellt werden. Die GPU-Virtualisierung wird darüber hinaus für Intel-CPUs der Generationen 5 und 6 mit Intel Iris Pro und Intel GVT-g unterstützt. Weitere Informationen zu den unterstützten Intel-Prozessoren finden Sie unter 5th Generation Intel Core Processors und 6th Generation Intel Core i5 Processors. Zudem wird für Serverkarten der AMD FirePro S-Serie GPU-Virtualisierung unterstützt, siehe AMD Professional Graphics virtualization solution.

HDX 3D Pro bietet die folgenden Features:

- Adaptive, auf dem H.264-Standard basierende Tiefenkomprimierung für optimale Leistung bei WAN-Verbindungen und drahtlosen Verbindungen. HDX 3D Pro verwendet die CPU-basierte

Vollbild-H.264-Komprimierung als Standardkomprimierungsverfahren zur Verschlüsselung. Hardwarecodierung wird für NVIDIA-Karten verwendet, die NVENC unterstützen.

- Verlustfreie Komprimierung für besondere Anwendungsfälle. HDX 3D Pro bietet einen verlustfreien CPU-basierten Codec zur Unterstützung von Anwendungen,in denen pixelgenaue Grafiken unerlässlich sind, z. B. für die medizinische Bilderstellung. Echte verlustfreie Komprimierung wird nur für besondere Anwendungsfälle empfohlen, da sie wesentlich mehr Netzwerk- und Verarbeitungsressourcen benötigt.

  Bei Verwendung von verlustfreier Komprimierung:

  - Die Anzeige für Verlustfreiheit, ein Symbol in der Taskleiste, zeigt an, ob es sich bei der Bildschirmanzeige um einen verlustreichen oder verlustfreien Frame handelt. Dies ist hilfreich, wenn die Richtlinieneinstellung Bildqualität auf Zu verlustfrei verbessern festgelegt ist. Die Anzeige für Verlustfreiheit wird grün, wenn die gesendeten Frames verlustfrei sind.
  - Über die Umschaltung für Verlustfreiheit können die Benutzer jederzeit innerhalb der Sitzung in den immer verlustfreien Modus wechseln. Zum Aktivieren oder Deaktivieren von Immer verlustfrei in einer Sitzung können Sie jederzeit mit der rechten Maustaste auf das Symbol klicken oder verwenden Sie die Tastenkombination ALT + UMSCHALT + 1.

    Für verlustfreie Komprimierung: HDX 3D Pro verwendet den verlustfreien Codec für die Komprimierung unabhängig von dem durch die Richtlinie ausgewählten Codec.

    Für die verlustreiche Komprimierung: HDX 3D Pro verwendet den ursprünglichen Codec, entweder den Standard oder den über die Richtlinie ausgewählten Codec.

    Einstellungen für die Umschaltung für Verlustfreiheit werden nicht für zukünftige Sitzungen gespeichert. Wenn Sie für alle Verbindungen den verlustfreien Codec verwenden möchten, legen Sie für die Richtlinie “Bildqualität”die Einstellung “Immer verlustfrei”fest.

- Sie können die Standardtastenkombination ALT + UMSCHALT + 1 zum Aktivieren oder Deaktivieren der Option “Verlustfrei”in einer Sitzung außer Kraft setzen. Konfigurieren Sie eine neue Registrierungseinstellung unter HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.

  - Name: HKLM_HotKey, Typ: String
  - Das Format zum Konfigurieren einer Tastenkombination ist C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K=val. Schlüssel müssen durch ein Komma (,) getrennt werden. Die Reihenfolge der Tasten ist egal.
  - A, C, S, W und K sind Tasten, wobei Folgendes gilt: C=STRG, A=ALT, S=UMSCHALT, W=Win und K=eine gültige Taste. Zulässige Werte für K sind a-z, 0-9 und jeder virtuelle Tastencode. Weitere Informationen zu virtuellen Tastencodes finden Sie auf MSDN unter Virtual-Key Codes.
  - Beispiel:
    - Taste F10 entspricht K=0x79

* Taste STRG + F10 entspricht C=1, K=0x79
* ALT + A entspricht A=1, K=a oder A=1, K=A oder K=A, A=1
* STRG + ALT + 5 entspricht C=1, A=1, K=5 oder A=1, K=5, C=1
* STRG + UMSCHALT + F5 entspricht A=1, S=1, K=0x74

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

- Unterstützung für mehrere Monitore und hochauflösende Monitore: Für Desktopbetriebssystemmaschinen unterstützt HDX 3D Pro Benutzergeräte mit bis zu vier Monitoren. Benutzer können ihre Monitore beliebig konfigurieren sowie Monitore mit unterschiedlichen Auflösungen und Ausrichtungen kombinieren. Die Anzahl der Monitore wird nur durch die Leistungsfähigkeit des GPU auf dem Hostcomputer, des Benutzergeräts und der verfügbaren Bandbreite begrenzt. HDX 3D Pro unterstützt alle Monitorauflösungen. Einschränkungen bestehen nur hinsichtlich der Leistungsfähigkeit der GPU auf dem Hostcomputer.

  Auf Windows XP-Desktops bietet HDX 3D Pro eingeschränkte Unterstützung für Dual-Monitor-Zugriff. Weitere Informationen hierzu finden Sie unter VDAs auf Maschinen mit Windows XP oder Windows Vista.

- Dynamische Auflösung: Sie können das Fenster des virtuellen Desktops oder der Anwendung auf eine beliebige Auflösung einstellen. **Hinweis**: Die einzige unterstützte Methode zum Ändern der Auflösung ist das Anpassen des VDA-Sitzungsfensters. Das Ändern der Auflösung in der VDA-Sitzung (über Systemsteuerung > Darstellung und Anpassung > Anzeige > Bildschirmauflösung) wird nicht unterstützt.

- Unterstützung der NVIDIA GRID-Architektur: HDX 3D Pro unterstützt NVIDIA GRID-Karten (siehe NVIDIA GRID) für GPU-Passthrough und GPU Sharing. Der NVIDIA GRID-vGPU ermöglicht mehreren VMs den gleichzeitigen direkten Zugriff auf einen physischen GPU und die Verwendung derselben NVIDIA-Grafiktreiber, die auf nicht-virtualisierten Betriebssystemen bereitgestellt werden.

- Unterstützung für VMware vSphere und VMware ESX mit Virtual Direct Graphics Acceleration (vDGA): Sie können HDX 3D Pro mit vDGA sowohl für Remotedesktopdienste- als auch für VDI-Arbeitslasten verwenden.

- Unterstützung für VMware vSphere/ESX mit NVIDIA GRID vGPU und AMD MxGPU.

- Unterstützung von Microsoft HyperV mit Discrete Device Assignment in Windows Server 2016:

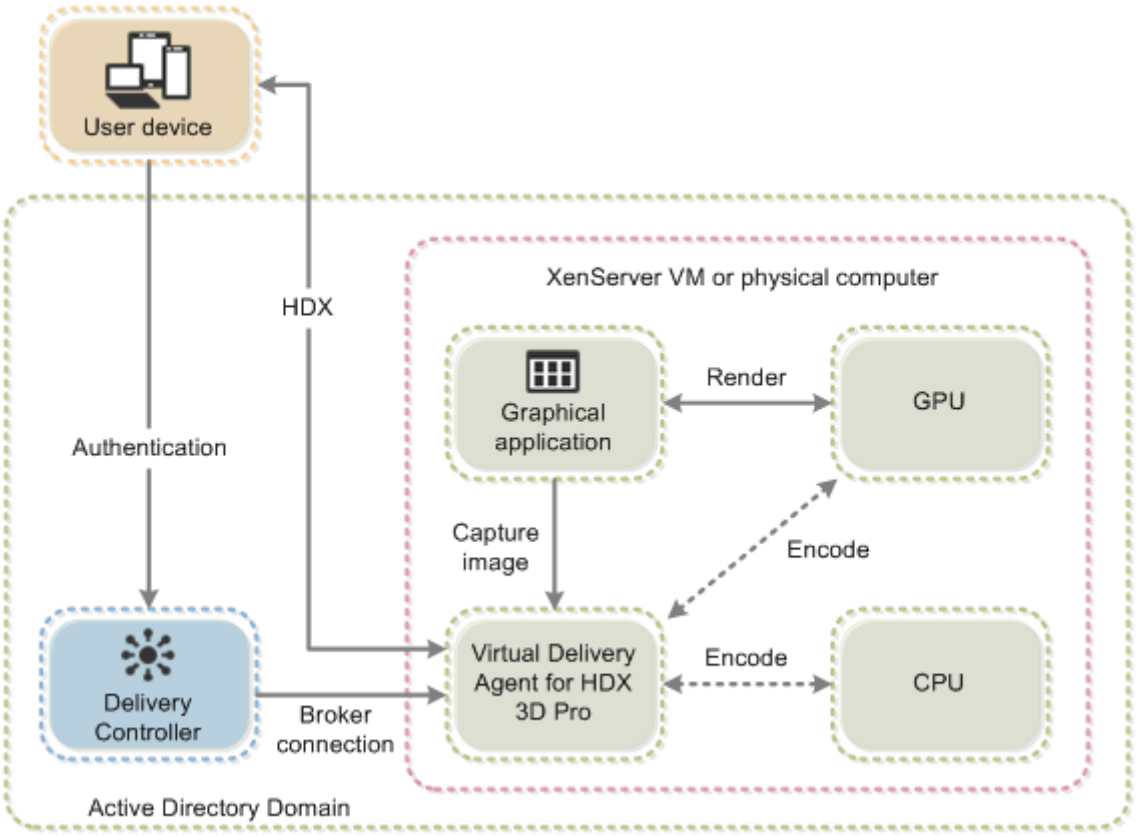
- Unterstützung von Datencenter-Grafikplattformen der Serie Intel Xeon Processor E3 HDX 3D Pro unterstützt die Verwendung von bis zu 3 Monitoren, das Ausblenden der Konsole, benutzerdefinierte Auflösungen und hohe Frameraten der unterstützten Intel-Serie. Weitere Informationen finden Sie unter https://www.citrix.com/intel und https://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Unterstützung für AMD RapidFire auf den Serverkarten der AMD FirePro S-Serie. HDX 3D Pro unterstützt den Betrieb von bis zu 6 Bildschirmen, Console Blanking, benutzerdefinierte Auflösungen und hohe Frameraten. Hinweis: HDX 3D Pro-Unterstützung für AMD MxGPU (GPU-Virtualisierung) funktioniert nur bei VMWare vSphere vGPUs. XenServer und Hyper-V werden mit GPU-Passthrough unterstützt. Weitere Informationen finden Sie unter AMD Virtualization Solution.
- Zugriff auf einen leistungsfähigen Videoencoder für NVIDIA-GPUs und Intel Iris Pro-Grafikprozessoren. Dieses Feature wird über eine (standardmäßig aktivierte) Richtlinie gesteuert und ermöglicht die Verwendung der Hardwarecodierung für die H.264-Codierung (falls verfügbar). Ist entsprechende Hardware nicht verfügbar, wird die CPU-basierte Codierung mit dem Software-Videocodec verwendet. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Grafiken".

Wie in der folgenden Abbildung dargestellt:

- Wenn sich ein Benutzer bei Citrix Receiver anmeldet und auf die virtuelle Anwendung oder den Desktop zugreift, authentifiziert der Controller den Benutzer und kontaktiert den VDA für HDX 3D Pro, um eine Verbindung zum Computer, der die grafische Anwendung hostet, zu vermitteln.

Der VDA für HDX 3D Pro komprimiert mit der entsprechenden Hardware auf dem Host die Ansicht des gesamten Desktops oder nur der grafischen Anwendung.

- Die Desktop- oder Anwendungsansichten und die dazugehörigen Interaktionen der Benutzer werden zwischen dem Hostcomputer und dem Benutzergerät über eine direkte HDX-Verbindung zwischen Citrix Receiver und VDA für HDX 3D Pro übertragen.



Installieren des VDA für HDX 3D Pro

Wenn Sie mit der grafischen Benutzeroberfläche des Installationsprogramms einen VDA für Windows-Desktopbetriebssysteme installieren, wählen Sie Ja auf der Seite "HDX 3D Pro". Wenn Sie die Befehlszeilenschnittstelle verwenden, schließen Sie die Option /enable_hdx_3d_pro in den Befehl XenDesktop VdaSetup.exe ein.

Für das Upgrade von HDX 3D Pro müssen Sie die separate Komponente HDX 3D für professionelle Grafiken und den VDA deinstallieren, bevor Sie den VDA im HDX 3D Pro-Modus installieren. Zum Wechsel vom standardmäßigen VDA-Modus für Windows-Desktopbetriebssysteme zum 3D Pro-Modus müssen Sie vor der Installation des VDAs im HDX 3D Pro-Modus den standardmäßigen VDA deinstallieren.

Standardmodus	HDX 3D Pro-Modus
Im Allgemeinen am besten für virtuelle Desktops ohne Grafikhardwarebeschleunigung und für Remote-PC-Zugriff geeignet.	Im Allgemeinen am besten geeignet für Desktops in Datencentern mit Grafikhardwarebeschleunigung, wenn nicht mehr als vier Monitore benötigt werden.

Standardmodus	HDX 3D Pro-Modus
Für Remote-PC-Zugriff kann jede GPU verwendet werden. Allerdings mit einigen Abstrichen bei der App-Kompatibilität: Unter Windows 7, 8 und 8.1 ist GPU-Beschleunigung für DirectX-Featureebenen bis 9.3 möglich. Einige DirectX 10, 11, 12-Anwendungen können u. U. nicht ausgeführt werden, wenn sie kein Fallback auf DirectX 9 tolerieren. Unter Windows 10 steht die GPU-Beschleunigung für DirectX 10-, 11- und 12-Apps im Fenstermodus zur Verfügung. DX 9-Apps werden über WARP wiedergegeben. DX-Apps können nicht im Vollbildmodus verwendet werden.	Unterstützt die GPU-Beschleunigung mit allen GPUs; das Ausblenden der Konsole, nicht standardmäßige Bildschirmauflösungen und echte Unterstützung für mehrere Bildschirme erfordern jedoch NVIDIA GRID, Intel Iris Pro Graphics oder AMD RapidFire Graphics. Verwendet den Grafiktreiber des Herstellers, der die umfassendste Anwendungskompatibilität bietet: alle 3D-APIs (DirectX oder OpenGL), die die GPU unterstützt. Unterstützung für Vollbild-3D-App mit Intel Iris Pro (nur Windows 10), NVIDIA GRID und AMD RapidFire.
OpenGL-Anwendungsbeschleunigung in Remotesitzungen, wenn vom GPU-Hersteller unterstützt (derzeit nur NVIDIA).	Unterstützung für benutzerdefinierte Treibererweiterungen und APIs. Beispiel: CUDA oder OpenCL.
Beliebige Monitorauflösungen (Limit hängt von Windows-Betriebssystem und Leistung ab) und bis zu acht Monitore.	Unterstützt bis zu vier Monitore.
H.264-Hardwarecodierung ist mit Intel Iris Pro-Grafikprozessoren verfügbar.	H.264-Hardwarecodierung ist mit NVIDIA-Smartcards verfügbar.

Installieren und Aktualisieren von NVIDIA-Treibern

Die NVIDIA GRID-API bietet direkten Zugriff auf den Framepuffer des Grafikprozessors und bietet die schnellste Framerate für eine gleichmäßige und interaktive Benutzererfahrung. Wenn Sie NVIDIA-Treiber vor einem VDA mit HDX 3D Pro installieren, ist NVIDIA GRID standardmäßig aktiviert.

Zum Aktivieren von NVIDIA GRID auf einer virtuellen Maschine müssen Sie den Microsoft Basic Display Adapter im Geräte-Manager deaktivieren. Führen Sie den folgenden Befehl aus und starten Sie dann den VDA neu: **NVFBCEnable.exe -enable -noreset**

Wenn Sie NVIDIA-Treiber nach einem VDA mit HDX 3D Pro installieren, ist NVIDIA GRID deaktiviert. Aktivieren Sie NVIDIA GRID mit dem von NVIDIA bereitgestellten Tool NVFBCEnable.

Führen Sie den folgenden Befehl aus, um NVIDIA GRID zu deaktivieren, und starten Sie dann den VDA neu: **NVFBCEnable.exe -disable -noreset**

Installieren von Intel-Grafiktreibern

Sie können die Intel-Grafiktreiber vor dem VDA installieren. Der folgende Schritt ist nur erforderlich, wenn Sie Intel-Treiber nach der Installation eines VDA mit HDX 3D Pro installieren oder wenn der Intel-Treiber aktualisiert wurde.

Zum Aktivieren der Intel-Treiber für Multimonitorunterstützung führen Sie mit GfxDisplayTool.exe den folgenden Befehl aus und starten Sie dann den VDA neu: **GfxDisplayTool.exe -vd enable**

GfxDisplayTool.exe ist im VDA-Installationsprogramm enthalten. GfxDisplayTool.exe ist in C:\Programme\Citrix\ICAServices.

> **Hinweis:**
>
> Das Deinstallieren von NVIDIA- oder Intel-Treibern in ICA-Sitzungen wird nicht unterstützt.

Optimierung der HDX 3D Pro-Benutzererfahrung

Stellen Sie bei der Verwendung von HDX 3D Pro mit mehreren Monitoren sicher, dass der Hostcomputer mit mindestens so vielen Monitoren konfiguriert ist, wie an den Geräten der Benutzer angeschlossen sind. Die an den Hostcomputer angeschlossenen Monitore können physikalische oder virtuelle Monitore sein.

Schließen Sie Monitore (physikalische oder virtuelle) nicht an Hostcomputer an, während Benutzer mit dem virtuellen Desktop oder der virtuellen Anwendung, die die grafische Anwendung bereitstellen, verbunden sind. Dies kann für die Dauer der Benutzersitzung zu Instabilität führen.

Teilen Sie den Benutzern mit, dass das Ausführen von Änderungen (von ihnen oder einer Anwendung) an der Desktopauflösung, während eine grafische Anwendungssitzung ausgeführt wird, nicht unterstützt wird. Nach dem Beenden der Anwendungssitzung können Benutzer die Auflösung des Desktop Viewer-Fensters in "Citrix Receiver - Desktop Viewer-Einstellungen"ändern.

Wenn mehrere Benutzer eine Verbindung mit beschränkter Bandbreite gemeinsam verwenden, z. B. in einer Zweigstelle, empfiehlt Citrix, die Richtlinieneinstellung "Bandbreitenlimit für Sitzung insgesamt"zu verwenden, um die für die einzelnen Benutzer verfügbare Bandbreite zu beschränken. Damit wird sichergestellt, dass die verfügbare Bandbreite beim Anmelden und Abmelden der Benutzer keinen großen Schwankungen unterworfen ist. Da HDX 3D Pro automatische Anpassungen durchführt, um die gesamte Bandbreite auszuschöpfen, kann sich die stark variierende verfügbare Bandbreite während der Benutzersitzungen negativ auf die Leistung auswirken.

Wenn beispielsweise 20 Benutzer eine Verbindung mit 60 MBit/s gemeinsam verwenden, kann die Bandbreite, die den einzelnen Benutzern zur Verfügung steht, abhängig von der Anzahl der gleichzeitigen Benutzer zwischen 3 MBit/s und 60 MBit/s variieren. Um die Benutzererfahrung in diesem Szenario zu optimieren, legen Sie die Bandbreite fest, die zu Spitzenzeiten pro Benutzer erforderlich ist, und stellen Sie sicher, dass die Benutzer diesen Wert nicht überschreiten können.

Citrix empfiehlt Benutzern einer 3D-Maus, die Priorität des virtuellen Kanals für die generische USB-Umleitung auf 0 zu erhöhen. Weitere Informationen dazu, wie Sie die Priorität virtueller Kanäle ändern können, finden Sie unter CTX128190.

OpenGL Software Accelerator

November 29, 2018

OpenGL Software Accelerator ist ein Softwarerasterizer für OpenGL-Anwendungen wie ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler sowie CAD- und CAM-Anwendungen. In einigen Fällen bietet OpenGL Software Accelerator auch ohne die Verwendung einer Grafikkarte eine gute Benutzererfahrung bei OpenGL-Anwendungen.

> **Wichtig**
>
> OpenGL Software Accelerator wird *ohne Gewähr* bereitgestellt und muss für alle Anwendungen getestet werden, da es evtl. nicht alle Anwendungen unterstützt. Es kann als Lösung dienen, wenn der Windows OpenGL-Rasterizer keine angemessene Leistung bietet. Wenn OpenGL Software Accelerator Ihre Anwendungen unterstützt, kann es Ihnen Kosten für GPU-Hardware sparen.

OpenGL Software Accelerator ist im Ordner "Support"auf dem Installationsmedium und wird auf allen gültigen VDA-Plattformen unterstützt.

Einsatzmöglichkeiten für OpenGL Software Accelerator:

- Wenn auf Servern ohne Grafikverarbeitungshardware die Leistung von OpenGL-Anwendungen in virtuellen Maschinen auf XenServer oder anderen Hypervisors unzureichend ist, versuchen Sie es mit OpenGL Accelerator. Bei einigen Anwendungen werden mit OpenGL Accelerator durch den Einsatz von SSE4.1 und AVX bessere Ergebnisse erzielt als mit dem in Windows enthaltenen Microsoft OpenGL Rasterizer. OpenGL Accelerator unterstützt zudem Anwendungen, die OpenGL-Versionen bis 2.1 verwenden.
- Bei Anwendungen, die auf einer Arbeitsstation ausgeführt werden, sollte zunächst die Standardversion von OpenGL verwendet werden, die von der Arbeitsstation des Grafikadapters bereitgestellt wird. Wenn es sich um eine aktuelle Grafikkarte handelt, wird damit normalerweise die beste Leistung erzielt. Bei Grafikkarten älterer Versionen oder weniger leistungsstarken Grafikkarten sollte OpenGL Software Accelerator eingesetzt werden.
- 3D OpenGL-Anwendungen, die nicht angemessen bereitgestellt wurden und CPU-basierte Softwarerasterisierung verwenden, profitieren möglicherweise von der OpenGL GPU-Hardwarebeschleunigung. Dieses Feature kann auf Bare-Metal- oder virtuellen Maschinen verwendet werden.

Thinwire

August 18, 2021

Einführung

ThinWire ist die in XenApp und XenDesktop verwendete Standardtechnologie von Citrix für das Anzeigeremoting.

Per Anzeigeremoting können auf einer Maschine erzeugte Grafiken (normalerweise über ein Netzwerk) auf eine andere Maschine für die Anzeige übertragen werden.

Eine gute Lösung für das Anzeigeremoting sollte eine hochgradig interaktive Benutzererfahrung –ähnlich wie bei einem lokalen Computer –liefern. Bei Thinwire wird dies mit komplexen und effizienten Bildanalyse- und Komprimierungsmethoden erzielt. Thinwire maximiert die Serverskalierbarkeit und verbraucht weniger Bandbreite andere Anzeigeremotingtechnologien.

Dank diesem Gleichgewicht ist Thinwire für die meisten geschäftlichen Anwendungsfälle geeignet und wird als Standardtechnologie für das Anzeigeremoting in XenApp und XenDesktop verwendet.

Verwendung von Thinwire oder Framehawk

Thinwire sollt für typische Desktoparbeitslasten (Bürogebrauch, browserbasierte Anwendungen o. Ä.) verwendet werden. Thinwire wird außerdem für Anwendungen mit mehreren Monitoren oder hohen Auflösungen und für heterogene Arbeitslasten mit und ohne Videoinhalte empfohlen.

Framehawk sollte für mobile Benutzer mit drahtlosen Breitbandverbindungen verwendet werden, in denen zeitweise hohe Paketverluste auftreten können.

HDX 3D Pro

In der Standardkonfiguration kann Thinwire 3D- oder hochgradig interaktive Grafik liefern. Allerdings ist für entsprechende Einsätze eine Aktivierung des HDX 3D Pro-Modus bei der Installation des VDAs für Desktopbetriebssysteme eine gute Option. Im 3D Pro-Modus wird Thinwire mit Vollbild-H.264-Codierung für Grafiken konfiguriert. Dies bietet eine flüssigere Anzeige professioneller 3D-Grafiken. Weitere Informationen finden Sie unter HDX 3D Pro und GPU-Beschleunigung für Windows-Desktopbetriebssysteme.

Anforderungen und Überlegungen

- Thinwire wurde für moderne Betriebssysteme, einschließlich Windows Server 2012 R2, Windows Server 2016, Windows 7 und Windows 10, optimiert. Für Windows Server 2008 R2 wird der Legacy-Grafikmodus empfohlen. Verwenden Sie die integrierten Citrix Richtlinienvorlagen "Hohe Serverskalierbarkeit – Legacy-OS" und "Für WAN optimiert – Legacy-OS" zum Bereitstellen der von Citrix für solche Anwendungsfälle empfohlenen Kombinationen von Richtlinieneinstellungen.
- Die Richtlinieneinstellung, die das Verhalten von Thinwire steuert (**Videocodec zur Komprimierung verwenden**), ist in VDA-Versionen in XenApp und XenDesktop 7.6 FP3 und höher verfügbar. Die Option **Videocodec verwenden, wenn bevorzugt** ist die Standardeinstellung für die VDA-Versionen XenApp und XenDesktop 7.9 und höher.
- Alle Citrix Receiver-Versionen unterstützen Thinwire. Einige Citrix Receiver-Versionen unterstützen jedoch unter Umständen manche Thinwire-Features nicht, z. B. 8- oder 16-Bit-Grafiken für eine reduzierte Bandbreitennutzung. Die Unterstützung solcher Features wird automatisch von Citrix Receiver ausgehandelt.
- Thinwire verwendet mehr Serverressourcen (CPU, Speicher) in Umgebungen mit mehreren Monitoren oder hoher Auflösung. Das Maß der Ressourcennutzung durch Thinwire kann eingestellt werden, dabei kann jedoch die Bandbreitennutzung steigen.
- In Umgebungen mit geringer Bandbreite oder hoher Latenz kann sich die Aktivierung von 8- oder 16-Bit-Grafik zur Verbesserung der Interaktivität anbieten, dadurch wird jedoch die Anzeigequalität, insbesondere bei einer 8-Bit-Farbtiefe, gemindert.

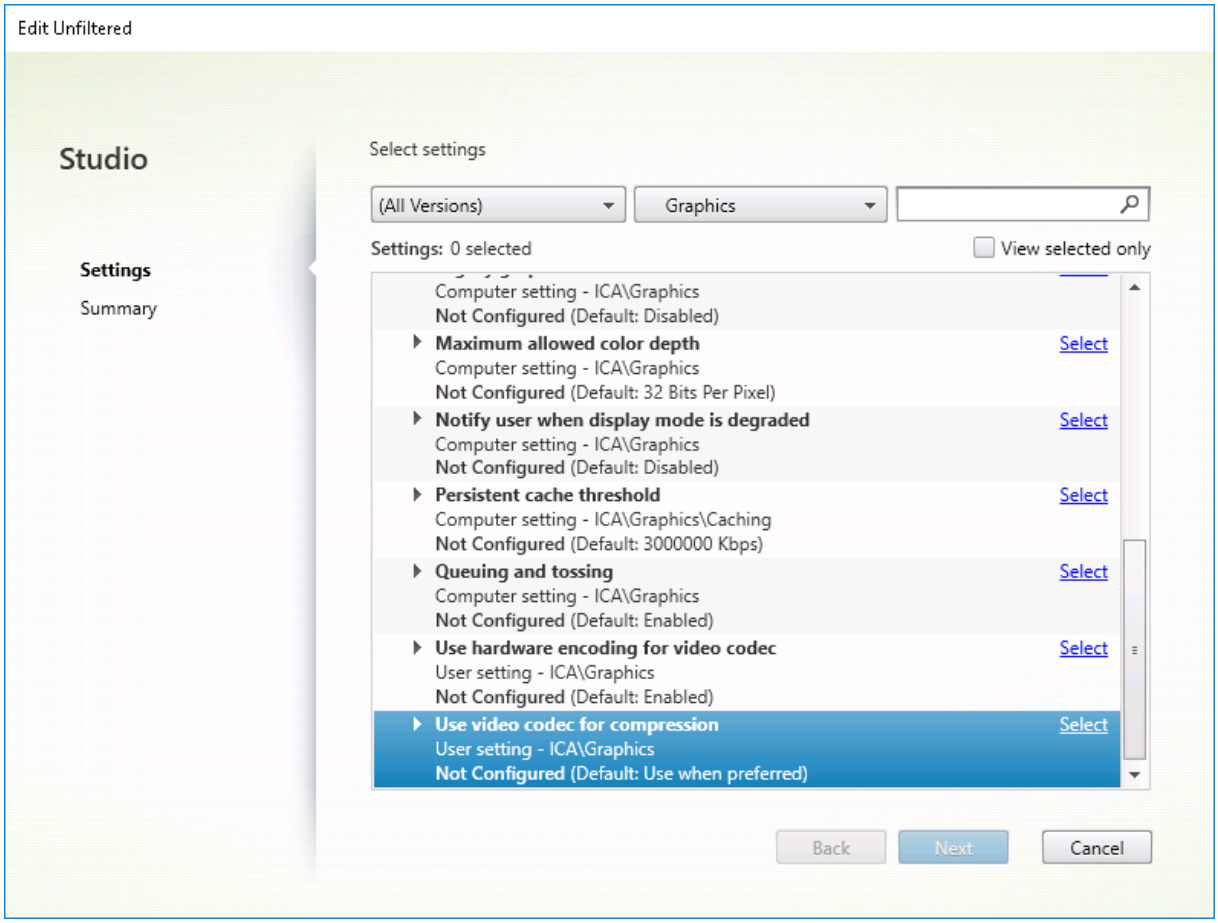
Konfiguration

Thinwire ist die Standardtechnologie für das Anzeigeremoting.

Die folgende Grafikrichtlinieneinstellung dient zum Festlegen der Standardeinstellung und zur Bereitstellung von Alternativen für verschiedene Anwendungsfälle:

- Verwenden von Videocodec für die Komprimierung
  - **Videocodec verwenden, wenn bevorzugt**. Dies ist die Standardeinstellung. Eine zusätzliche Konfiguration ist nicht erforderlich. Wenn Sie diese Einstellung als Standard beibehalten, dann wird Thinwire für alle Citrix Verbindungen ausgewählt und für Skalierbarkeit, Bandbreite und bessere Bildqualität bei typischen Desktoparbeitslasten optimiert.
- Von anderen Optionen in dieser Richtlinieneinstellung wird Thinwire auch verwendet und zwar in Kombination mit anderen Technologien für verschiedene Anwendungsfälle. Beispiel:

- **Für aktive Änderungsbereiche**. Die Technologie für adaptive Anzeige von Thinwire identifiziert bewegliche Bilder (Video, 3D In Motion) und verwendet H.264 nur in dem Bildschirmbereich, in dem das Bild sich bewegt.
- **Für den gesamten Bildschirm**. Thinwire wird mit Vollbild-H.264 zur Optimierung der Benutzererfahrung und Bandbreite, insbesondere bei intensiver 3D-Grafiknutzung, verwendet.



Einige weitere Richtlinieneinstellungen, einschließlich der nachfolgend aufgeführten Einstellungen der Richtlinie "Visuelle Anzeige", können zur Optimierung der Anzeigeremoting-Leistung verwendet werden und werden allesamt von Thinwire unterstützt:

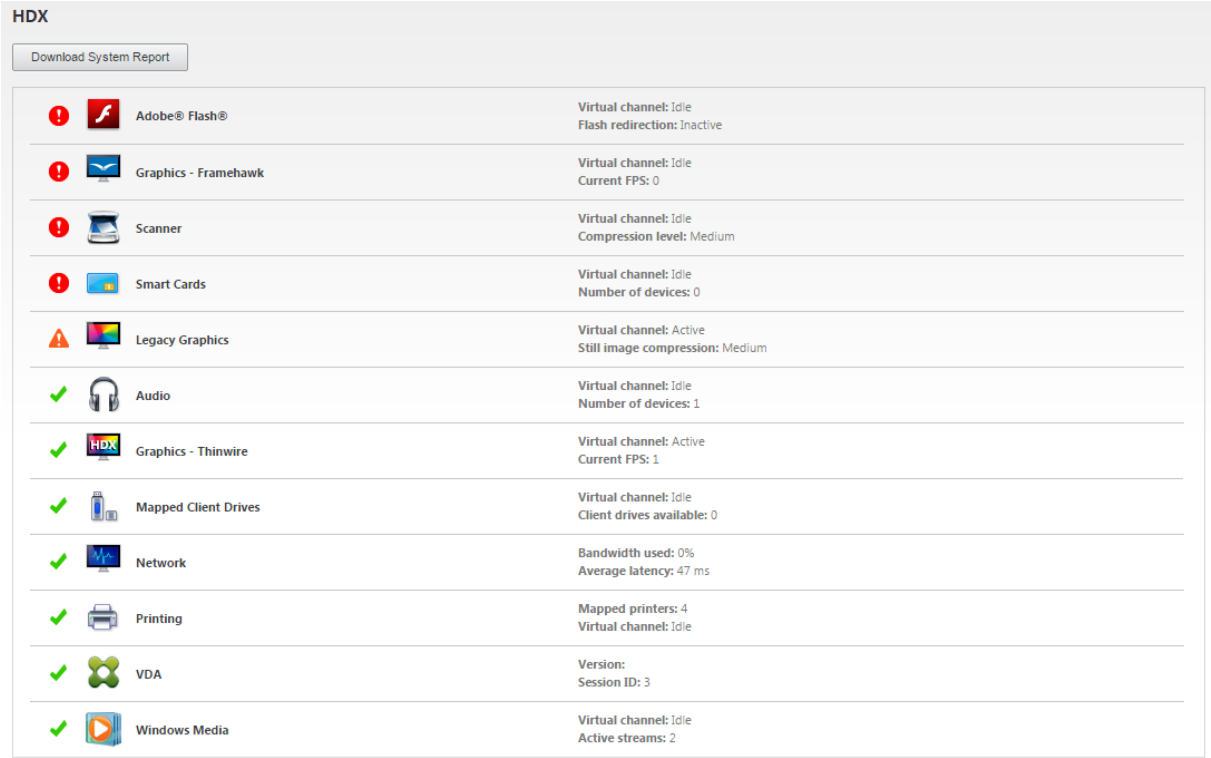
- Bevorzugte Farbtiefe für einfache Grafiken
- Frameratesollwert
- Bildqualität

Zur Aktivierung der von Citrix für verschiedene Anwendungsfälle empfohlenen Kombinationen von Richtlinieneinstellungen verwenden Sie die integrierten Citrix Richtlinienvorlagen. Die Vorlagen **Hohe Serverskalierbarkeit** und **Besonders gute High Definition-Benutzererfahrung** verwenden beide Thinwire mit der optimalen Kombination von Richtlinieneinstellungen für die Prioritäten Ihres Unternehmens und den Erwartungen Ihrer Benutzer.

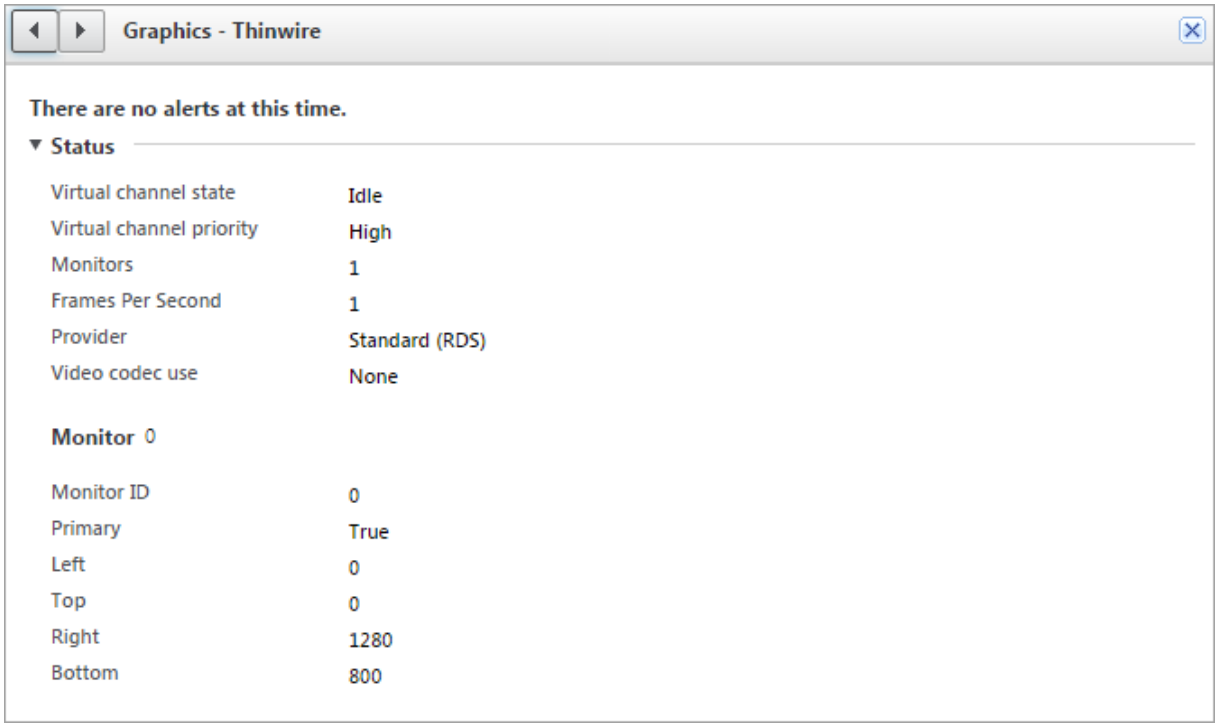
Überwachen von Thinwire

Sie können die Verwendung und Leistung von Thinwire über Citrix Director überwachen. Die Detailansicht für den virtuellen HDX-Kanal enthält nützliche Informationen zur Überwachung und Problembehandlung von Thinwire in jeder Sitzung. Gehen Sie zum Anzeigen für Thinwire relevanter Kennzahlen folgendermaßen vor:

1. Suchen Sie in Director einen Benutzer, eine Maschine oder einen Endpunkt, öffnen Sie eine aktive Sitzung und klicken Sie auf **Details**. Oder Sie können **Filter** > **Sitzungen** > **Alle Sitzungen** wählen, eine aktive Sitzung öffnen und auf **Details** klicken.
2. Führen Sie einen Bildlauf nach unten zum Bereich **HDX** aus.



1. Wählen Sie **Grafiken - Thinwire**.



Multimedia

December 31, 2019

Der HDX-Technologiestack unterstützt die Bereitstellung von Multimediaanwendungen über zwei einander ergänzende Methoden:

- Serverseitige Wiedergabe
- Clientseitige Wiedergabe mit Multimediaumleitung

Diese Strategie gewährleistet, dass Sie alle Multimediaformate mit einer guten Benutzererfahrung und bei maximaler Serverskalierbarkeit zu möglichst geringen Kosten pro Benutzer bereitstellen können.

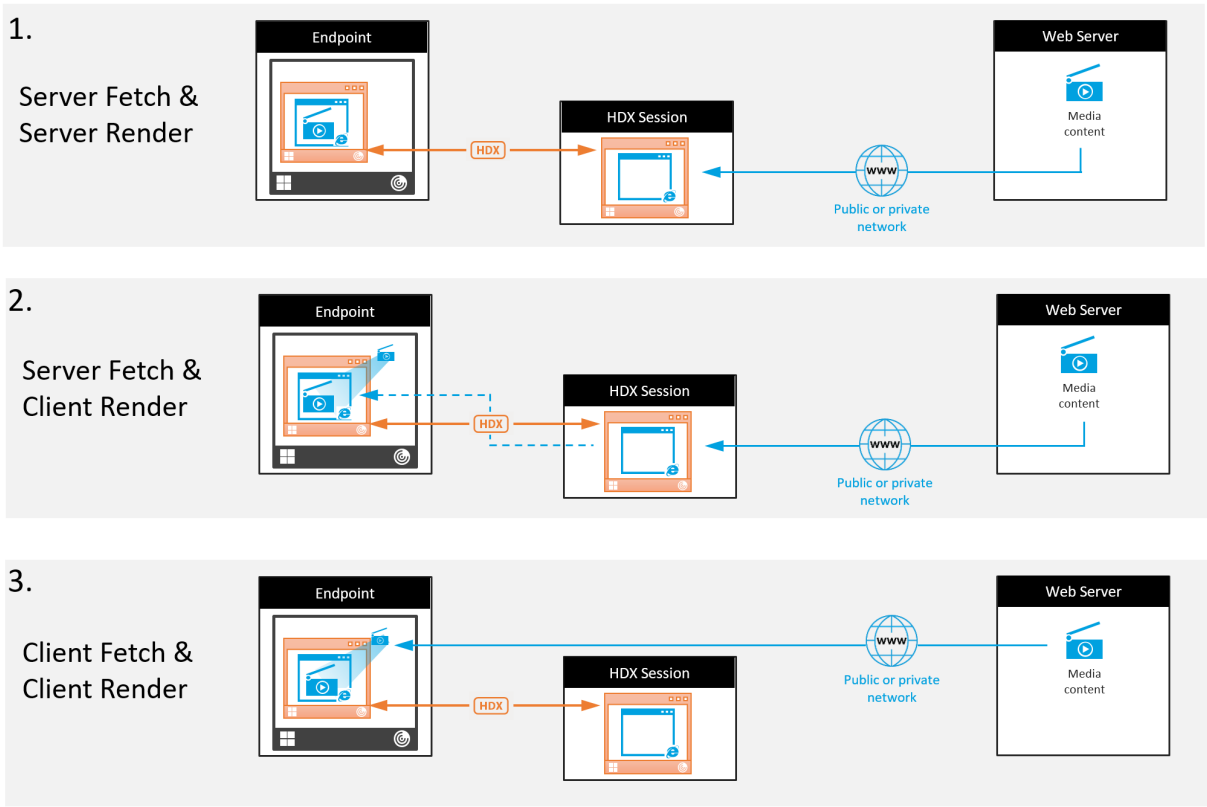
Bei der serverseitigen Wiedergabe wird Audio- und Videoinhalte decodiert und auf dem XenApp- oder XenDesktop-Server von der Anwendung wiedergegeben. Der Inhalt wird dann komprimiert und unter Einsatz des ICA-Protokolls an die Citrix Receiver-Instanz auf dem Benutzergerät gesendet. Diese Methode bietet die größtmögliche Kompatibilität mit verschiedenen Anwendungen und Medienformaten. Da die Videoverarbeitung rechenintensiv ist, profitiert die serverseitige Wiedergabe stark von einer platineninternen Hardwarebeschleunigung. DirectX Video Acceleration (DXVA) entlastet die CPU beispielsweise, da die H.264-Decodierung in einer separaten Hardware erfolgt. Intel Quick Sync und NVIDIA NVENC bieten H.264-Codierung mit Hardwarebeschleunigung.

Da die meisten Server keine Hardwarebeschleunigung für die Videokomprimierung bieten, beeinträchtigt eine Abwicklung der gesamten Videoverarbeitung auf der Server-CPU die Serverskalierbarkeit. Zur Wahrung einer hohen Serverskalierbarkeit können viele Multimediaformate zur lokalen Wiedergabe an die Benutzergeräte umgeleitet werden. Die Windows Media-Umleitung entlastet den Server bei vielen Medienformaten, die normalerweise Windows Media Player zugeordnet sind.

Die Flash-Umleitung leitet Adobe Flash-Videoinhalte auf einen Flash-Player um, der lokal auf dem Benutzergerät ausgeführt wird.
HTML5-Video ist mittlerweile gängig und Citrix hat eine Umleitungstechnologie für diese Art von Inhalt eingeführt.
Außerdem können Sie die allgemeinen Kontaktumleitungstechnologien der Host-zu-Client-Umleitung und des lokalen App-Zugriffs für Multimediainhalte nutzen.

Wenn Sie keine Umleitung konfigurieren, erfolgt bei HDX die Wiedergabe serverseitig.
Wenn Sie eine Umleitung konfigurieren verwendet HDX entweder den serverseitigen Abruf mit clientseitiger Wiedergabe oder den clientseitigen Abruf mit clientseitiger Wiedergabe. Wenn diese Methoden fehlschlagen, wechselt HDX zu serverseitigen Wiedergabe. Hier kommt dann die Richtlinie zum Verhindern von Videofallback zur Anwendung.

Beispielszenarios



Szenario 1. (Serverseitiger Abruf und serverseitige Wiedergabe):

1. Der Server ruft die Mediendatei von der Quelle ab, decodiert sie und sendet den Inhalt an ein Audio- oder Anzeigegerät.
2. Die Server extrahiert das von dem Gerät erzeugte Bild bzw. Audio.
3. Der Server komprimiert den Inhalt optional und sendet ihn an den Client.

Diese Methode ist mit einer starken CPU-Auslastung und, falls der extrahierte Inhalt nicht effizient komprimiert wurde, einer hohen Bandbreite sowie geringer Serverskalierbarkeit verbunden.

Thinwire und virtuelle Audiokanäle sind bei dieser Methode im Einsatz. Die Methode hat den Vorteil geringerer Anforderungen an Hardware und Software auf dem Client. Die Decodierung erfolgt auf dem Server und die Methode gestattet vielfältigere Geräte und Formate.

Szenario 2. (Serverseitiger Abruf und clientseitige Wiedergabe):

Diese Methode stützt sich auf die Möglichkeit, Medieninhalte abzufangen, bevor sie decodiert und auf einem Gerät ausgegeben werden. Die komprimierten Inhalte werden stattdessen an den Client gesendet und dort decodiert und wiedergegeben. Der Vorteil dieses Ansatzes besteht darin„ dass die Decodierung und Wiedergabe auf den Clients stattfindet und die Server-CPU entlastet wird.

Sie bedeutet jedoch einige zusätzliche Anforderungen an die Clienthardware und -software. Der Client muss jedes empfangene Format decodieren können.

Szenario 3. (Clientseitiger Abruf und clientseitige Wiedergabe):

Diese Methode stützt sich auf die Möglichkeit, die URL von Medieninhalten abzufangen, bevor diese von der Quelle abgerufen werden. Die URL wird an den Client gesendet, wo die Inhalte dann lokal abgerufen, decodiert und wiedergegeben werden. Das Konzept dieser Methode ist einfach. Sie bietet den Vorteil einer Entlastung der Server-CPU sowie einer geringeren Bandbreitennutzung, da vom Server nur Steuerbefehle gesendet werden. Die Clients können jedoch nicht immer auf Medieninhalte zugreifen.

Framework und Plattform

Desktopbetriebssysteme (Windows, Mac OS X und Linux) bieten Multimediaframeworks zum schnelleren und einfacheren Entwickeln von Multimediaanwendungen. Die nachstehende Tabelle enthält einige gebräuchliche Multimediaframeworks. Bei jedem Framework ist die Medienverarbeitung in mehreren Phasen unterteilt und es wird eine Pipelinearchitektur verwendet.

Framework	Plattform
DirectShow	Windows (98 und höher)
Media Foundation	Windows (Vista und höher)
Gstreamer	Linux

Framework	Plattform
Quicktime	Mac OS X

Double-Hop-Unterstützung mit Medienumleitungstechnologien

Media-Umleitung	Support
HDX Flash-Umleitung	Nein
Windows Media-Umleitung	Ja
HTML5-Videoumleitung	Ja
Audioumleitung	Nein

Verwandte Informationen

- Audiofeatures
- Flash-Umleitung
- HTML5-Multimediaumleitung
- Windows Media-Umleitung
- Allgemeine Inhaltsumleitung

Audiofeatures

August 2, 2022

Sie können die folgenden Citrix Richtlinieneinstellungen konfigurieren und einer Richtlinie hinzufügen, mit der HDX-Audiofeatures optimiert werden. Nutzungsinformationen sowie Beziehungen mit und Abhängigkeiten von anderen Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "Audio", Einstellungen der Richtlinie "Bandbreite" und Einstellungen der Richtlinie "Multistreamverbindungen".

> **Wichtig**
>
> Die Audiobereitstellung erfolgt zwar am besten über UDP (User Datagram Protocol) und nicht über TCP, doch ist die UDP-Audioverschlüsselung mit DTLS nur zwischen NetScaler Gateway und Citrix Receiver möglich. Daher ist in manchen Fällen möglicherweise die Verwendung von TCP

> vorzuziehen. TCP unterstützt die lückenlose TLS-Verschlüsselung zwischen VDA und Citrix Receiver.

Audioqualität

Im Allgemeinen erfordert eine höhere Audioqualität mehr Bandbreite und führt zu einer höheren CPU-Auslastung, da mehr Audiodaten an die Benutzergeräte gesendet werden. Mit der Audiokomprimierung können Sie die Audioqualität und die Sitzungsleistung aufeinander abstimmen; verwenden Sie Citrix Richtlinieneinstellungen, um den Komprimierungsgrad für Audiodateien zu konfigurieren.

Standardmäßig wird die Richtlinieneinstellung Audioqualität auf "Hoch - High Definition Audio" eingestellt, wenn TCP-Transport verwendet wird, und auf "Mittel - optimiert für Sprache", wenn UDP-Transport (empfohlen) verwendet wird. Die Einstellung High Definition-Audio bietet Audio in Hi-Fi-Stereoqualität, verbraucht aber mehr Bandbreite als die anderen Einstellungen. Verwenden Sie diese Audioqualität nicht für nicht optimierte Chat- und Videochat-Anwendungen (z. B. Softphones), da es hierbei zu Verzögerungen im Audiopfad kommen kann, was bei Echtzeitkommunikation ungeeignet ist. Die Richtlinieneinstellung "für Sprache optimiert"wird, unabhängig vom ausgewählten Transportprotokoll, für Echtzeitaudio empfohlen.

Bei Verbindungen mit begrenzter Bandbreite (z. B. bei Satelliten- oder DFÜ-Verbindungen) kann durch Verringern der Audioqualität auf **Niedrig** sichergestellt werden, dass die geringste Bandbreite verbraucht wird. Erstellen Sie in diesem Fall eigene Richtlinien für Benutzer von Verbindungen mit geringer Bandbreite, damit Benutzer von Verbindungen mit hoher Bandbreite nicht eingeschränkt werden.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe "Audioeinstellungsrichtlinien für Benutzergeräte").

Clientaudioumleitung

Damit der Audioempfang von einer Anwendung auf dem Server über Lautsprecher oder andere Soundgeräte (z. B. Kopfhörer) auf dem Benutzergerät zugelassen wird, übernehmen Sie für die Einstellung "Clientaudioumleitung"den Standardwert (Zugelassen).

Die Clientaudiozuordnung belastet Server und Netzwerk zusätzlich. Wenn die Clientaudioumleitung jedoch nicht zugelassen ist, sind alle HDX-Audiofunktionen deaktiviert.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe "Audioeinstellungsrichtlinien für Benutzergeräte").

Clientmikrofonumleitung

Damit die Audioaufzeichnung mit Eingabegeräten wie Mikrofonen auf dem Benutzergerät zugelassen wird, übernehmen Sie für die Einstellung "Clientmikrofonumleitung"den Standardwert (Zugelassen).

Aus Sicherheitsgründen werden Benutzer darauf hingewiesen, wenn Server, die keine vertrauenswürdige Beziehung zu den Benutzergeräten haben, auf Mikrofone zugreifen und können dann den Zugriff vor Verwenden des Mikrofons akzeptieren oder ablehnen. Benutzer können die diesbezügliche Warnung in Citrix Receiver deaktivieren.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe "Audioeinstellungsrichtlinien für Benutzergeräte").

Audio Plug & Play

Die Richtlinie Audio Plug & Play steuert, ob mehrere Audiogeräte zum Aufzeichnen und Wiedergeben zulässig sind. Diese Einstellung ist standardmäßig **aktiviert**. Audio-Plug & Play ermöglicht die Erkennung von Audiogeräten, selbst wenn diese erst nach Beginn einer Sitzung angeschlossen werden.

Diese Einstellung gilt nur für Windows-Serverbetriebssystemmaschinen.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Audio".

Bandbreitenlimit für die Audioumleitung und Bandbreitenlimit für die Audioumleitung (Prozent)

Die Richtlinieneinstellung "Bandbreitenlimit für die Audioumleitung"gibt die maximale Bandbreite (in Kilobits pro Sekunde) für die Wiedergabe und Aufzeichnung von Audio in einer Sitzung an. Die Einstellung Bandbreitenlimit für die Audioumleitung (Prozent) gibt die maximale Bandbreite für die Umleitung als Prozentsatz der insgesamt verfügbaren Bandbreite an. Standardmäßig ist Null (Maximum) für beide Einstellungen angegeben. Wenn beide Einstellungen konfiguriert sind, wird die Einstellung mit dem niedrigsten Bandbreitenlimit verwendet.

Informationen zu Einstellungen finden Sie unter Einstellungen der Richtlinie "Bandbreite". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe "Audioeinstellungsrichtlinien für Benutzergeräte").

Audio über UDP - Real-time Transport und Audio-UDP-Portbereich

Standardmäßig ist
Audio über UDP - Real-time Transport auf "Zugelassen"eingestellt (sofern die entsprechende Option

bei der Installation ausgewählt wurde), sodass ein UDP-Port auf dem Server für alle Verbindungen geöffnet wird, die für die Echtzeitübertragung von Audio über UDP konfiguriert wurden. Citrix empfiehlt, dass Sie UDP/RTP für Audio konfigurieren, um auch bei Netzwerküberlastung oder Paketverlust die beste Benutzererfahrung sicherzustellen. Für Echtzeit-Audio, z. B. Softphone-Anwendungen wird UDP-Audio jetzt gegenüber EDT bevorzugt. Bei UDP ist Paketverlust ohne Neuübertragung möglich, sodass bei Verbindungen mit hohen Paketverlusten keine zusätzliche Latenz entsteht.

> **Wichtig:**
>
> Mit UDP übertragene Audiodaten werden nicht verschlüsselt, wenn NetScaler Gateway nicht im Pfad ist. Ist NetScaler Gateway für den Zugriff auf XenApp- und XenDesktop-Ressourcen konfiguriert, wird der Audioverkehr zwischen Endpunktgerät und NetScaler Gateway mit DTLS gesichert.

Mit der Einstellung "Audio-UDP-Portbereich"geben Sie den Bereich der Portnummern an, die der Virtual Delivery Agent (VDA) zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet.

Der Standardbereich ist 16500 –16509.

Informationen zu den Einstellungen von "Audio über UDP - Real-time Transport"finden Sie unter Einstellungen der Richtlinie "Audio". Informationen zu "Audio-UDP-Portbereich"finden Sie unter Einstellungen der Richtlinie "Multistreamverbindungen". Denken Sie daran, die Clientaudioeinstellungen auf dem Benutzergerät zu aktivieren (siehe "Audioeinstellungsrichtlinien für Benutzergeräte").

Audioeinstellungsrichtlinien für Benutzergeräte

1. Laden Sie die Gruppenrichtlinienvorlagen gemäß den Anweisungen unter Konfigurieren der administrativen Gruppenrichtlinienobjektvorlage herunter.
2. Erweitern Sie im Gruppenrichtlinien-Editor "Administrative Vorlagen > Citrix Components > Citrix Receiver > User Experience".
3. Wählen Sie für **Clientaudioeinstellungen** die Option **Nicht konfiguriert**, **Aktiviert** oder **Deaktiviert**.
    - **Nicht konfiguriert**. Standardmäßig ist die Audioumleitung mit hoher Qualität oder zuvor konfigurierten benutzerdefinierten Audioeinstellungen aktiviert.
    - **Aktiviert.** Die Audioumleitung wird mit den ausgewählten Optionen aktiviert.
    - **Deaktiviert**. Die Audioumleitung wird deaktiviert.
4. Wenn Sie **Aktiviert** eingestellt haben, wählen Sie eine Tonqualität. Verwenden Sie für UDP-Audio die Standardeinstellung **Mittel**.
5. Aktivieren Sie nur für UDP-Audio die Einstellung **Real-Time Transport** und legen Sie den Bereich der eingehenden Ports so fest, dass der Durchgang durch die lokale Windows Firewall gewährleistet ist.

6. Zur Verwendung von UDP-Audio mit NetScaler Gateway wählen Sie die Option **Echtzeittransport über Gateway zulassen**. NetScaler Gateway muss mit DTLS konfiguriert sein. Weitere Informationen finden Sie unter UDP Audio Through a NetScaler Gateway.

Wenn Sie als Administrator auf Endpunktgeräten solche Änderungen nicht vornehmen können (beispielsweise im Fall von BYOD-Geräten oder Heimcomputern), aktivieren Sie UDP-Audio über die default.ica-Attribute von StoreFront.

1. Öffnen Sie auf der Maschine mit StoreFront die Datei C:\inetpub\wwwroot\Citrix\<Store Name>\App_Data\default.ica in einem Texteditor.
2. Fügen Sie unter dem Abschnitt [Application] Folgendes hinzu:

```
; This is to enable Real-Time Transport
EnableRtpAudio=true
; This is to Allow Real-Time Transport Through gateway
EnableUDPThroughGateway=true
; This is to set audio quality to Medium
AudioBandwidthLimit=1
; UDP Port range
RtpAudioLowestPort=16500
RtpAudioHighestPort=16509
 <!--NeedCopy-->
```

Wird UDP-Audio über die Datei default.ica aktiviert, gilt die Aktivierung für alle Benutzer des Stores.

Vermeiden von Echo in Multimediakonferenzen

Teilnehmer von Audio- oder Videokonferenzen hören eventuell ein Echo. Echos treten normalerweise auf, wenn der Abstand zwischen Lautsprechern und Mikrofonen nicht groß genug ist. Aus diesem Grund empfiehlt Citrix, dass Sie für Audio- und Videokonferenzen Kopfhörer verwenden.

HDX verfügt über eine Option zur Echounterdrückung (standardmäßig aktiviert), die das Auftreten von Echo minimiert. Die Qualität der Echounterdrückung hängt stark vom Abstand zwischen den Lautsprechern und dem Mikrofon ab. Der Abstand zwischen den Geräten darf nicht zu groß aber auch nicht zu klein sein.

Sie können eine Registrierungseinstellung ändern, um die Echounterdrückung zu deaktivieren.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des

> Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. Navigieren Sie mit dem Registrierungs-Editor auf dem Benutzergerät zu einer der folgenden Optionen:
   - 32-Bit-Computer: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advance
   - 64-Bit-Computer: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Ändern Sie den Wert im Feld Wertdaten in FALSE.

Softphones

Eine Softphone ist Software, die als Telefonbenutzeroberfläche fungiert. Mit einem Softphone können Anrufe von einem Computer oder einem anderen Gerät über das Internet getätigt werden. Das Softphone ermöglicht das Wählen einer Telefonnummer und die Nutzung weiterer Telefonfunktionen über einen Bildschirm.

XenApp und XenDesktop unterstützen verschiedene Bereitstellungsmethoden für Softphones.

- **Steuermodus:** Das gehostete Softphone steuert einfach ein physisches Telefon. In diesem Modus werden keine Audiodaten über den XenApp- oder XenDesktop-Server gesendet.
- **Softphone-Unterstützung mit HDX RealTime-Optimierung:** Die Media Engine wird auf dem Benutzergerät ausgeführt und der VoIP-Datenverkehr erfolgt Peer-to-Peer. Beispiele:
  - HDX RealTime Optimization Pack zur Optimierung der Bereitstellung von Microsoft Skype for Business und Lync
  - Cisco Virtualization Experience Media Engine (VXME) für Jabber
  - Avaya VDI Communicator für one-X Communicator und one-X Agent (one-X Agent kann nur als Fernsteuerungs-App für Desktoptelefone verwendet werden.)
- **Lokaler App-Zugriff:** XenApp- und XenDesktop-Funktion, welche die lokale Ausführung von Softphones und ähnlichen Anwendungen auf dem Windows-Gerät eines Benutzers ermöglicht, wobei die Anwendung nahtlos in dessen virtuellen/veröffentlichte Desktop integriert erscheint. Dadurch wird die gesamte Audioverarbeitung auf das Benutzergerät übertragen. Weitere Informationen finden Sie unter Lokaler App-Zugriff und URL-Umleitung.
- **Generische Softphone-Unterstützung mit HDX RealTime-Optimierung:** VoIP über ICA

Generische Softphone-Unterstützung

Mit der generischen Softphone-Unterstützung können Sie ein unverändertes Softphone unter XenApp oder XenDesktop im Datencenter hosten. Für den Audiodatenverkehr an das Benutzergerät mit Citrix Receiver wird das Citrix ICA-Protokoll (vorzugsweise mit UDP/RTP) verwendet.

Die generische Softphone-Unterstützung ist ein Feature von HDX RealTime. Diese Art der Softphone-Bereitstellung eignet sich besonders in folgenden Fällen:

- Wenn keine optimierte Lösung für die Softphone-Bereitstellung zur Verfügung steht und der Benutzer kein Windows-Gerät verwendet, auf dem der lokale App-Zugriff verwendet werden kann
- Wenn die Media Engine für die optimierte Softphone-Bereitstellung nicht auf dem Benutzergerät installiert ist oder für dessen Betriebssystemversion nicht verfügbar ist In diesem Szenario ist die generische Unterstützung mit HDX RealTime eine nützliche Fallback-Lösung.

Bei der Softphone-Bereitstellung mit XenApp und XenDesktop sind zwei Punkte zu beachten:

- Art der Bereitstellung des Softphones auf dem virtuellen/veröffentlichten Desktop
- Art der Übermittlung der Audiodaten von und zu dem Kopfhörer, Mikrofon, Lautsprecher und/oder USB-Telefon des Benutzers

XenApp und XenDesktop umfassen zahlreiche Technologien für die generische Softphone-Bereitstellung:

- Sprachoptimierter Codec zur schnellen und bandbreiteneffizienten Echtzeit-Audiocodierung
- Audio Stack mit geringer Latenz
- Serverseitiger Jitter-Puffer zur Audiooptimierung bei schwankender Netzwerklatenz
- Paket-Markierung (DSCP und WMM) für Servicequalität
  - DSCP-Markierung für RTP-Pakete (Layer-3)
  - WMM-Markierung für WLAN

Die Citrix Receiver-Versionen für Windows, Linux, Chrome und Mac sind auch VoIP-fähig. Citrix Receiver für Windows bietet die folgenden Features:

- Clientseitiger Jitter-Puffer zur Audiooptimierung bei schwankender Netzwerklatenz
- Echounterdrückung, die größere Unterschiede beim Abstand zwischen Mikrofon und Lautsprecher ausgleicht, wenn Mitarbeiter kein Headset verwenden
- Audio-Plug & Play, sodass Audiogeräte nicht vor Sitzungsstart angeschlossen werden müssen. Sie können jederzeit angeschlossen werden.
- Audiogeräterouting, sodass die Benutzer den Klingelton an den Lautsprecher und die Sprachausgabe an ihr Headset senden können
- Multistream-ICA für ein flexibles, servicequalitätsbasiertes Routing über das Netzwerk
- ICA unterstützt vier TCP- und zwei UDP-Streams. Einer der UDP-Streams unterstützt Echtzeit-Audio über RTP.

Eine Übersicht über die Funktionen von Citrix Receiver finden Sie in der Citrix Receiver-Featurematrix.

Empfehlungen für die Systemkonfiguration

Clienthardware und -software: Zur Gewährleistung der optimalen Audioqualität empfiehlt Citrix die Verwendung der aktuellen Citrix Receiver-Version und eines hochwertigen Headsets mit akustischer

Echounterdrückung (AEC). Citrix Receiver-Versionen für Windows, Linux und Mac unterstützen VoIP. Dell Wyse bietet überdies VoIP-Unterstützung für ThinOS (WTOS).

CPU: Überwachen Sie die CPU-Auslastung auf dem VDA, um festzustellen, ob jeder virtuellen Maschine zwei virtuelle CPUs zugewiesen werden müssen. Echtzeit Sprach- und Videoanrufe sind datenintensiv. Durch Konfigurieren von zwei virtuellen CPUs wird die Latenz beim Threadwechsel reduziert. Daher wird empfohlen, dass Sie in einer XenDesktop VDI-Umgebung zwei virtuelle CPUs konfigurieren.

Die Konfiguration von zwei virtuellen CPUs bedeutet nicht unbedingt die Verdoppelung der Zahl physischer CPUs, da diese von Sitzungen geteilt werden können.

Auch das für die Sitzungszuverlässigkeit verwendete Citrix Gateway Protocol (CGP) erhöht den CPU-Verbrauch. Bei Netzwerkverbindungen mit hoher Qualität können Sie dieses Feature zum Verringern des CPU-Verbrauchs auf dem VDA deaktivieren. Auf einem leistungsstarken Server ist evtl. keiner der o. g. Schritte erforderlich.

UDP-Audio: Audio über UDP bietet eine hervorragende Toleranz bei starker Netzwerklast und Paketverlusten. Citrix empfiehlt die Verwendung anstelle von TCP, sofern möglich.

LAN/WAN-Konfiguration: Die richtige Konfiguration des Netzwerks ist für eine gute Echtzeit-Audioqualität unerlässlich. Normalerweise müssen Sie virtuelle LANs (VLANs) konfigurieren, da eine hohe Zahl Broadcastpakete Jitter verursachen können. IPv6-aktivierte Geräte können eine hohe Zahl Broadcastpakete generieren. Wenn IPv6 nicht erforderlich ist, können Sie es auf den Geräten deaktivieren. Konfigurieren Sie es für Servicequalitätszwecke.

Einstellungen für WAN-Verbindungen:
Sie können Sprach-Chat über das lokale Netzwerk (LAN) und ein Wide Area Network (WAN) verwenden. Bei WAN-Verbindungen hängt die Audioqualität von der Latenz, Paketverlust und Jitter ab. Für die Bereitstellung von Softphones über eine WAN-Verbindung empfiehlt Citrix zur Gewährleistung einer hohen Servicequalität die Verwendung von Citrix SD-WAN zwischen dem Datencenter und dem Remotestandort. Citrix SD-WAN unterstützt Multistream-ICA und UDP. Bei TCP-Einzelstreams kann überdies die Priorität der verschiedenen virtuellen ICA-Kanäle unterschieden werden, um sicherzustellen, dass Echtzeit-Audiodaten mit hoher Priorität bevorzugt werden.

Mit der direkten Workloadverbindung kann Audio über UDP nach der Authentifizierung über das Gateway mit Citrix SD-WAN verschlüsselt werden.

Verwenden Sie Director oder HDX Monitor zum Überprüfen der HDX-Konfiguration.

Remotebenutzerverbindungen: NetScaler Gateway 11 unterstützt DTLS für die native (ohne TCP-Einkapselung) Bereitstellung von UDP/RTP-Datenverkehr.
Sie müssen Firewalls bidirektional für UDP-Datenverkehr über Port 443 öffnen.

Codec-Auswahl und Bandbreitenverbrauch:
Für den Datenverkehr zwischen dem Benutzergerät und dem VDA im Datencenter empfiehlt Citrix, die

Codec-Einstellung "Sprachoptimiert"(= mittlere Audioqualität) zu verwenden. Zwischen VDA und IP-Telefon verwendet das Softphone den konfigurierten oder ausgehandelten Codec. Beispiel:

- G711 bietet eine bessere Sprachqualität, erfordert jedoch eine Bandbreite von 80 bis 100 Kilobit pro Sekunde und Anruf (abhängig vom Overhead in Netzwerkschicht 2).
- G729 bietet eine gute Sprachqualität bei geringer Bandbreitennutzung von 30 bis 40 Kilobit pro Sekunde und Anruf (abhängig vom Overhead in Netzwerkschicht 2).

Bereitstellung von Softphone-Anwendungen auf dem virtuellen Desktop

Es gibt zwei Methoden zur Bereitstellung von Softphones auf virtuellen XenDesktop-Desktops:

- Die Anwendung kann auf dem virtuellen Desktopimage installiert werden.
- Die Anwendung kann mit Microsoft App-V an den virtuellen Desktop gestreamt werden. Diese Methode ist verwaltungsmäßig besser, da das virtuelle Desktopimage übersichtlich bleibt. Nach dem Streaming an den virtuellen Desktop wird die Anwendung so ausgeführt, als wäre sie normal installiert worden. Nicht alle Anwendungen sind mit App-V kompatibel.

Übertragen von Audiodaten auf Benutzergeräten

Generisches HDX RealTime unterstützt zwei Methoden der Audiobereitstellung für Benutzergeräte:

- **Citrix Audio Virtual Channel:** Citrix Audio Virtual Channel wird von Citrix normalerweise empfohlen, da es speziell für die Audioübertragung entwickelt wurde.
- **Generische USB-Umleitung:** Diese Methode ist nützlich für Audiogeräte mit Tasten und/oder einem Bildschirm oder Eingabegerät, wenn zwischen Benutzergerät und XenApp- oder XenDesktop-Server eine LAN- oder LAN-ähnliche Verbindung besteht.

Citrix Audio Virtual Channel

Der bidirektionale Citrix Audio Virtual Channel (CTXCAM) ermöglicht die effiziente Audioübertragung über das Netzwerk. Beim generischen HDX RealTime werden Audiodaten vom Headset oder Mikrofon komprimiert und über ICA an die Softphone-Anwendung auf dem virtuellen Desktop gesendet. Die Audioausgabe des Softphones wird ebenfalls komprimiert und in die Gegenrichtung gesendet. Diese Komprimierung ist unabhängig von der Komprimierung des Softphones selbst (z. B. G.729 oder G.711). Sie erfolgt unter Einsatz des sprachoptimierten Codec (mittlere Qualität). Die Eigenschaften sind ideal für VoIP (Voice-over-IP). Die Codierung ist schnell und die Netzwerkbandbreite ist mit nur ca. 56 Kilobit pro Sekunde (28 Kbit/s in jede Richtung) gering. Dieses Codec muss in der Studio-Konsole ausgewählt werden, da er nicht standardmäßig aktiviert ist. Der Standard-Codec ist HD-Audio (hohe Qualität). Dieser Codec eignet sich hervorragend für Hi-Fi-Stereosound, ist aber im Vergleich zum sprachoptimierten Codec langsamer.

Generische USB-Umleitung

Die generische USB-Umleitung von Citrix (CTXGUSB –virtueller Kanal) bietet eine generische Methode für das Remoting von USB-Geräten, auch für Kombi-Geräte (Audio plus Eingabegerät) sowie

isochrone USB-Geräte. Diese Methode ist auf LAN-Verbindungen beschränkt, da das USB-Protokoll latenzempfindlich ist und eine beträchtliche Netzwerkbandbreite erfordert. Die isochrone USB-Umleitung funktioniert bei einigen Softphones gut. Sie bietet eine hervorragende Sprachqualität und geringe Latenz, doch Citrix Audio Virtual Channel ist zu bevorzugen, da es für Audioverkehr optimiert ist. Die primäre Ausnahme bilden Audiogeräte mit Tasten, z. B. an ein Benutzergerät mit LAN-Verbindung zum Datencenter angeschlossene USB-Telefone. Die generische USB-Umleitung unterstützt in diesem Fall Tasten auf dem Telefon oder Headset zur Steuerung von Features unter Rückgabe eines Signals an das Softphone. Dies ist kein Problem bei Tasten, die lokal auf dem Gerät funktionieren.

Browserinhaltsumleitung

August 18, 2021

Mit diesem Feature wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Durch das Feature werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC. Nur der Viewport (der für Benutzer sichtbare Bereich der Webseite) wird zum Endpunkt umgeleitet.
Die Browserinhaltsumleitung leitet die Benutzeroberfläche (Adressleiste, Symbolleiste usw.) des Browsers auf dem VDA nicht um.

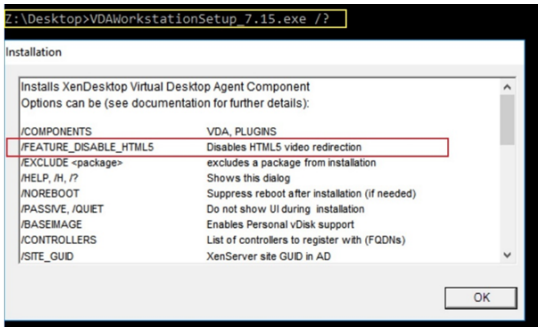
Systemanforderungen

Diese Anforderungen gelten für das BCR.msi mit XenApp und XenDesktop 7.15 LTSR CU5. Ignorieren Sie sämtliche für andere Versionen von XenApp, XenDesktop und Citrix Virtual Apps and Desktops aufgeführten Systemanforderungen für die Browserinhaltsumleitung.

- Version 7.15 LTSR CU5 oder höher auf dem Delivery Controller und dem VDA.
- Citrix Workspace-App 1809 oder später für Windows.
- Citrix Receiver für Linux 13.9.1 oder höher.
- BCR.msi –verfügbar auf der Citrix Downloadseite.
- Chrome (mit installierter Browserinhaltsumleitungserweiterung aus dem Chrome Web Store) oder Internet Explorer 11 (mit aktiviertem Browser Helper Object (BHO) Citrix HDXJsInjector).

Installation

1. Installieren Sie über die Befehlszeilenoption /FEATURE_DISABLE_HTML5 Version 7.15 LTSR CU5 des VDA (bzw. führen Sie ein Upgrade auf diese Version durch).



   Diese Option entfernt die HTML5-Videoumleitung, was vor dem Ausführen des BCR.msi-Pakets erforderlich ist. Durch das BCR.msi werden das Feature selbst sowie die entsprechenden Dienste während der Installation wieder hinzugefügt. Öffnen Sie nach diesem Schritt die services.msc-Konsole und vergewissern Sie sich, dass **Citrix HDX HTML5 Video Redirection Service** nicht aufgeführt wird.

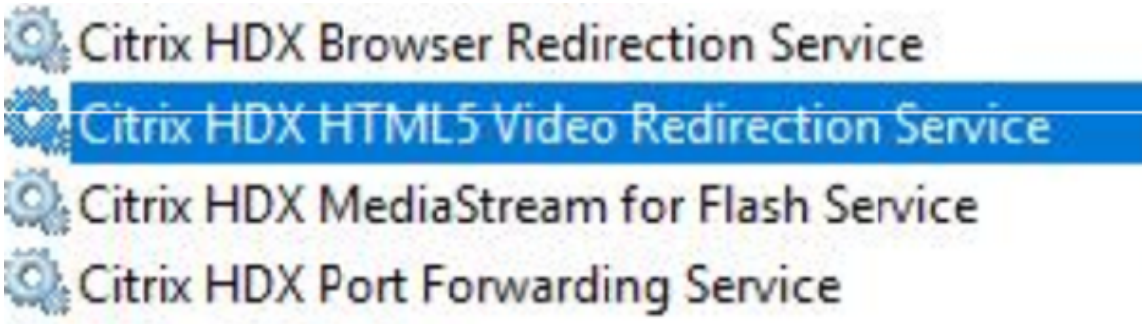
2. Starten Sie die Installation der Browserinhaltsumleitung mit dem BCR.msi. Systemabhängig werden die BCR.msi-Dateien unter einem der folgenden Pfade installiert:

   C:\Programme\Citrix\ICAService

   oder

   C:\Programme (x86)\Citrix\ICAService

   Da die Installation schnell erfolgt, wird das Dialogfeld möglicherweise schnell geschlossen. Führen Sie in diesem Fall services.msc erneut aus, um zu prüfen, ob die Dienste hinzugefügt wurden.

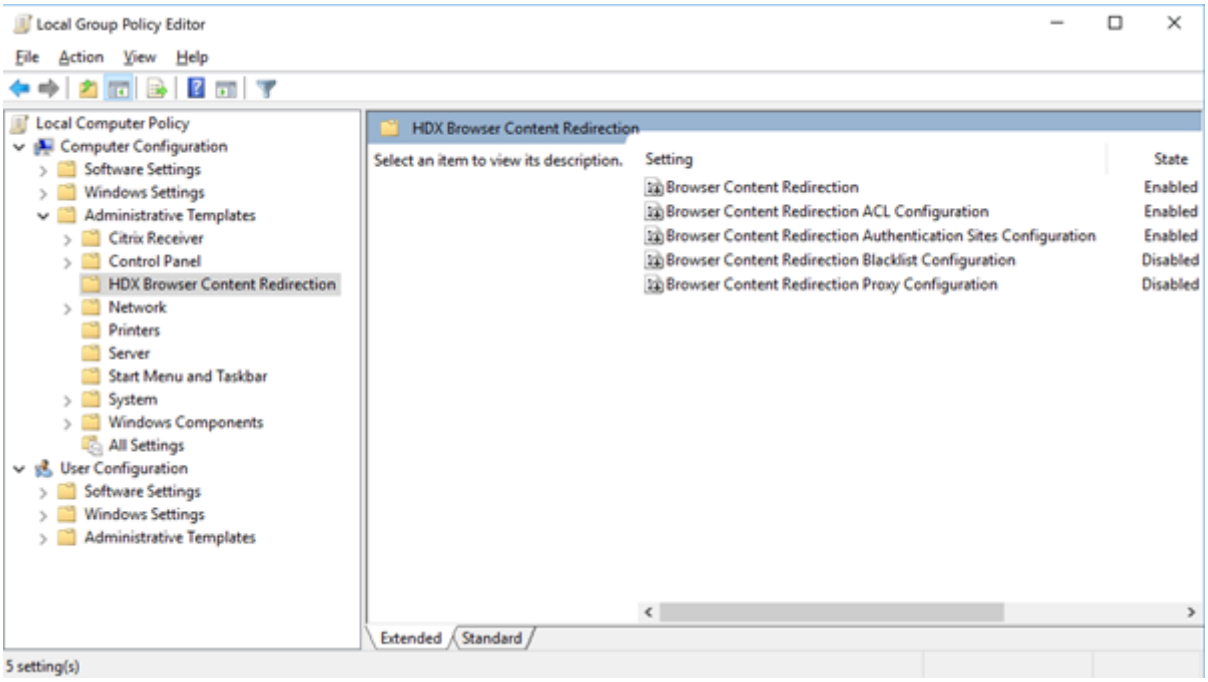


Richtlinien

Sie können Richtlinien über Registrierungseinträge unter HKEY_LOCAL_MACHINE auf dem VDA oder die administrative Vorlage **HDX Browser Content Redirection** von Citrix für die Gruppenrichtlinien-

Verwaltungskonsole steuern.

Sie können die Vorlage von citrix.com unter Citrix Virtual Apps and Desktops (XenApp & XenDesktop) > XenApp 7.15 LTSR / XenDesktop 7.15 LTSR > Components herunterladen. Citrix Studio enthält diese Richtlinien nicht.



Weitere Informationen finden Sie unter Richtlinieneinstellungen für die Browserinhaltsumleitung. Informationen zur Problembehandlung finden Sie im Knowledge Center-Artikel CTX230052.

Flash-Umleitung

August 18, 2021

> **Wichtig**
>
> Am 25. Juli 2017 kündigte Adobe das End of Life (EOL) für Flash an. Adobe plant, die Aktualisierung und Verteilung von Flash Player Ende des Jahres 2020 einzustellen.
>
> Microsoft hat angekündigt, die Unterstützung für Flash im Internet Explorer vor dem von Adobe angekündigten Datum zu stoppen. Bis zum Ende des Jahres 2020 wird Flash aus Windows entfernt. Ab dem Zeitpunkt können Benutzer Flash nicht mehr in Internet Explorer aktivieren oder ausführen.
>
> Citrix richtet sich nach Microsoft und wird die Wartung und Unterstützung für die HDX Flash-Umleitung bis Ende 2020 fortsetzen. Es wurde noch nicht entschieden, in welchen

> Versionen von XenApp und XenDesktop der Code für die Flash-Umleitung ausgeschlossen wird, aber wir empfehlen, dass Sie sobald wie möglich zu HTML5-Videoumleitung wechseln. HTML5-Videoumleitung eignet sich ideal zum Steuern von Multimediainhalt. Beispiele sind Kommunikationsvideos von Unternehmen, Schulungsvideos oder wenn ein Drittanbieter den Inhalt hostet.
>
> Weitere Informationen zur HTML5-Videoumleitung finden Sie unter HTML5-Multimediaumleitung.

Bei der Flash-Umleitung wird die Verarbeitung der meisten Adobe Flash-Inhalte (einschließlich Animationen, Videos und Anwendungen) an über LAN- und WAN-angeschlossene Windows-Benutzergeräte und 32-Bit-Linux x86-Geräte übertragen, wodurch Server- und Netzwerklast verringert werden. Dies führt zu größerer Skalierbarkeit, während gleichzeitig eine High Definition-Benutzererfahrung sichergestellt wird. Das Konfigurieren der Flash-Umleitung erfordert sowohl server- als auch clientseitige Einstellungen.

> **Achtung:**
>
> Bei der Flash-Umleitung findet eine erhebliche Anzahl von Interaktionen zwischen dem Benutzergerät und den Serverkomponenten statt. Verwenden Sie dieses Feature nur in Umgebungen, in denen eine sicherheitsbedingte Trennung zwischen dem Benutzergerät und dem Server nicht erforderlich ist. Zudem müssen Benutzergeräte so konfiguriert werden, dass sie dieses Feature nur mit vertrauenswürdigen Servern verwenden. Da für die Flash-Umleitung Adobe Flash Player auf dem Benutzergerät installiert sein muss, aktivieren Sie diese Funktion nur, wenn der Flash Player gesichert ist.

Die Flash-Umleitung wird sowohl auf Clients als auch auf Servern unterstützt. Wenn der Client die Flash-Umleitung der zweiten Generation unterstützt, werden Flash-Inhalte auf dem Client wiedergegeben. Flash-Umleitungsfeatures bieten Unterstützung für Benutzerverbindungen über das WAN, intelligentes Fallback und eine URL-Kompatibilitätsliste. Weitere Details finden Sie weiter unten.

Flash-Umleitung verwendet die Windows-Ereignisprotokollierung auf dem Server, um Flash-Ereignisse zu protokollieren. Das Ereignisprotokoll gibt an, ob Flash-Umleitung verwendet wird und ob Probleme vorliegen. Folgendes gilt für alle Ereignisse, die von der Flash-Umleitung protokolliert werden:

- Die Flash-Umleitung meldet Ereignisse an das Anwendungsprotokoll.
- Unter Windows 10, Windows 8 und Windows 7 wird ein spezifisches Protokoll für die Flash-Umleitung im Knoten “Anwendungs- und Dienstprotokolle”angezeigt.
- Der Quellwert ist Flash.
- Es wird keine Kategorie angegeben.

Aktuelle Updates für HDX Flash-Kompatibilität finden Sie unter CTX136588.

Konfigurieren der Flash-Umleitung auf dem Server

Zum Konfigurieren der Flash-Umleitung auf dem Server verwenden Sie die folgenden Citrix Richtlinieneinstellungen: Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Flash-Umleitung".

- Standardmäßig ist die Flash-Umleitung aktiviert. Zum Überschreiben dieses Standardverhaltens für einzelne Webseiten und Flash-Instanzen verwenden Sie die Einstellung Flash-URL-Kompatibilitätsliste.
- Flash - intelligentes Fallback: erkennt kleinere Flash-Filme (z. B. Werbefilme) und gibt sie auf dem Server wieder, anstatt sie zur Wiedergabe auf das Benutzergerät umzuleiten. Diese Optimierung verursacht keine Unterbrechung oder Fehler beim Laden der Webseite oder der Flash-Anwendung. Standardmäßig ist "Flash - intelligentes Fallback"aktiviert. Zum Umleiten aller Flash-Inhalte für die Wiedergabe auf dem Benutzergerät deaktivieren Sie diese Richtlinieneinstellung. Einige Flash-Inhalte werden möglicherweise nicht erfolgreich umgeleitet.
- URL-Liste für serverseitigen Flash-Inhaltsabruf: Mit dieser Liste können Sie die Websites angeben, deren Flash-Inhalte auf den Server heruntergeladen und dann zur Wiedergabe zum Benutzergerät gesendet werden sollen. (Bei der standardmäßigen Flash-Umleitung werden Flash-Inhalte per clientseitigem Abruf direkt auf das Benutzergerät heruntergeladen und dort wiedergegeben.) Diese Einstellung ist zwingend mit der Einstellung Serverseitigen Inhaltsabruf aktivieren auf dem Benutzergerät verknüpft und ist hauptsächlich für Intranetsites und interne Flash-Anwendungen vorgesehen. Weitere Informationen finden Sie weiter unten. Sie funktioniert auch mit den meisten Websites und kann verwendet werden, wenn das Benutzergerät keinen direkten Internetzugang hat (z. B. wenn der XenApp- oder XenDesktop-Server die Verbindung herstellt).

  Hinweis: Beim serverseitigen Inhaltsabruf werden keine Flash-Anwendungen unterstützt, die Real Time Messaging Protocol (RTMP) verwenden; stattdessen wird serverseitiges Rendering verwendet, bei dem HTTP und HTTPS unterstützt werden.
- Flash-URL-Kompatibilitätsliste: Gibt an, wo Flash-Inhalte von aufgelisteten Websites wiedergegeben werden: auf dem Benutzergerät, auf dem Server oder ob die Wiedergabe blockiert wird.
- Flash-Hintergrundfarbenliste: Hiermit können Sie die Farben von Webseiten und Flash-Instanzen aufeinander abstimmen, wodurch die Darstellung der Webseite bei Flash-Umleitung verbessert wird.

Konfigurieren der Flash-Umleitung auf dem Benutzergerät

Installieren Sie Citrix Receiver und Adobe Flash Player auf dem Benutzergerät. Es ist keine weitere Konfiguration auf dem Benutzergerät erforderlich.

Sie können die Standardeinstellungen mit Active Directory-Gruppenrichtlinienobjekten ändern. Importieren und fügen Sie die administrative Vorlage für HDX MediaStream Flash-Umleitung - Client (HdxFlashClient.adm) hinzu, die im folgenden Verzeichnis verfügbar ist:

- 32-Bit-Computer: %Programme%\Citrix\ICA Client\Configuration\Sprache
- 64-Bit-Computer: %Programme (x86)%\Citrix\ICA Client\Configuration\Sprache

Die Einstellungen werden unter Administrative Vorlagen > Klassische administrative Vorlage (ADM) > HDX MediaStream Flash-Umleitung - Client aufgeführt. Weitere Informationen über Gruppenrichtlinienobjekten und Vorlagen finden Sie in der Dokumentation zu Microsoft Active Directory.

Ändern der Verwendung der Flash-Umleitung:

Zusammen mit serverseitigen Einstellungen steuert die Richtlinie HDX MediaStream-Flash-Umleitung auf dem Benutzergerät, ob Adobe Flash-Inhalte für die lokale Wiedergabe auf dem Benutzergerät umgeleitet werden. Standardmäßig ist die Flash-Umleitung aktiviert und ermittelt mit der intelligenten Netzwerkerkennung, wann Flash-Inhalte auf dem Benutzergerät wiedergegeben werden.

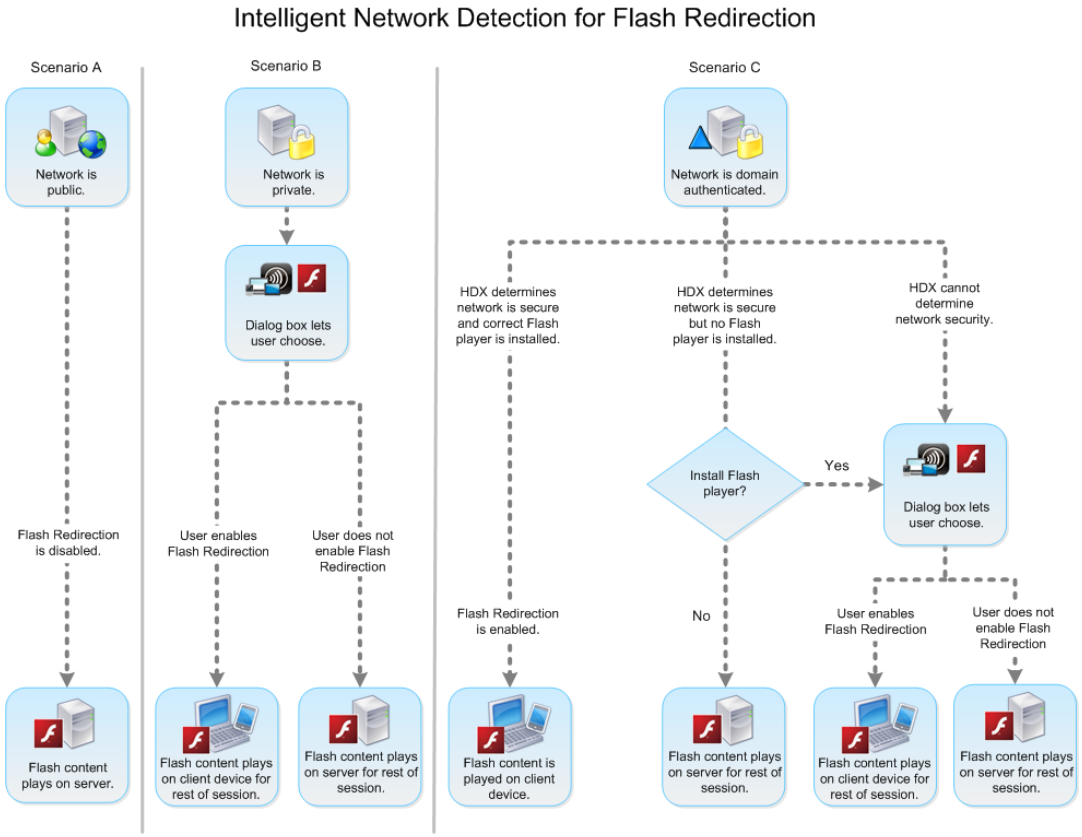
Wenn keine Konfiguration festgelegt ist und Desktop Lock verwendet wird, wird die Flash-Umleitung auf dem Benutzergerät standardmäßig aktiviert.

Gehen Sie zum Ändern der Verwendung von Flash-Umleitung bzw. zum Deaktivieren der Flash-Umleitung auf dem Benutzergerät wie folgt vor:

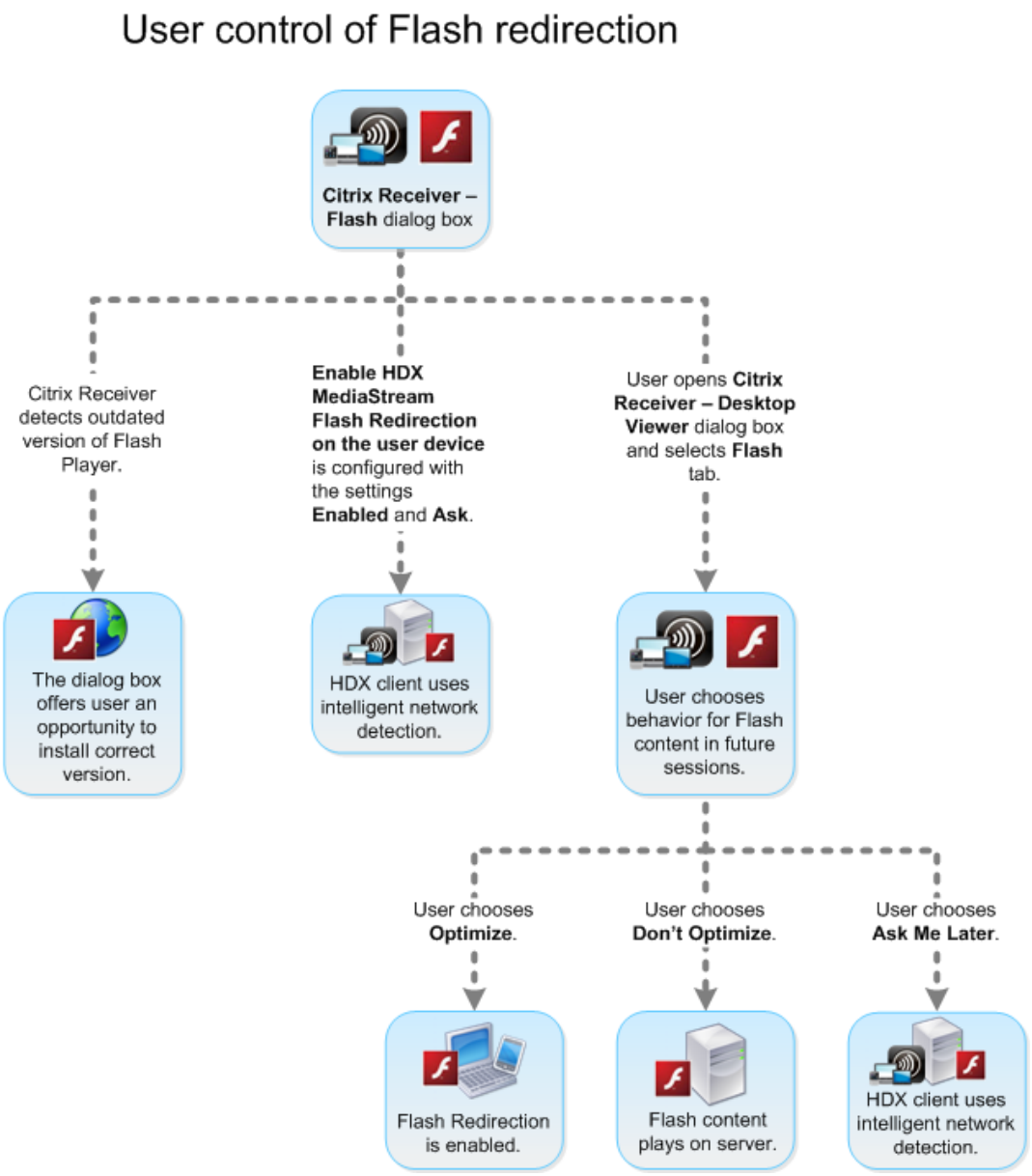
1. Wählen Sie aus der Einstellungsliste den Eintrag HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie “Nicht konfiguriert”, “Aktiviert”(Standardeinstellung) oder “Deaktiviert”.
3. Wenn Sie Aktiviert eingestellt haben, wählen Sie eine Option unter HDX MediaStream Flash-Umleitung verwenden aus:

    - Die Einstellung Nur zweite Generation dient dazu, die aktuelle Flash-Umleitung zu verwenden, wenn die erforderliche Konfiguration vorhanden ist bzw. auf serverseitige Wiedergabe umzuschalten, wenn dies nicht der Fall ist.
    - Bei Wahl von Immer wird die Flash-Umleitung immer verwendet. Flash-Inhalte werden auf dem Benutzergerät wiedergegeben.
    - Bei Wahl von Nie wird die Flash-Umleitung nie verwendet. Flash-Inhalte werden auf dem Server wiedergegeben.
    - Mit Fragen (Standardeinstellung) wird festgelegt, dass die Entscheidung, ob Flash-Umleitung verwendet wird, durch intelligente Netzwerkerkennung zur Beurteilung der Sicherheitsstufe des clientseitigen Netzwerks erfolgt. Wenn die Sicherheit des Netzwerks nicht bestimmt werden kann, erhält der Benutzer die Entscheidung über die Flash-Umleitung. Es erscheint eine Aufforderung, die Flash-Umleitung zu aktivieren bzw. zu deaktivieren.

Die folgende Abbildung zeigt, wie die Flash-Umleitung für verschiedene Netzwerktypen verarbeitet wird.



Benutzer können die intelligente Netzwerkerkennung über das Dialogfeld Citrix Receiver - Desktop Viewer-Einstellungen mit der Option Optimieren überschreiben oder über die Option Nicht optimieren auf der Registerkarte Flash. Welche Optionen zur Auswahl stehen, hängt davon ab, wie die Flash-Umleitung auf dem Benutzergerät konfiguriert ist (siehe folgende Abbildung).



Synchronisieren der clientseitigen HTTP-Cookies mit den serverseitigen HTTP-Cookies:

Die Option zur serverseitigen HTTP-Cookie-Synchronisierung ist standardmäßig deaktiviert. Aktivieren Sie die Synchronisierung, um HTTP-Cookies vom Server herunterzuladen. Diese HTTP-Cookies werden dann für den clientseitigen Inhaltsabruf verwendet und können bei Bedarf von Sites mit Flash-Inhalten gelesen werden.

> **Hinweis:**
>
> Clientseitige Cookies werden bei der Synchronisierung nicht ersetzt; sie sind weiterhin verfügbar, wenn die Synchronisierungsrichtlinie zu einem späteren Zeitpunkt deaktiviert wird.

1. Wählen Sie aus der Einstellungsliste die Option Synchronisierung der clientseitigen HTTP-

Cookies mit den serverseitigen HTTP-Cookies aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert (Standardeinstellung).

Aktivieren des serverseitigen Inhaltsabrufs:

Bei der standardmäßigen Flash-Umleitung werden Flash-Inhalte direkt auf das Benutzergerät heruntergeladen und dort wiedergegeben. Bei Aktivierung des serverseitigen Inhaltsabrufs werden die Flash-Inhalte zum Server heruntergeladen und dann an das Benutzergerät gesendet. Die Inhalte werden auf dem Benutzergerät wiedergegeben, sofern keine Richtlinie mit höherer Priorität dies verhindert, z. B. wenn eine Site durch die Richtlinieneinstellung Flash-URL-Kompatibilitätsliste blockiert wird.

Serverseitiger Inhaltsabruf wird häufig verwendet, wenn das Benutzergerät eine Verbindung zu internen Sites über NetScaler Gateway herstellt und wenn das Benutzergerät keinen direkten Internetzugang hat.

> **Hinweis:**
>
> Der serverseitige Inhaltsabruf unterstützt keine Flash-Anwendungen, die Real Time Messaging Protocol (RTMP) verwenden. Stattdessen wird die serverseitige Wiedergabe für solche Sites verwendet.

Die Flash-Umleitung unterstützt drei Aktivierungsoptionen für den serverseitigen Inhaltsabruf. Zwei dieser Optionen umfassen das Zwischenspeichern serverseitiger Inhalte auf dem Benutzergerät, wodurch die Leistung verbessert wird, da wiederverwendeter Inhalt bereits wiedergabebereit auf dem Benutzergerät verfügbar ist. Der Inhalt dieses Caches wird separat von anderen HTTP-Inhalten auf dem Benutzergerät gespeichert.

Der Fallback auf serverseitigen Inhaltsabruf wird automatisch gestartet, wenn eine der Aktivierungsoptionen ausgewählt ist und der clientseitige Abruf von SWF-Dateien fehlschlägt.

Zum Aktivieren des serverseitigen Inhaltsabrufs müssen auf dem Clientgerät und dem Server Einstellungen festgelegt sein.

1. Wählen Sie in der Einstellungsliste den Eintrag Serverseitigen Inhaltsabruf aktivieren und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie Nicht konfiguriert, Aktiviert oder Deaktiviert (Standardeinstellung). Wenn Sie diese Einstellung aktivieren, wählen Sie eine der Optionen aus der Liste Serverseitiger Inhaltsabrufstatus:

Option	Beschreibung
Deaktiviert	Deaktiviert serverseitigen Inhaltsabruf und überschreibt die Einstellung URL-Liste für serverseitigen Flash-Inhaltsabruf auf dem Server. Fallback auf serverseitigen Inhaltsabruf ist auch deaktiviert.
Aktiviert	Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar, aber der Inhalt wird nicht zwischengespeichert.
Aktiviert (permanentes Caching)	Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar. Über serverseitigen Inhaltsabruf erhaltener Inhalt wird auf dem Benutzergerät zwischengespeichert und von Sitzung zu Sitzung gespeichert.
Aktiviert (temporäres Caching)	Aktiviert serverseitigen Inhaltsabruf für Webseiten und Flash-Anwendungen, die in der URL-Liste für serverseitigen Flash-Inhaltsabruf angegeben sind. Fallback auf serverseitigen Inhaltsabruf ist verfügbar. Über serverseitigen Inhaltsabruf erhaltener Inhalt wird auf dem Benutzergerät zwischengespeichert und am Ende der Sitzung gelöscht.

3. Aktivieren Sie auf dem Server die Richtlinieneinstellung URL-Liste für serverseitigen Flash-Inhaltsabruf und füllen Sie sie mit Ziel-URLs.

Umleiten der Benutzergeräte für clientseitigen Inhaltsabruf an andere Server:

Sie können einen Versuch, Flash-Inhalte abzurufen, mit der Einstellung URL-Neuschreibregeln für clientseitigen Inhaltsabruf umleiten. Hierbei handelt es sich um ein Feature der Flash-Umleitung der zweiten Generation. Bei der Konfiguration dieses Features geben Sie zwei URL-Schemas an. Wenn das Benutzergerät versucht, Inhalte von einer Webseite abzurufen, die dem ersten Schema (dem URL-Übereinstimmungsschema) entspricht, werden sie an eine Webseite weitergeleitet, die mit dem

zweiten Schema festgelegt wurde (dem Ersetzungsschema).

Mit dieser Einstellung können Sie die Auswirkungen von Inhaltsübermittlungsnetzwerken (Content Delivery Networks, CDN) kompensieren. Manche Webseiten, die Flash-Inhalte bereitstellen, verwenden CDN-Umleitung, damit Benutzer den Inhalt vom nächstgelegenen Server in einer Gruppe von Servern, auf denen derselbe Inhalt zur Verfügung steht, abrufen können. Bei der Verwendung des clientseitigen Inhaltsabrufs der Flash-Umleitung wird der Flash-Inhalt vom Benutzergerät abgerufen, während der Rest der Webseite, auf der sich der Flash-Inhalt befindet, vom Server abgerufen wird. Wenn CDN verwendet wird, wird die Serveranfrage an den am nächsten gelegenen Server geleitet und die Benutzergerätanfrage geht an denselben Standort. Dies möglicherweise nicht der Speicherort ist, der dem Benutzergerät am nächsten liegt; je nach Entfernung, kann eine sichtbare Verzögerung zwischen dem Laden der Webseite und die Wiedergabe von Flash-Inhalten entstehen.

1. Wählen Sie in der Einstellungsliste den Eintrag URL-Neuschreibregeln für clientseitigen Inhaltsabruf und klicken Sie auf Richtlinieneinstellung.
2. Wählen Sie “Nicht konfiguriert”, “Aktiviert”oder “Deaktiviert”. Nicht konfiguriert ist der Standardwert; Deaktiviert bewirkt, dass alle URL-Neuschreibregeln des nächsten Schrittes ignoriert werden.
3. Wenn Sie die Einstellung aktivieren, klicken Sie auf Anzeigen. Verwenden Sie die Perl-Syntax für reguläre Ausdrücke und geben Sie das URL-Schema im Feld “Wert”und das neu geschriebene URL-Format im Feld “Wert”ein.

Angabe erforderlicher Mindestversionen für Flash-Umleitung

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Sie können Registrierungseinstellungen hinzufügen, um die erforderliche Mindestversion für die Flash-Umleitung für Clientgeräte festzulegen, die auf VDAs mit Citrix Receiver für Windows oder Citrix Receiver für Linux zugreifen. Dieses Sicherheitsfeature gewährleistet, dass keine veraltete Flash-Version verwendet wird.

ServerFlashPlayerVersionMinimum ist ein Zeichenfolgenwert, der die erforderliche Mindestversion des Flash Players auf dem ICA-Server (VDA) angibt.

ClientFlashPlayerVersionMinimum ist ein Zeichenfolgenwert, der die erforderliche Mindestversion des Flash Players auf dem ICA-Client (Citrix Receiver) angibt.

Diese Versionszeichenfolgen können als “10”, “10.2”oder “10.2.140”angegeben werden. Nur die Hauptversions-, Nebenversions- und Buildnummern werden verglichen. Die Revisionsnummer wird ignoriert. Bei der Angabe von “10”als Versionszeichenfolge mit ausschließlicher Angabe der Hauptversionsnummer wird für die Nebenversions- und Buildnummer von Null ausgegangen.

FlashPlayerVersionComparisonMask ist ein DWORD-Wert, der, wenn auf 0 festgelegt wird, den Vergleich der Flash Player-Version auf dem ICA-Client mit der auf dem ICA-Server deaktiviert. Die Vergleichsmaske hat auch andere Werte, die jedoch nicht verwendet werden sollten, da sich die Bedeutung jeder Maske mit einem Wert ungleich 0 ändern kann. Es wird empfohlen, die Vergleichsmaske für die gewünschten Clients nur auf 0 festzulegen. Es ist nicht empfehlenswert, die Vergleichsmaske unter den clientagnostischen Einstellungen festzulegen. Wenn keine Vergleichsmaske festgelegt ist, erfordert die Flash-Umleitung auf dem ICA-Client dieselbe Flash Player-Version wie auf dem ICA-Server oder eine höhere Version. Hierfür wird nur die Hauptversionsnummer verglichen.

Für die Umleitung müssen neben der Prüfung anhand der Vergleichsmaske die Prüfungen auf Mindestversion auf Client und Server bestanden werden.

Der Unterschlüssel “ClientID0x51”gibt Citrix Receiver für Linux an. Der Unterschlüssel “ClientID0x1” gibt Citrix Receiver für Windows an. Der Name des Unterschlüssels entsteht durch Anfügen der hexadezimalen Clientprodukt-ID (ohne führende Nullen) an die Zeichenfolge “ClientID”.

Beispiel für eine 32-Bit-VDA-Registrierungskonfiguration:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] clientagnostische Einstellungen

“ClientFlashPlayerVersionMinimum”=”13.0”Mindestversion für ICA-Client “ServerFlashPlayerVersionMinimum”=”13.0”Mindestversion für ICA-Server [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
Windows-ICA-Client-Einstellungen

“ClientFlashPlayerVersionMinimum”=”16.0.0”Gibt die Flash-Player-Mindestversion für den Windows-Client an [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x5
Linux-ICA-Clienteinstellungen

“FlashPlayerVersionComparisonMask”=dword:00000000 Deaktiviert den Versionsvergleich für den Linux-Client (Prüfung, um festzustellen, ob die Flash Player-Version auf dem Client neuer ist als auf dem Server) “ClientFlashPlayerVersionMinimum”=”11.2.0”Flash Player-Mindestversion für Linux-Client.

Beispiel für eine 64-Bit-VDA-Registrierungskonfiguration:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

“ClientFlashPlayerVersionMinimum”=”13.0”“ServerFlashPlayerVersionMinimum”=”13.0”[HKEY_LOCAL_MACHINE

“ClientFlashPlayerVersionMinimum”=”16.0.0”[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMed

“FlashPlayerVersionComparisonMask”=dword:00000000 “ClientFlashPlayerVersionMinimum”=” 11.2.0”

HTML5-Multimediaumleitung

August 18, 2021

Die HTML5-Multimediaumleitung ist eine Erweiterung der Multimediaumleitung von HDX Mediastream für HTML5-Audio und -Video. Aufgrund der Zunahme online zur Verfügung gestellter Multimediainhalte (insbesondere für mobile Geräte) haben Browseranbieter effizientere Methoden für die Präsentation von Audio und Video entwickelt.

Der bisherige Standard Flash erfordert ein Plug-In, funktioniert nicht auf allen Geräten und verursacht auf Mobilgeräten einen erhöhten Akkuverbrauch. Youtube, Netflix und neuere Browserversionen von Mozilla, Google und Microsoft verwenden HTML5 als neuen Standard.

HTML5-basiertes Multimedia bietet gegenüber proprietären Plug-Ins zahlreiche Vorteile:

- Unternehmensunabhängige Standards (W3C)
- Vereinfachter DRM-Workflow (Verwaltung digitaler Rechte)
- Bessere Leistung ohne die bei Plug-Ins bestehenden Sicherheitsproblemen

Progressive Downloads mit HTTP

Progressiver Download ist eine HTTP-basierte Pseudostreamingmethode, die HTML5 unterstützt. Bei einem progressiven Download gibt der Browser eine einzelne Datei wieder (die in einer einzigen Qualität codiert ist), während diese von einem HTTP-Webserver heruntergeladen wird. Das Video wird beim Empfang auf der Festplatte gespeichert und von dort abgespielt. Wenn das Video erneut angesehen wird, kann es aus dem Cache geladen werden.

Ein Beispiel für progressiven Download finden Sie auf der Testseite für die HTML5-Videoumleitung. Untersuchen Sie mit den Entwicklertools des Browsers das Videoelement der Webseite auf dessen Quelle (ein MP4-Containerformat) im HTML5-Video-Tag:

```
<video src="https://www.citrix.com/content/dam/citrix61/en_us/images/
offsite/html5-redirect.mp4"controls=""style="width:800px;"></video>
```

Vergleich zwischen HTML5 und Flash

Feature	HTML5	Flash
Proprietärer Player erforderlich	Nein	Ja
Läuft auf Mobilgeräten	Ja	Auf einigen
Wiedergabegeschwindigkeit auf unterschiedlichen Plattformen	Hoch	Langsam
Von iOS unterstützt	Ja	Nein
Ressourcennutzung	Weniger	Mehr
Schnelleres Laden	Ja	Nein

Anforderungen

Citrix unterstützt nur die Umleitung für progressive Downloads im MP4-Format. WebM und Adaptive Bitrate-Streamingtechnologien wie DASH/HLS werden nicht unterstützt.

Citrix unterstützt Folgendes:

- Serverseitige Wiedergabe
- Serverseitiger Abruf/clientseitige Wiedergabe
- Clientseitiger Abruf und clientseitige Wiedergabe

Die Steuerung erfolgt über Richtlinien. Weitere Informationen finden Sie unter Richtlinieneinstellungen für Multimedia.

Mindestversionen von Citrix Receiver:

- Citrix Receiver für Windows 4.5
- Citrix Receiver für Linux 13.5

VDA-Mindestbrowserversion und Windows-Betriebssystemversion/-Build/-SP:

- **Internet Explorer 11.0**
  - Windows 10 x86 (1607 RS1) und x64 (1607 RS1)
  - Windows 7 x86 und x64
  - Windows Server 2016 RTM 14393 (1607)
  - Windows Server 2012 R2
  - Windows Server 2008 R2
- **Firefox 47:** Fügen Sie die Zertifikate manuell in den Firefox-Zertifikatspeicher ein oder konfigurieren Sie die Firefox-Suche für Zertifikate aus einem vertrauenswürdigen Windows-

Zertifikatspeicher. Weitere Informationen finden Sie unter https://wiki.mozilla.org/CA:AddRootToFirefox

  - Windows 10 x86 (1607 RS1) und x64 (1607 RS1)
  - Windows 7 x86 und x64
  - Windows Server 2016 RTM 14393 (1607)
  - Windows Server 2012 R2
  - Windows Server 2008 R2

- **Chrom 51**

  - Windows 10 x86 (1607 RS1) und x64 (1607 RS1)
  - Windows 7 x86 und x64
  - Windows Server 2016 RTM 14393 (1607)
  - Windows Server 2012 R2
  - Windows Server 2008 R2

Komponenten der HTML5-Videoumleitung

- **HdxVideo.js:** JavaScript-Hook, der Videobefehle auf der Website abfängt. HdxVideo.js kommuniziert mit WebSocketService über Secure WebSockets (SSL/TLS).
- **WebSocket-SSL-Zertifikate**

  - Für die Zertifizierungsstelle (root): **Citrix XenApp/XenDesktop HDX In-Product-Zertifizierungsstelle** (C = USA; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc .; OU = XenApp / XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product-Zertifizierungsstelle)
    Speicherort: Zertifikate (Lokaler Computer)> Vertrauenswürdige Stammzertifizierungsstellen> Zertifikate.
  - Für die Endentität (Blatt): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    Speicherort: Zertifikate (Lokaler Computer)> Eigene Zertifikate > Zertifikate.

- **WebSocketService.exe** wird im lokalen System für SSL-Beendigung und Benutzersitzungszuordnung ausgeführt. TLS Secure WebSocket überwacht auf 127.0.0.1 an Port 9001.
- **WebSocketAgent.exe** wird in der Sitzung des Benutzers ausgeführt und gibt das Video gemäß den WebSocketService-Befehlen wieder.

Aktivieren der HTML5-Videoumleitung

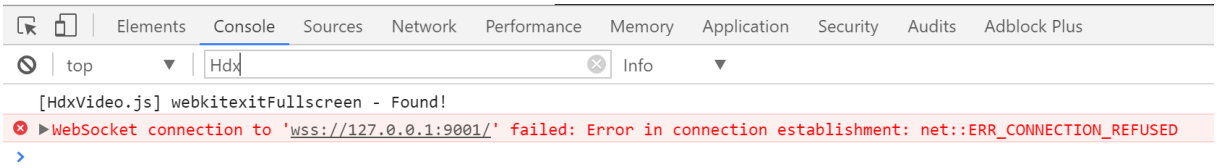
In diesem Release ist dieses Feature nur für Webseiten verfügbar, die unter Ihrer Kontrolle stehen. Die Aktivierung erfordert das Hinzufügen der JavaScript-Datei HdxVideo.js (auf dem XenDesktop/XenApp-Installationsmedium enthalten) zu Webseiten mit HTML5-Multimediainhalt. Beispiel: Videos auf einer internen Website.

Websites wie youtube.com, die auf adaptive Bitratetechnologien bauen, werden nicht unterstützt (z. B. HTTP Live Streaming (HLS) und Dynamic Adaptive Streaming über HTTP (DASH)).

Weitere Informationen finden Sie unter Richtlinieneinstellungen für Multimedia.

Tipps zur Problembehandlung

Bei dem Versuch, HdxVideo.js auszuführen, können Fehler auftreten. Kann das JavaScript nicht geladen werden, schlägt die HTML5-Umleitung fehl. Prüfen Sie mithilfe der Browser-Entwicklertools HdxVideo.js auf Fehler. Beispiel:



Windows Media-Umleitung

August 18, 2021

Die Windows Media-Umleitung steuert und optimiert die Art und Weise, mit der Streamingaudio und -video von Servern bereitgestellt wird. Durch Wiedergabe der Laufzeitdateien von Medieninhalten auf dem Client statt auf dem Server werden die Bandbreitenanforderungen beim Abspielen von Multimediadateien verringert. Windows Media-Umleitung verbessert die Leistung von Windows Media Player und anderen kompatiblen Playern, die auf virtuellen Windows-Desktops ausgeführt werden.

Wenn die Anforderungen des clientseitigen Windows Media-Inhaltsabrufs nicht erfüllt sind, erfolgt automatisch der serverseitige Inhaltsabruf. Diese Methode ist für die Benutzer unsichtbar. Sie können mit XenDesktop Collector einen CDF-Trace (Citrix Diagnostics Facility) von HostMMTransport.dll durchführen, um zu ermitteln, welche Methode verwendet wird.

Die Windows Media-Umleitung fängt die Medienpipeline auf dem Hostserver ab, erfasst Mediendaten im ursprünglichen, komprimierten Format und leitet den Inhalt an das Clientgerät um. Auf dem Clientgerät wird die Medienpipeline zum Dekomprimieren und Wiedergeben der vom Hostserver empfangenen Mediendaten neu erstellt. Die Windows Media-Umleitung funktioniert gut auf Clientgeräten

mit Windows-Betriebssystem. Solche Geräte besitzen das erforderliche Multimedia-Framework zum Neuaufbau der Medienpipeline in der Form, wie diese auf dem Hostserver vorhanden war. Linux-Clients verwenden ähnliche Open-Source-Frameworks für den Neuaufbau der Medienpipeline.

Die Richtlinieneinstellung **Windows Media-Umleitung** steuert dieses Feature und ist standardmäßig auf **Zugelassen** festgelegt. Normalerweise erhöht diese Einstellung die Audio- und Videoqualität von vom Server stammenden Medien auf ein mit einer lokalen Wiedergabe vergleichbares Niveau. In Ausnahmefällen kann die Wiedergabe von Medien mit der Windows Media-Umleitung schlechter scheinen, als bei Verwendung der ICA-Komprimierung und von regulärem Audio. Sie können das Feature deaktivieren, indem Sie einer Richtlinie die Einstellung **Windows Media-Umleitung** hinzufügen und den Wert auf **Nicht zugelassen** festlegen.

Weitere Informationen zu den Richtlinieneinstellungen finden Sie unter Einstellungen der Richtlinie "Multimedia".

Allgemeine Inhaltsumleitung

April 30, 2019

Bei der Inhaltsumleitung können Sie steuern, wie die Benutzer auf die Informationen zugreifen: über die auf den Servern veröffentlichten Anwendungen oder über lokal auf den Benutzergeräten ausgeführte Anwendungen.

Clientordnerumleitung

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Windows-Desktopgerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Host-zu-Client-Umleitung

Ziehen Sie die Host-zu-Client-Umleitung für bestimmte ungewöhnliche Anwendungsfälle in Betracht. Normalerweise sind andere Formen der Inhaltsumleitung besser. Diese Umleitungsart wird nur auf Serverbetriebssystem-VDAs (nicht auf Desktopbetriebssystem-VDAs) unterstützt.

Lokaler App-Zugriff und URL-Umleitung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert, ohne dass ein Wechsel zwischen Computern nötig ist.

Überlegungen zu USB und Clientlaufwerk

HDX-Technologie bietet **generische USB-Umleitung** für Spezialgeräte ohne optimierte Unterstützung oder wenn diese ungeeignet ist.

Verwandte Informationen

- Clientordnerumleitung
- Host-zu-Client-Umleitung
- Lokaler App-Zugriff und URL-Umleitung
- Überlegungen zu USB und Clientlaufwerk
- Multimedia

Clientordnerumleitung

July 1, 2019

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wird auf dem Server nur die Clientlaufwerkzuordnung aktiviert, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner statt des kompletten Dateisystems auf dem Benutzergerät werden als UNC-Links in den Sitzungen angezeigt. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt.

Die Clientordnerumleitung wird nur auf Windows-Desktopbetriebssystemmaschinen unterstützt.

Die Clientordnerumleitung für ein externes USB-Laufwerk wird beim Trennen und Wiederverbinden des Geräts nicht gespeichert.

Aktivieren Sie die Clientordnerumleitung auf dem Server. Geben Sie dann auf dem Clientgerät an, welche Ordner umgeleitet werden sollen (die Anwendung, die Sie zur Angabe der Clientordneroptionen verwenden, ist in diesem Release von Citrix Receiver enthalten).

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des

> Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. Auf dem Server:
    a) Erstellen Sie einen Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
    b) Erstellen Sie einen Wert für REG_DWORD.
        - Name: CFROnlyModeAvailable
        - Typ: REG_DWORD
        - Daten: Stellen Sie 1 ein.
2. Auf dem Benutzergerät:
    a) Stellen Sie sicher, dass die neueste Version von Citrix Receiver installiert ist.
    b) Starten Sie vom Installationsverzeichnis von Citrix Receiver aus CtxCFRUI.exe.
    c) Wählen Sie das Optionsfeld "Benutzerdefiniert"und fügen Sie Ordner hinzu oder bearbeiten oder entfernen Sie Ordner.
    d) Trennen Sie die Sitzungen und stellen Sie dann neue Verbindungen her, damit die Einstellung wirksam wird.

Host-zu-Client-Umleitung

August 18, 2021

Bei der Inhaltsumleitung können Sie steuern, wie die Benutzer auf die Informationen zugreifen: über die auf den Servern veröffentlichten Anwendungen oder über lokal auf den Benutzergeräten ausgeführte Anwendungen.

Host-zu-Client-Umleitung ist eine Art der Inhaltsumleitung. Sie wird nur auf Serverbetriebssystem-VDAs (nicht auf Desktopbetriebssystem-VDAs) unterstützt.

- Wenn die Host-zu-Client-Umleitung aktiviert ist, werden URLs auf dem Server-VDA abgefangen und an das Benutzergerät gesendet. Die URLs werden im Webbrowser oder Multimedia-Player auf dem Benutzergerät geöffnet.
- Wenn Sie die Host-zu-Client-Umleitung aktivieren und ein Benutzergerät keine Verbindung zu einer URL herstellen kann, wird die URL an den Server-VDA zurückgeleitet.
- Ist die Host-zu-Client-Umleitung deaktiviert, öffnen die Benutzer die URLs mit Webbrowsern oder Multimedia-Playern auf dem Server-VDA.
- Wenn Sie die Host-zu-Client-Umleitung aktivieren, können Benutzer sie nicht deaktivieren.

Die Host-zu-Client-Umleitung wurde früher **Server-zu-Client-Umleitung** genannt.

Einsatz der Host-zu-Client-Umleitung

Der Einsatz der Host-zu-Client-Umleitung ist in bestimmten –allerdings seltenen –Fällen aus Leistungs-, Kompatibilitäts- oder Konformitätsgründen zu empfehlen. Normalerweise sind andere Formen der Inhaltsumleitung besser.

Leistung:

Sie können die Host-zu-Client-Umleitung zur Leistungssteigerung einsetzen, sodass auf den Benutzergeräten installierte Anwendungen den Vorzug vor denen auf dem VDA erhalten.

Die Host-zu-Client-Umleitung verbessert die Leistung nur unter bestimmten Bedingungen, da der VDA bereits Adobe Flash- und andere Arten von Multimediainhalten optimiert. Vor Einsatz der Host-zu-Client-Umleitung sollten Sie zunächst andere Methoden (Richtlinieneinstellungen, siehe Tabellen weiter unten) in Betracht ziehen. Diese Einstellungen bieten mehr Flexibilität und normalerweise eine bessere Benutzererfahrung, insbesondere bei leistungsschwächeren Geräten.

Kompatibilität:

Sie können die Host-zu-Client-Umleitung für Kompatibilitätszwecke in folgenden Fällen verwenden:

- Für Inhalte anderen Typs als HTML oder Multimedia (z. B. einen benutzerdefinierten URL-Typ).
- Für ältere Medienformate (z. B. Real Media), die vom Multimedia-Player des VDAs mit Multimediaumleitung nicht unterstützt werden.
- Die für den Inhaltstyp benötigte Anwendung wird nur von wenigen Benutzern verwendet und ist auf deren Geräten bereits installiert.
- Der VDA hat keinen Zugriff auf bestimmte Websites (beispielsweise interne Websites einer anderen Organisation).

Konformität:

Sie können die Host-zu-Client-Umleitung für Konformitätszwecke in folgenden Fällen verwenden:

- Der Lizenzvertrag für die Anwendung oder den Inhalt lässt keine Veröffentlichung über den VDA zu.
- Eine Organisationsrichtlinie verbietet das Hochladen eines Dokuments auf den VDA.

Einige Situationen kommen in komplexen Umgebungen, oder wenn Benutzergerät und VDA verschiedenen Organisationen angehören, eher vor.

Überlegungen zu Benutzergeräten

Eine Umgebung kann viele verschiedene Benutzergerätetypen enthalten.

Benutzergerät	Szenario	Ansatz der Inhaltsumleitung
Tablet	-	Beliebig (siehe nächsten Tabelle)
Laptop	-	Beliebig (siehe nächsten Tabelle)
Desktop-PC	Benutzer verwenden viele verschiedene, auf den Benutzergeräten installierte Anwendungen.	Beliebig (siehe nächsten Tabelle)
Desktop-PC	Benutzer verwenden nur einige auf den Benutzergeräten installierte Anwendungen.	Lokaler App-Zugriff
Desktop-PC	Benutzer verwenden keine auf den Benutzergeräten installierten Anwendungen.	Multimediaumleitung und/oder Flash-Umleitung
Desktopgerät	Hersteller unterstützt Multimedia- und/oder Flash-Umleitung	Multimediaumleitung und/oder Flash-Umleitung
Thin Client	Hersteller unterstützt Multimedia-, Flash- und Host-zu-Client-Umleitung.	Beliebig (siehe nächsten Tabelle)
Zero Client	Hersteller unterstützt Multimedia- und/oder Flash-Umleitung	Multimediaumleitung und/oder Flash-Umleitung

Wählen Sie anhand der folgenden Beispiele eine geeignete Inhaltsumleitungsmethode.

URL-Link	Szenario	Ansatz der Inhaltsumleitung
Webseite oder Dokument	Der VDA hat keinen Zugriff auf die URL.	Host-zu-Client-Umleitung
Webseite	Die Webseite enthält Adobe Flash-Inhalte.	Flash-Umleitung
Multimediadatei oder Stream	Der VDA hat einen kompatiblen Multimedia-Player.	Multimediaumleitung
Multimediadatei oder Stream	Der VDA hat keinen kompatiblen Multimedia-Player.	Host-zu-Client-Umleitung

URL-Link	Szenario	Ansatz der Inhaltsumleitung
Dokument	Der VDA hat keine Anwendung für den Dokumenttyp.	Host-zu-Client-Umleitung
Dokument	Dokument nicht auf Benutzergeräte herunterladen	Keine Umleitung
Dokument	Dokument nicht auf den VDA hochladen	Host-zu-Client-Umleitung
Benutzerdefinierter URL-Typ	Der VDA hat keine Anwendung für den benutzerdefinierten URL-Typ.	Host-zu-Client-Umleitung

Die Host-zu-Client-Umleitung wird von Citrix Receiver für Windows, Citrix Receiver für Mac, Citrix Receiver für Linux, Citrix Receiver für HTML5 und Citrix Receiver für Chrome unterstützt.

Zur Verwendung der Host-zu-Client-Umleitung muss auf dem Benutzergerät ein Webbrowser, ein Multimedia-Player oder eine andere, für den Inhalt geeignete Anwendung vorliegen. Handelt es sich bei einem Benutzergerät um ein Desktopgerät, einen Thin Client oder einen Zero Client, vergewissern Sie sich, dass es über geeignete Anwendungen verfügt und ausreichend Leistung bietet.

Für den lokalen App-Zugriff aktivierte Benutzergeräte verwenden eine andere Inhaltsumleitungsmethode und erfordern keine Host-zu-Client-Umleitung.

Sie können Citrix Richtlinien verwenden, um eine Host-zu-Client-Inhaltsumleitung auf ungeeignete Geräte zu verhindern.

Auswirkungen der Host-zu-Client-Umleitung auf die Benutzer

Die Host-zu-Client-Umleitung wird für folgende URLs verwendet:

- URLs, die als Hyperlink in einer Anwendung eingebettet sind (z. B. in einer E-Mail oder einem Dokument)
- URLs, die über ein Menü oder Dialogfeld einer VDA-Anwendung ausgewählt werden, wenn die Anwendung die Windows-API ShellExecuteEx verwendet
- URLs, die in das Windows-Fenster "Ausführen"eingegeben werden

Die Host-zu-Client-Umleitung wird nicht für URLs in einem Webbrowser verwendet (URLs in Webseiten oder in der Adressleiste eingegebene URLs).

> **Hinweis:**

> Wenn Benutzer ihren Standardwebbrowser auf dem VDA ändern (z. B. über "Standardprogramme festlegen"), kann dies die Host-zu-Client-Umleitung für Anwendungen stören.

Wenn die Host-zu-Client-Umleitung aktiviert ist, hängt es von der Konfiguration des Benutzergeräts für den URL- und Inhaltstyp ab, in welcher Anwendung eine URL geöffnet wird. Beispiel:

- Eine HTTP-URL mit HTML-Inhalt wird im Standardbrowser geöffnet.
- Eine HTTP-URL mit PDF-Inhalt wird entweder im Standardbrowser oder einer anderen Anwendung geöffnet.

Diese Benutzergerätekonfiguration wird nicht über die Host-zu-Client-Inhaltsumleitung gesteuert. Wenn Sie die Konfiguration von Benutzergeräten nicht steuern, erwägen Sie die Verwendung der Flash-Umleitung oder der Multimedia-Umleitung anstelle der Host-zu-Client-Umleitung.

URLs des folgenden Typs werden lokal auf Benutzergeräten geöffnet, wenn die Host-zu-Client-Umleitung aktiviert ist:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player und QuickTime)
- RTSPU (Real Player und QuickTime)
- PNM (Legacy-Real Player)
- MMS (Microsoft Media Format)

Sie können der Liste der URL-Typen für die Host-zu-Client-Umleitung URL-Typen (einschließlich benutzerdefinierter Typen) hinzufügen und sie aus dieser löschen.

Aktivieren der Host-zu-Client-Umleitung

Zum Aktivieren der Host-zu-Client-Umleitung müssen Sie zunächst eine Citrix Richtlinieneinstellung aktivieren.

Die Richtlinieneinstellung für die Host-zu-Client-Umleitung ist Teil der Einstellungen der Richtlinie Dateiumleitung. Diese Einstellung ist standardmäßig deaktiviert.

Außerdem müssen Sie möglicherweise, je nach VDA-Betriebssystem, Registrierungsschlüssel und die Gruppenrichtlinie für die Server-VDAs einrichten.

- Für Windows Server 2008 R2 SP1-VDAs müssen Sie weder Registrierungsschlüssel noch die Gruppenrichtlinie einrichten.
- Für VDAs unter Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016 müssen Sie Registrierungsschlüssel und die Gruppenrichtlinie einrichten.

> **Warnung**
>
> Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Registrierungsänderungen

1. Kopieren Sie den Text zwischen **Reg file start** und **Reg file end** unten und fügen Sie ihn in den Editor ein.
2. Speichern Sie die Editor-Datei mit **Speichern unter** unter Auswahl des Typs **Alle Dateien** und Eingabe des Namens **ServerFTA.reg**.
3. Verteilen Sie die Datei **ServerFTA.reg** mit der Active Directory-Gruppenrichtlinie auf die Server.

```
--  Reg file start --

Windows Registry Editor Version 5.00


[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]

@="\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"


[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]

@="ServerFTA"


[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

"ApplicationDescription"="Server FTA URL."

"ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.
   exe,0"

"ApplicationName"="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\
   URLAssociations]
```



```
27
28 "http"="ServerFTAHTML"
29
30 "https"="ServerFTAHTML"
31
32
33
34 [HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]
35
36 "Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"
37
38 -- Reg file end -- ---
```

Gruppenrichtlinienänderungen

Erstellen Sie eine XML-Datei. Kopieren Sie den Text zwischen **xml file start**und **xml file end** im Beispiel, fügen Sie ihn in die XML-Datei ein und speichern Sie die Datei unter dem Namen **ServerFTAdefaultPolicy.xml**.

```
1  -- xml file start --
2
3  <?xml version="1.0" encoding="UTF-8"?>
4
5  <DefaultAssociations>
6
7  <Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
       ServerFTA" />
8
9  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
10
11 </DefaultAssociations>
12
13 -- xml file end -- ---
```

Navigieren Sie in der aktuellen Gruppenrichtlinien-Verwaltungskonsole zu **Computerkonfiguration** > **Administrative Vorlagen** > **Windows-Komponenten** > **Datei-Explorer** > **Konfigurationsdatei für Standardzuordnungen festlegen** und geben Sie die zuvor erstellte Datei ServerFTAdefaultPolicy.xml an.

Ändern der URL-Typenliste für die Host-zu-Client-Umleitung

Zum Ändern der URL-Typenliste für die Host-zu-Client-Umleitung legen Sie auf dem Server-VDA den folgenden Registrierungsschlüssel fest:

Schlüssel: HKLM\Software\Wow6432Node\Citrix\SFTA

Zum Löschen von URL-Typen aus der Liste legen Sie DisableServerFTA und NoRedirectClasses fest:

Name: DisableServerFTA

Typ: REG_DWORD

Wert: 1

Name: NoRedirectClasses
Typ: REG_MULTI_SZ
Daten: Geben Sie eine beliebige Kombination der Werte "http", "https", "rtsp", "rtspu", "pnm"und "mms"ein. Geben Sie mehrere Werte auf separaten Zeilen an. Beispiel:

http

https

rtsp

Zum Hinzufügen von URL-Typen zu der Liste legen Sie ExtraURLProtocols fest:

Name: ExtraURLProtocols

Typ: REG_MULTI_SZ

Daten: Geben Sie eine beliebige Kombination von URL-Typen an. Die URL-Typen müssen das Suffix :// enthalten. Trennen Sie mehrere Werte durch Semikola. Beispiel:

customtype1://;customtype2://

Aktivieren der Host-zu-Client-Umleitung für spezifische Websites

Zum Aktivieren der Host-zu-Client-Umleitung für spezifische Websites legen Sie folgenden Registrierungsschlüssel auf dem Server-VDA fest:

Schlüssel: HKLM\Software\Wow6432Node\Citrix\SFTA

Name: ValidSites

Typ: REG_MULTI_SZ

Daten: Geben Sie eine beliebige Kombination vollständig qualifizierter Domänennamen (FQDN) an. Geben Sie mehrere FQDNs auf separaten Zeilen an. Ein FQDN darf nur an der Stelle ganz links einen Platzhalter enthalten. Dies entspricht einer Domänenebene und somit den Vorgaben von RFC 6125. Beispiel:

```
www.example.com
```

```
*.example.com
```


Bidirektionale Inhaltsumleitung

Durch die bidirektionale Inhaltsumleitung können HTTP- oder HTTPS-URLs in Webbrowsern oder in Anwendungen eingebettet zwischen der Citrix VDA-Sitzung und dem Clientendpunkt in beide Richtungen weitergeleitet werden. Eine URL, die in einem in der Citrix Sitzung ausgeführten Browser eingegeben wurde, kann mit dem Standardbrowser des Clients geöffnet werden. Umgekehrt kann eine URL, die in einem auf dem Client ausgeführten Browser eingegeben wurde, in einer Citrix Sitzung geöffnet werden, entweder mit einer veröffentlichten Anwendung oder einem Desktop. Einige gängige Anwendungsfälle für die bidirektionale Inhaltsumleitung sind:

- Umleitung von Web-URLs in Fällen, in denen der Startbrowser keinen Netzwerkzugriff auf die Quelle hat.
- Umleitung von Web-URLs aus Gründen der Browserkompatibilität und der Sicherheit.
- Die Umleitung von Web-URLs, die in Anwendungen eingebettet sind, wenn nicht ein Webbrowser in der Citrix Sitzung oder auf dem Client verwendet werden soll.

Systemanforderungen

- Desktopbetriebssystem- und Serverbetriebssystem-VDAs
- Citrix Workspace-App für Windows
- Internet Explorer 11

Konfiguration

Die bidirektionale Inhaltsumleitung muss mit der Citrix-Richtlinie sowohl auf dem VDA als auch auf dem Client aktiviert werden, damit die Umleitung funktioniert. Die bidirektionale Inhaltsumleitung ist standardmäßig deaktiviert.

Informationen zur VDA-Konfiguration finden Sie unter Bidirektionale Inhaltsumleitung in den ICA-Richtlinieneinstellungen.

Informationen zur Clientkonfiguration finden Sie unter Bidirektionale Inhaltsumleitung in der Dokumentation von Citrix Workspace-App für Windows.

Die Browsererweiterung muss mit den angezeigten Befehlen registriert werden. Führen Sie die Befehle auf dem VDA und dem Client nach Bedarf aus.

Um die Browsererweiterung auf dem VDA zu registrieren, öffnen Sie eine Eingabeaufforderung. Führen Sie dann `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` mit der erforderlichen Browseroption aus, wie in dem Beispiel gezeigt:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```


Um die Registrierung der Browsererweiterung aufzuheben, verwenden Sie die Option /unregIE wie im Beispiel gezeigt:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Um die Browsererweiterung auf dem Client zu registrieren, öffnen Sie eine Eingabeaufforderung und führen Sie %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe mit denselben Optionen wie in den Beispielen gezeigt aus.

Andere Überlegungen

- Die Anforderungen und Konfigurationen des Browsers gelten nur für den Browser, der die Umleitung startet. Der Zielbrowser, in dem die URL geöffnet wird, nachdem die Umleitung erfolgreich war, wird bei der Unterstützung nicht berücksichtigt. Beim Umleiten von URLs vom VDA zu einem Client ist nur auf dem VDA eine unterstützte Browserkonfiguration erforderlich. Umgekehrt ist beim Umleiten von URLs vom Client zu einem VDA nur auf dem Client eine unterstützte Browserkonfiguration erforderlich. Umgeleitete URLs werden je nach Richtung an den Standardbrowser auf der Zielmaschine übergeben, entweder der Client oder der VDA. Es ist NICHT erforderlich, denselben Browsertyp auf dem VDA und dem Client zu verwenden.
- Stellen Sie sicher, dass Umleitungsregeln keine Schleifenkonfiguration ergeben. Beispiel: Eine VDA-Richtlinie legt die Umleitung von https://www.citrix.com fest. Die Clientrichtlinie ist auch so eingestellt, dass dieselbe URL umgeleitet wird. Damit entsteht eine Endlosschleife.
- Es werden nur URLs im HTTP-/HTTPS-Protokoll unterstützt. URL-Abkürzungsprogramme werden nicht unterstützt.
- Für die Client-zu-VDA-Umleitung muss der Windows-Client mit Administratorrechten installiert sein.
- Wenn der Zielbrowser bereits geöffnet ist, wird die umgeleitete URL auf einer neuen Registerkarte geöffnet. Sonst wird die URL in einem neuen Browserfenster geöffnet.
- Die bidirektionale Inhaltsumleitung funktioniert nicht, wenn lokaler App-Zugriff (LAA) aktiviert ist.

Lokaler App-Zugriff und URL-Umleitung

August 18, 2021

Einführung

Durch lokalen App-Zugriff werden lokal installierte Windows-Anwendungen problemlos in eine gehostete Desktopumgebung integriert, ohne dass ein Wechsel zwischen Computern nötig ist.

Lokaler App-Zugriff ermöglicht Folgendes:

- Direkter Zugriff von virtuellen Desktops auf Anwendungen, die lokal auf einem Laptop, PC oder einem anderen Gerät installiert sind
- Bereitstellung einer flexiblen Anwendungsbereitstellungslösung Wenn Benutzer lokale Anwendungen haben, die Sie nicht virtualisieren können oder die IT nicht verwaltet, verhalten sich diese Anwendungen weiterhin so, als ob sie auf einem virtuellen Desktop installiert wären.
- Eliminieren Sie Doppelhoplatenz bei separat vom virtuellen Desktop gehosteten Anwendungen, indem Sie eine Verknüpfung mit der veröffentlichten Anwendung auf das Windows-Gerät des Benutzers platzieren.
- Unter anderem können die folgenden Anwendungen verwendet werden:
  - Videokonferenzsoftware, z. B. GoToMeeting.
  - Spezial- oder Nischenanwendungen, die noch nicht virtualisiert sind.
  - Anwendungen und Peripheriegeräte, die andernfalls große Datenmengen von einem Benutzergerät zum Server und zurück zum Benutzergerät senden würden, wie DVD-Brenner und TV-Tuner.

In XenApp und XenDesktop verwenden gehostete Desktopsitzungen die URL-Umleitung zum Starten von lokalen App-Zugriff-Anwendungen. Durch URL-Umleitung wird die Anwendung unter mehr als einer URL-Adresse bereitgestellt. Durch Auswählen eingebetteter Links in einem Browser in einer Desktopsitzung wird ein lokaler Browser gestartet (basierend auf der URL-Sperrliste des Browsers). Wenn Sie auf eine URL klicken, die nicht auf der Sperrliste steht, wird die URL erneut in der Sitzung geöffnet.

Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen. Für Anwendungssitzungen können Sie nur die Host-zu-Client-Inhaltsumleitung verwenden, wobei es sich um eine Art von Server-Dateitypzuordnung handelt. Diese FTA leitet bestimmte Protokolle an den Client um, z. B. HTTP, HTTPS, RTSP oder MMS. Wenn Sie beispielsweise nur eingebettete Links mit HTTP öffnen, werden die Links direkt in der Clientanwendung geöffnet. Für diese Art der Umleitung wird keine URL-Sperrliste oder URL-Positivliste unterstützt.

Wenn der lokale App-Zugriff aktiviert ist, werden URLs, die Benutzern als Links von lokal ausgeführten Anwendungen oder von Benutzern gehosteten Anwendungen bzw. als Verknüpfungen auf dem Desktop angezeigt werden, auf eine der folgenden Arten umgeleitet:

- Umleitung vom Computer des Benutzers zum gehosteten Desktop
- Umleitung vom XenApp- bzw. XenDesktop-Server auf den Computer des Benutzers
- Wiedergabe in der Umgebung, in der sie gestartet werden (keine Umleitung)

Zur Angabe des Pfads für die Inhaltsumleitung von bestimmten Websites konfigurieren Sie die URL-Positivliste und die URL-Sperrliste auf dem Virtual Delivery Agent. Diese Listen enthalten mehrteilige Registrierungsschlüssel, die die Richtlinieneinstellungen für die URL-Umleitung festlegen; weitere Informationen hierzu finden Sie unter "Einstellungen der Richtlinie 'Lokaler App-Zugriff'".

Mit den folgenden Ausnahmen können URLs auf dem VDA wiedergegeben werden:

- Regions-/Gebietsschemainformationen: Websites, die Gebietsschemainformationen benötigen, wie msn.com oder news.google.com (je nach Region wird eine bestimmte Seite geöffnet). Wenn VDA beispielsweise von einem Datenzentrum in Großbritannien bereitgestellt wird und der Client eine Verbindung aus Indien herstellt, würde der Benutzer erwarten, dass die Website in.msn.com erscheint, es wird jedoch uk.msn.com angezeigt.
- Multimedia-Inhalt: Websites mit Rich-Media-Inhalten, die auf dem Clientgerät wiedergegeben werden, ermöglichen eine gewohnte Benutzererfahrung und das Einsparen von Bandbreite während die Funktionalität auch in Netzwerken mit hoher Latenz gewährleistet ist. Die Flash-Umleitung wird durch die Umleitung von Sites mit anderen Medientypen wie Silverlight ergänzt. Somit ist die Umgebung sehr sicher. Die vom Administrator genehmigten URLs werden auf dem Client ausgeführt, während die restlichen URLs an VDA weitergeleitet werden.

Zusätzlich zur URL-Umleitung können Sie die Umleitung nach Dateitypzuordnung verwenden. FTA startet lokale Anwendungen, wenn Dateien in einer Sitzung geöffnet werden sollen. Wenn die lokale Anwendung gestartet wird, muss sie Zugriff auf die Datei haben, um sie zu öffnen. Daher können Sie mit lokalen Anwendungen nur Dateien öffnen, die sich auf Netzwerkfreigaben oder auf Clientlaufwerken (mit Clientlaufwerkzuordnung) befinden. Wenn beispielsweise der PDF-Reader eine lokale Anwendung ist und eine PDF-Datei geöffnet werden soll, wird zum Öffnen der Datei der lokale PDF-Reader verwendet. Da die lokale Anwendung direkt auf die Datei zugreifen kann, erfolgt keine Netzwerkübertragung über ICA zum Öffnen der Datei.

Anforderungen, Faktoren und Einschränkungen

Lokaler App-Zugriff wird auf den gültigen Betriebssystemen für VDAs für Windows-Serverbetriebssysteme und VDAs für Windows-Desktopbetriebssysteme unterstützt und erfordert mindestens Citrix Receiver für Windows Version 4.1. Die folgenden Browser werden unterstützt:

- Internet Explorer 11. Sie können Internet Explorer 8, 9 oder 10 verwenden, doch die von Microsoft unterstützte und von Citrix empfohlene Version ist Version 11.
- Firefox 3.5 bis 21.0
- Chrome 10

Beachten Sie die folgenden Punkte und Einschränkungen, wenn Sie lokalen App-Zugriff und URL-Umleitung verwenden.

- Lokaler App-Zugriff ist für virtuelle Desktops im Vollbildmodus unter Einbeziehung aller Monitore gedacht:
  - Die Benutzererfahrung kann beeinträchtigt werden, wenn lokaler App-Zugriff auf einem virtuellen Desktop verwendet wird, der im Fenstermodus ausgeführt wird oder der nicht auf allen Monitoren ausgeführt wird.

  - Bei der Verwendung mehrerer Monitore ist der maximierte Monitor der Standarddesktop für alle Anwendungen, die in der Sitzung gestartet werden, selbst wenn nachfolgende Anwendungen normalerweise auf einem anderen Monitor starten würden.
  - Das Feature unterstützt einen VDA; es ist keine Integration mit mehreren gleichzeitigen VDAs möglich.

- Einige Anwendungen können sich unerwartet verhalten und Benutzer beeinträchtigen:
  - Benutzer können die Laufwerkbuchstaben verwechseln, z. B. das lokale C:-Laufwerk mit dem virtuellen C:-Desktoplaufwerk.
  - Auf virtuellen Desktops verfügbare Drucker sind nicht für die lokalen Anwendungen verfügbar.
  - Anwendungen, die erweiterte Berechtigungen erfordern, können nicht als clientgehostete Anwendungen gestartet werden.
  - Keine spezielle Behandlung von Anwendungen mit einer Instanz (z. B. Windows Media Player).
  - Lokale Anwendungen werden mit dem Windows-Design der lokalen Maschine angezeigt.
  - Vollbildanwendungen werden nicht unterstützt. Dies schließt Anwendungen ein, die im Vollbildmodus geöffnet werden, z. B. PowerPoint-Bildschirmpräsentationen oder Fotoanzeigen, die den gesamten Desktop ausfüllen.
  - Lokaler App-Zugriff kopiert die Eigenschaften der lokalen Anwendung (z. B. die Verknüpfungen auf dem Clientdesktop und im Startmenü) auf dem VDA. Es werden jedoch keine anderen Eigenschaften, wie Tastenkombinationen und schreibgeschützte Attribute, kopiert.
  - Anwendungen, die die Reihenfolge der überlappenden Fenster anpassen, können unvorhersehbare Ergebnisse verursachen. Beispielsweise könnten einige Fenster ausgeblendet werden.
  - Verknüpfungen, einschließlich Arbeitsplatz, Papierkorb, Systemsteuerung, Netzlaufwerkverknüpfungen und Ordnerverknüpfungen werden nicht unterstützt.
  - Die folgenden Dateitypen und Dateien werden nicht unterstützt: benutzerdefinierte Dateitypen, Dateien ohne zugeordnete Programme, ZIP-Dateien und ausgeblendete Dateien.
  - Taskleistengruppierung wird nicht für gemischte 32-Bit und 64-Bit clientgehostete Anwendungen und VDA-Anwendungen unterstützt, z. B. die Gruppierung von 32-Bit-Versionen lokaler Anwendungen mit 64-Bit-VDA-Anwendungen.
  - Anwendungen können nicht über COM gestartet werden. Beispiel: Wenn Sie auf ein eingebettetes Office-Dokument in einer Office-Anwendung klicken, wird der Prozessstart nicht erkannt und die Integration der lokalen Anwendung schlägt fehl.

- Double-Hop-Szenarien, bei denen ein Benutzer einen virtuellen Desktop aus einer anderen virtuellen Desktopsitzung startet, werden nicht unterstützt.
- Die URL-Umleitung unterstützt nur explizite URLs, d. h. solche, die in der Adressleiste des Browsers angezeigt werden oder mit der browserinternen Suchfunktion gefunden wurden (je

nach Browser).

- Die URL-Umleitung funktioniert nur in Desktopsitzungen und nicht in Anwendungssitzungen.
- Benutzer haben keine Berechtigung, im lokalen Desktopordner in einer VDA-Sitzung neue Dateien zu erstellen.
- Mehrere Instanzen einer lokal ausgeführten Anwendung verhalten sich entsprechend den Taskleisteneinstellungen für den virtuellen Desktop. Verknüpfungen zu lokal ausgeführten Anwendungen werden jedoch nicht mit ausgeführten Instanzen dieser Anwendungen gruppiert. Sie werden auch nicht mit ausgeführten Instanzen von gehosteten Anwendungen oder mit an gehosteten Anwendungen angehefteten Verknüpfungen gruppiert. Benutzer können nur Fenster von lokal ausgeführten Anwendungen von der Taskleiste aus schließen. Zwar können Benutzer die Fenster von lokalen Anwendungen in der Desktop-Taskleiste und im Startmenü anheften, jedoch starten die Anwendungen bei Verwendung dieser Verknüpfungen möglicherweise nicht konsistent.

Interaktion mit Windows

Bei der Interaktion zwischen lokaler App-Zugriff und Windows tritt u. a. das folgende Verhalten auf.

- Verknüpfungen in Windows 8 und Windows Server 2012
  - Windows Store-Apps, die auf dem Client installiert sind, werden nicht als Teil der Verknüpfungen von lokalem App-Zugriff aufgelistet.
  - Bild- und Videodateien werden normalerweise standardmäßig mit Windows Store-Apps geöffnet. Lokaler App-Zugriff listet die Windows Store-Apps jedoch auf und öffnet Verknüpfungen mit Desktopanwendungen.
- Local Programs
  - In Windows 7 ist der Ordner im Startmenü verfügbar.
  - In Windows 8 ist der Ordner "Local Programs"nur verfügbar, wenn der Benutzer **Alle Apps** als Kategorie auf der Startseite auswählt. Nicht alle Unterordner werden in Local Programs angezeigt.
- Windows 8-Grafikfunktionen für Anwendungen
  - Desktopanwendungen sind auf den Desktopbereich beschränkt und werden von der Startseite bzw. Anwendungen im Windows 8-Stil vollständig abgedeckt.
  - Mit lokalem App-Zugriff verwendete Anwendungen verhalten sich jedoch bei der Verwendung von mehreren Monitoren nicht wie Desktopanwendungen. Bei der Verwendung mehrerer Monitore werden die Startseite und der Desktop auf unterschiedlichen Monitoren angezeigt.
- Windows 8 und lokaler App-Zugriff mit URL-Umleitung

- Da bei Windows 8 Internet Explorer keine Add-Ons aktiviert sind, müssen Sie den Desktop-Internet Explorer zum Aktivieren von URL-Umleitung verwenden.
- In Windows Server 2012 werden Add-Ons von Internet Explorer standardmäßig deaktiviert. Um URL-Umleitung zu implementieren, deaktivieren Sie die verstärkte Sicherheitskonfiguration für Internet Explorer. Setzen Sie die Internet Explorer-Optionen zurück und starten Sie das Programm neu, um sicherzustellen, dass Add-Ons für Standardbenutzer aktiviert sind.

Konfigurieren von lokalem App-Zugriff und URL-Umleitung

Verwenden von lokalem App-Zugriff und URL-Umleitung für die Citrix Workspace-App:

- Installieren Sie die Citrix Workspace-App auf dem lokalen Client. Sie können beide Features während der Installation der Citrix Workspace-App aktivieren. Alternativ können Sie die Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor aktivieren.
- Legen Sie die Richtlinieneinstellung **Lokalen App-Zugriff zulassen** auf **Aktiviert** fest. Sie können auch die Richtlinie für URL-Positiv- und -Sperrlisten für die URL-Umleitung konfigurieren. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Lokaler App-Zugriff".

Aktivieren von lokalem App-Zugriff und URL-Umleitung

Führen Sie die folgenden Schritte aus, um den lokalen App-Zugriff für alle lokalen Anwendungen zu aktivieren:

1. Starten Sie Citrix Studio.
   - Öffnen Sie **Citrix Studio** für On-Premises-Bereitstellungen über das **Startmenü**.
   - Wechseln Sie für Cloud-Servicebereitstellungen zu **Citrix Cloud > Virtual Apps and Desktops Service > Verwalten**.
2. Klicken Sie im Studio-Navigationsbereich auf **Richtlinien**.
3. Klicken Sie im Bereich "Aktionen"auf **Richtlinie erstellen**.
4. Geben Sie im Fenster "Richtlinie erstellen"den Begriff "Lokalen App-Zugriff zulassen"im Suchfeld ein und klicken Sie auf **Auswählen**.
5. Wählen Sie im Fenster "Einstellung bearbeiten"die Option **Zulässig** aus. Standardmäßig ist die Richtlinie **Lokalen App-Zugriff zulassen** deaktiviert. Wenn diese Einstellung zugelassen wird, können Endbenutzer selbst entscheiden, ob veröffentlichte Anwendungen und Verknüpfungen für den lokalen App-Zugriff in der Sitzung aktiviert sind. (Wenn die Einstellung nicht zulässig ist, sind sowohl veröffentlichte Anwendungen als auch Verknüpfungen für den lokalen App-Zugriff für den VDA deaktiviert.) Diese Richtlinie gilt für die gesamte Maschine und für die URL-Umleitungsrichtlinie.

6. Geben Sie im Fenster "Richtlinie erstellen"den Begriff "URL-Umleitungspositivliste"im Suchfeld ein und klicken Sie auf **Auswählen**. Die URL-Umleitungspositivliste gibt URLs an, die im Standardbrowser der Remotesitzung geöffnet werden können.
7. Klicken Sie im Fenster "Einstellung bearbeiten"auf **Hinzufügen**, um die URLs hinzuzufügen, und klicken Sie auf **OK**.
8. Geben Sie im Fenster "Richtlinie erstellen"den Begriff "URL-Umleitungssperrliste"im Suchfeld ein und klicken Sie auf **Auswählen**. Die URL-Umleitungssperrliste gibt URLs an, die an den Standardbrowser auf dem Endpunkt weitergeleitet werden.
9. Klicken Sie im Fenster "Einstellung bearbeiten"auf **Hinzufügen**, um die URLs hinzuzufügen, und klicken Sie auf **OK**.
10. Klicken Sie auf der Seite "Einstellungen"auf **Weiter**.
11. Weisen Sie die Richtlinie auf der Seite "Benutzer und Maschinen"den entsprechenden Bereitstellungsgruppen zu und klicken Sie auf **Weiter**.
12. Überprüfen Sie auf der Seite "Zusammenfassung"die gewählten Einstellungen und klicken Sie auf **Fertig stellen**.

Führen Sie die folgenden Schritte aus, um bei der Installation der Citrix Workspace-App die URL-Umleitung für alle lokalen Anwendungen zu aktivieren:

1. Aktivieren Sie die URL-Umleitung für alle Benutzer einer Maschine, wenn Sie die Citrix Workspace-App installieren. Dadurch werden auch die für URL-Umleitung erforderlichen Browser-Add-Ons registriert.
2. Führen Sie an der Eingabeaufforderung den jeweiligen Befehl zum Installieren der Citrix Workspace-App mit einer der folgenden Optionen aus:
   - Für CitrixReceiver.exe verwenden Sie `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - Für CitrixReceiverWeb.exe verwenden Sie `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Aktivieren der Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor

> **Hinweis:**
>
> - Bevor Sie mit dem Gruppenrichtlinien-Editor die Vorlage für den lokalen App-Zugriff aktivieren, fügen Sie dem lokalen Gruppenrichtlinienobjekt die Vorlagendateien receiver.admx/adml hinzu. Weitere Informationen finden Sie unter Konfigurieren der administrativen Gruppenrichtlinienobjektvorlage.
> - Die Vorlagendateien für die Citrix Workspace-App sind nur dann im lokalen Gruppenrichtlinienobjekt unter **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace** verfügbar, wenn Sie die Dateien CitrixBase.admx/CitrixBase.adml dem Ordner %systemroot%\policyDefinitions hinzufügen.

Führen Sie folgende Schritte aus, um die Vorlage für den lokalen App-Zugriff mit dem Gruppenrichtlinien-Editor zu aktivieren:

1. Führen Sie **gpedit.msc** aus.
2. Navigieren Sie zu **Computerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlage (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.
3. Klicken Sie auf **Einstellungen für 'Lokaler App-Zugriff'**.
4. Wählen Sie **Aktiviert** und anschließend **URL-Umleitung zulassen**. Registrieren Sie für die URL-Umleitung Browser-Add-Ons über die Befehlszeile (siehe *Registrieren von Browser-Add-Ons* weiter unten).

Zugriffsbeschränkung auf veröffentlichte Anwendungen

Sie können den Zugriff auf veröffentlichte Anwendungen folgende Weise gewähren:

Verwenden Sie den Registrierungs-Editor.

1. Führen Sie auf dem Server, auf dem der Citrix Studio installiert ist, regedit.exe aus.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`.
3. Fügen Sie den REG_DWORD-Eintrag `ClientHostedAppsEnabled` mit dem Wert 1 hinzu. (Durch den Wert 0 wird der lokale App-Zugriff deaktiviert.)

Verwenden Sie das PowerShell-SDK.

1. Öffnen Sie PowerShell auf der Maschine mit dem Delivery Controller.
2. Geben Sie den folgenden Befehl ein: `set-configsitemetadata -name "studio_clientHosted"-value "true"`.

Verwenden Sie das Citrix Virtual Apps and Desktops Remote PowerShell SDK, um Zugriff auf **Anwendung für lokalen App-Zugriff hinzufügen** in einer Cloudservicebereitstellung zu erhalten. Weitere Informationen finden Sie unter Citrix Virtual Apps and Desktops Remote PowerShell SDK.

1. Laden Sie das Installationsprogramm herunter:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Führen Sie die folgenden Befehle aus:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. Geben Sie den folgenden Befehl ein: `set-configsitemetadata -name "studio_clientHosted" -value "true"`.

Nachdem Sie die zutreffenden Schritte oben ausgeführt haben, führen Sie die folgenden Schritte aus, um fortzufahren.

1. Öffnen Sie **Citrix Studio** über das **Startmenü**.
2. Klicken Sie im Studio-Navigationsbereich auf **Anwendungen**.
3. Klicken Sie im oberen mittleren Bereich mit der rechten Maustaste auf den leeren Bereich, und wählen Sie im Kontextmenü die Option **Anwendung für lokalen App-Zugriff hinzufügen**. Sie können auch im Aktionsbereich auf **Anwendung für lokalen App-Zugriff hinzufügen** klicken. Klicken Sie auf **Aktualisieren**, um die Option "Anwendung für lokalen App-Zugriff hinzufügen" im Aktionsbereich anzuzeigen.
4. Veröffentlichen Sie die Anwendung "Lokaler App-Zugriff".
    - Der Assistent zum Hinzufügen von lokalem App-Zugriff wird mit der Einführungsseite gestartet, die Sie für zukünftige Starts des Assistenten deaktivieren können.
    - Der Assistent führt Sie durch die im Folgenden beschriebenen Seiten "Gruppen", "Standort", "Identifizierung", "Bereitstellung"und "Zusammenfassung". Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur Zusammenfassung gelangen.
    - Wählen Sie auf der Seite "Gruppen"eine oder mehrere Bereitstellungsgruppen, den die Anwendungen hinzugefügt werden und klicken Sie dann auf **Weiter**.
    - Geben Sie auf der Seite "Speicherort"den vollständigen Pfad der ausführbaren Datei für die Anwendung auf dem lokalen Computer des Benutzers ein und geben Sie den Pfad zu dem Ordner ein, in dem sich die Anwendung ist. Citrix empfiehlt, für den Systemumgebungsvariablenpfad zu verwenden, z. B. %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
    - Übernehmen Sie auf der Seite "Identifizierung"die Standardwerte oder geben Sie die Informationen ein und klicken Sie dann auf **Weiter**.
    - Konfigurieren Sie auf der Seite "Bereitstellung", wie diese Anwendung an Benutzer bereitgestellt wird, und klicken Sie dann auf **Weiter**. Sie können das Symbol für die ausgewählte Anwendung angeben. Sie können auch angeben, ob die Verknüpfung mit der lokalen Anwendung auf dem virtuellen Desktop im Startmenü, auf dem Desktop oder beiden angezeigt wird.
    - Überprüfen Sie auf der Seite "Zusammenfassung"die gewählten Einstellungen und klicken Sie auf **Fertig stellen**, um den Assistenten für Zugriff auf lokale Anwendungen zu beenden.

Registrieren von Browser-Add-Ons

> **Hinweis:**
>
> Die für URL-Umleitung erforderlichen Browser-Add-Ons werden automatisch registriert, wenn Sie die Citrix Workspace-App über die Befehlszeile mit folgender Option installieren: /ALLOW_CLIENTHOSTEDAPPSURL=1.

Sie können ein Add-On oder alle mit den folgenden Befehlen registrieren und die Registrierung aufheben:

- Registrieren von Add-Ons auf einem Clientgerät: <*client-installation-folder*>\redirector.exe /reg<*browser*>
- Aufheben der Registrierung von Add-Ons auf einem Clientgerät: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- Registrierung von Add-Ons auf einem VDA: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- Aufheben der Registrierung von Add-Ons auf einem VDA: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

Wobei <*Browser*> Internet Explorer, Firefox, Chrome oder All ist.

Beispiel: Mit dem folgenden Befehl werden Internet Explorer-Add-Ons auf einem Gerät mit der Citrix Workspace-App registriert.

C:\Programme\Citrix\ICA Client\redirector.exe/regIE

Mit dem folgenden Befehl werden alle Add-Ons auf einem VDA für Windows-Multisitzungs-OS registriert.

C:\Programme (x86)\Citrix\System32\VDARedirector.exe /regAll

URL-Interception in Browsern

- Standardmäßig wird die angegebene URL von Internet Explorer umgeleitet. Wenn die URL nicht in der Sperrliste enthalten ist und dennoch vom Browser oder der Website an eine andere URL-Adresse umgeleitet wird, wird die endgültige URL nicht umgeleitet. Sie wird nicht umgeleitet, selbst wenn sie in der Sperrliste enthalten ist.

Zum richtigen Funktionieren der URL-Umleitung müssen Sie bei entsprechender Aufforderung durch den Browser das Add-On aktivieren. Wenn die mit Internetoptionen verbundenen Add-Ons bzw. die angeforderten Add-Ons deaktiviert sind, funktioniert die URL-Umleitung nicht richtig.

- Firefox-Add-Ons leiten URLs immer um.

Wenn ein Add-On installiert wurde, bietet Firefox auf einer neuen Registerkarte die Möglichkeit, die Add-On-Installation zuzulassen oder zu verhindern. Lassen Sie das Add-On zu, damit das Feature funktioniert.

- Chrome-Add-Ons leiten die endgültige URL stets um, wenn es sich um geleitete und nicht eingegebene URLs handelt.

Die Erweiterungen wurden extern installiert. Wenn Sie die Erweiterung deaktivieren, funktioniert die URL-Umleitung in Google Chrome nicht. Wenn die URL-Umleitung im Inkognito-Modus erforderlich ist, lassen Sie durch Auswählen dieser Option in den Browsereinstellungen zu, dass die Erweiterung im Inkognito-Modus ausgeführt wird.

Konfigurieren des Verhaltens von lokalen Anwendungen bei der Abmeldung und Trennung

> **Hinweis:**
>
> Wenn Sie die Einstellungen nicht mit dem unten aufgeführten Verfahren konfigurieren, werden lokale Anwendungen standardmäßig weiter ausgeführt, wenn ein Benutzer sich abmeldet oder die Verbindung zum virtuellen Desktop trennt. Nach der Wiederverbindung werden lokale Anwendungen wieder integriert, wenn sie auf dem virtuellen Desktop verfügbar sind.

1. Führen Sie auf dem gehosteten Desktop **gpedit.msc** aus.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State`.

   Navigieren Sie bei 64-Bit-Systemen zu `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State`.
3. Fügen Sie den REG_DWORD-Eintrag **Terminate** mit einem der folgenden Werte hinzu:

   - 1: Lokale Anwendungen werden weiterhin ausgeführt, wenn sich ein Benutzer abmeldet oder die Verbindung zum virtuellen Desktop trennt. Bei der Wiederverbindung werden lokale Anwendungen wieder integriert, wenn sie im virtuellen Desktop verfügbar sind.
   - 3: Lokale Anwendungen werden geschlossen, wenn sich ein Benutzer abmeldet oder die Verbindung zum virtuellen Desktop trennt.

Überlegungen zu USB und Clientlaufwerk

August 18, 2021

HDX-Technologie bietet **optimierte Unterstützung** für die gebräuchlichsten USB-Geräte. Hierzu gehören:

- Monitore
- Mäuse
- Tastaturen

- VoIP-Telefone
- Headsets
- Webcams
- Scanner
- Kameras
- Drucker
- Laufwerke
- Smartcardleser
- Grafiktablets
- Signaturtablets

Die optimierte Unterstützung bietet eine verbesserte Benutzererfahrung, Leistung und Bandbreiteneffizienz über ein WAN. Die optimierte Unterstützung ist normalerweise, insbesondere aber in Umgebungen mit hoher Latenz oder hohen Sicherheitsanforderungen, die beste Option.

HDX-Technologie bietet **generische USB-Umleitung** für Spezialgeräte ohne optimierte Unterstützung oder wenn diese ungeeignet ist. Beispiele:

- Ein USB-Gerät hat Merkmale, die nicht von der optimierten Unterstützung abgedeckt werden, z. B. eine Maus oder Webcam mit zusätzlichen Tasten.
- Benutzer benötigen Funktionen, die nicht von der optimierten Unterstützung abgedeckt werden, z. B. das Brennen von CDs.
- Bei dem USB-Gerät handelt es sich um ein Spezialgerät, z. B. ein Test- oder Messgerät oder ein industrielles Steuergerät.
- Eine Anwendung erfordert direkten Zugriff auf das Gerät als USB-Gerät.
- Für das USB-Gerät gibt es nur einen Windows-Treiber. Ein Smartcardleser kann beispielsweise keinen Treiber für Citrix Receiver für Android haben.
- Die Version von Citrix Receiver bietet keine optimierte Unterstützung für solche USB-Geräte.

Vorteile von generischer USB-Umleitung:

- Benutzer müssen keine Gerätetreiber auf den Benutzergeräten installieren.
- USB-Clienttreiber werden auf der VDA-Maschine installiert.

> **Hinweis:**
>
> - Die generische USB-Umleitung kann zusammen mit der optimierten Unterstützung verwendet werden. Wenn Sie die generische USB-Umleitung aktivieren, konfigurieren Sie Einstellungen für die Citrix Richtlinie "USB-Geräte" für die generische USB-Umleitung und für die optimierte Unterstützung, um inkonsistentes und unerwartetes Verhalten zu verhindern.
> - Die Citrix Richtlinieneinstellung Regeln für die USB-Clientgeräteoptimierung ist eine spezifische Einstellung für die generische USB-Umleitung für ein bestimmtes USB-Gerät. Es handelt sich hierbei nicht um die hier beschriebene optimierte Unterstützung.

> - Das verwandte Feature Client-USB-Geräteumleitung für Plug & Play-Geräte bietet optimierte Unterstützung für Geräte wie Kameras und Medienplayer, die Picture Transfer Protocol (PTP) oder Media Transfer Protocol (MTP) verwenden. Die Client-USB-Geräteumleitung für Plug & Play-Geräte ist nicht Teil der generischen USB-Umleitung. Eine Liste der unterstützten VDA-Versionen finden Sie unter Standardrichtlinieneinstellungen.

Überlegungen zur Leistung für USB-Geräte

Bei der generischen Umleitung bestimmter USB-Gerätetypen können sich Netzwerklatenz und Bandbreite auf die Benutzererfahrung und den USB-Gerätebetrieb auswirken. Die Funktion zeitempfindlicher Geräte kann beispielsweise bei geringer Bandbreite und hoher Latenz gestört werden. Verwenden Sie, falls möglich, stattdessen die optimierte Unterstützung.

Einige Geräte erfordern eine hohe Bandbreite, z. B. 3D-Mäuse (die mit bandbreitenintensiven 3D-Anwendungen verwendet werden). Sie können Leistungsprobleme durch Citrix Richtlinien vermeiden. Weitere Informationen finden Sie unter Einstellungen der Richtlinie "Bandbreite" für die Client-USB-Geräteumleitung und unter Einstellungen der Richtlinie "Multistreamverbindungen".

Überlegungen zur Sicherheit für USB-Geräte

Einige USB-Geräte sind von Haus aus sicherheitsempfindlich, z. B. Smartcardleser, Fingerabdruckleser und Signatur-Tablets. Andere, etwa USB-Speichergeräte, können zur Übertragung vertraulicher Daten verwendet werden.

USB-Geräte werden häufig zur Verbreitung von Schadsoftware verwendet. Über die Konfiguration von Citrix Receiver, XenApp und XenDesktop können entsprechende Sicherheitsrisiken vermindert, jedoch nicht eliminiert werden Dies gilt sowohl für die generische USB-Umleitung als auch für die optimierte Unterstützung.

> **Wichtig**
>
> Verwenden Sie für sicherheitsempfindliche Geräte und Daten immer sichere HDX-Verbindungen mit TLS oder IPsec.
>
> Aktivieren Sie nur Unterstützung für USB-Geräte, die Sie benötigen. Konfigurieren Sie die generische USB-Umleitung und die optimierte Unterstützung für diese Anforderungen.
>
> Informieren Sie die Benutzer über die sichere Verwendung von USB-Geräten: nur USB-Geräte von vertrauenswürdigen Quellen, USB-Geräte in offen zugänglichen Umgebungen nicht unbeaufsichtigt lassen (z. B. USB-Flashlaufwerk im Internetcafé), Risiken der Verwendung von USB-Geräten auf mehreren Computern.

Kompatibilität mit der generischen USB-Umleitung

Die generische USB-Umleitung unterstützt USB 2.0- und ältere Geräte. Die generische USB-Umleitung unterstützt außerdem USB 3.0-Geräte, wenn diese an einem USB 2.0- oder USB 3.0-Anschluss angeschlossen sind. Die generische USB-Umleitung bietet keine Unterstützung für USB-Features wie Super Speed, die mit USB 3.0 eingeführt wurden.

Folgende Citrix Receiver-Versionen unterstützen die generische USB-Umleitung:

- Citrix Receiver für Windows (siehe Konfigurieren der USB-Unterstützung)
- Citrix Receiver für Mac (siehe Konfigurieren von Citrix Receiver für Mac)
- Citrix Receiver für Linux (siehe Optimieren)
- Citrix Receiver für Chrome (siehe Neue Features)

Informationen zu den Citrix Receiver-Versionen finden Sie in der Citrix Receiver-Featurematrix.

Wenn Sie eine ältere Citrix Receiver-Version verwenden, konsultieren Sie die zugehörige Dokumentation zu Informationen über die Unterstützung der generischen USB-Umleitung. Die Dokumentation zu Citrix Receiver enthält Informationen zu jeglichen Einschränkungen für unterstützte USB-Gerätetypen.

Die generische USB-Umleitung unterstützt Desktopsitzungen mit VDAs für Desktopbetriebssysteme ab Version 7.6 bis zur aktuellen Version.

Die generische USB-Umleitung unterstützt Desktopsitzungen mit VDAs für Serverbetriebssysteme ab Version 7.6 bis zur aktuellen Version unter folgenden Bedingungen:

- Der VDA muss unter Windows Server 2012 R2 oder Windows Server 2016 ausgeführt werden.
- Der USB-Gerätetreiber muss mit dem Remotedesktop-Sitzungshost für Windows 2012 R2 einschließlich Virtualisierung vollständig kompatibel sein.

Einige USB-Gerätetypen werden nicht von der generischen USB-Umleitung unterstützt, da ihre Umleitung nicht nützlich wäre:

- USB-Modems
- USB-Netzwerkadapter
- USB-Hubs. Mit USB-Hubs verbundene USB-Geräte werden separat behandelt.
- Virtuelle USB-COM-Anschlüsse. Verwenden Sie hierfür statt der generischen USB-Umleitung die COM-Anschlussumleitung.

Weitere Informationen zu USB-Geräten, für die die generische USB-Umleitung getestet wurde, finden Sie unter CTX123569. Einige USB-Geräte funktionieren bei generischer USB-Umleitung nicht einwandfrei.

Konfigurieren der generischen USB-Umleitung

Sie können festlegen, für welche USB-Gerätetypen die generische USB-Umleitung verwendet werden soll. Dies kann separat konfiguriert werden:

- Auf dem VDA mit Citrix Richtlinieneinstellungen. Weitere Informationen finden Sie unter Umleitung von Clientlaufwerken und Benutzergeräten und Einstellungen der Richtlinie "USB-Geräte".
- In Citrix Receiver über Citrix Receiver-abhängige Mechanismen. Citrix Receiver für Windows hat beispielsweise Registrierungseinstellungen, die über eine administrative Vorlage gesteuert werden können. Standardmäßig ist die USB-Umleitung für einige USB-Geräteklassen zulässig und für andere nicht. Weitere Informationen hierzu finden Sie unter Konfigurieren der USB-Unterstützung in der Dokumentation zu Citrix Receiver für Windows.

Diese separate Konfiguration ist flexibler. Beispiel:

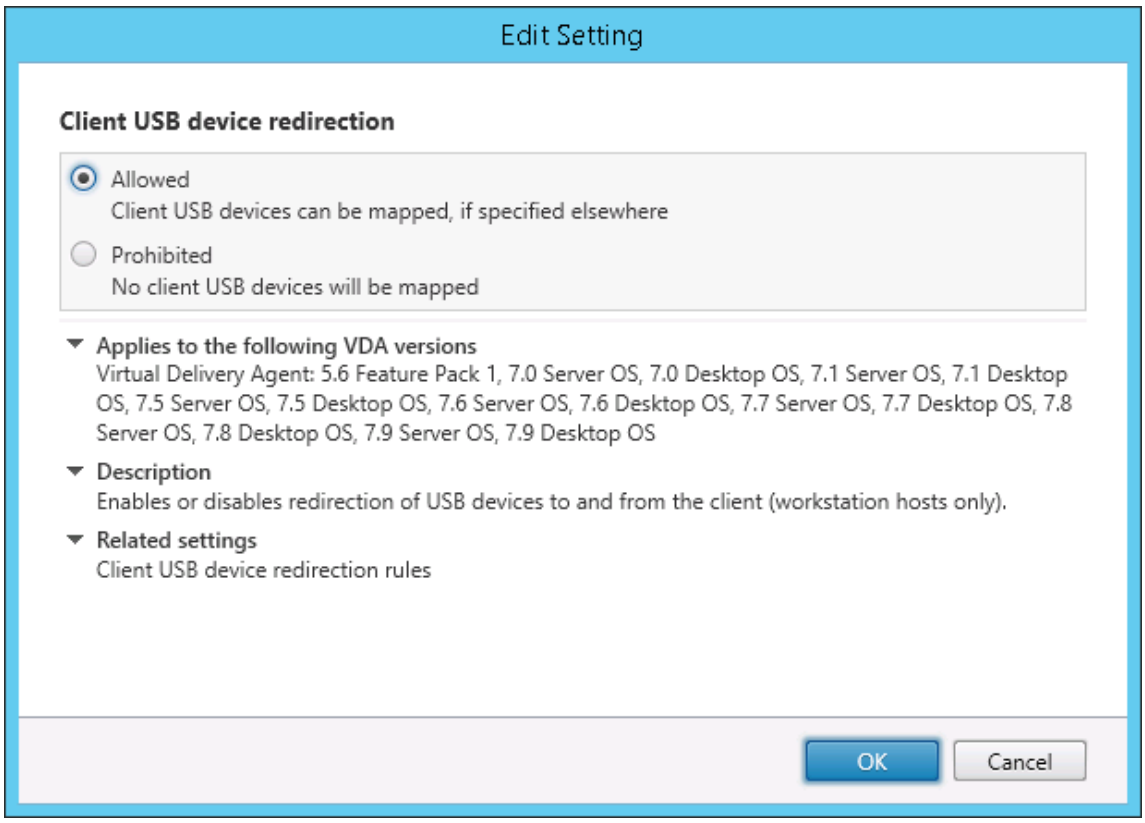
- Wenn zwei verschiedene Abteilungen für Citrix Receiver und VDA verantwortlich sind, können sie eigene Vorgaben festlegen. Diese gelten dann, wenn ein Benutzer in einer Abteilung auf eine Anwendung in einer anderen Abteilung zugreift.
- Wenn USB-Geräte nur für bestimmte Benutzer oder nur für Benutzer, die eine Verbindung über das LAN anstelle von NetScaler Gateway herstellen, zugelassen werden sollen, kann die entsprechende Steuerung über Citrix Richtlinieneinstellungen erfolgen.

Aktivieren der generischen USB-Umleitung

Zum Aktivieren der generischen USB-Umleitung konfigurieren Sie Citrix Richtlinieneinstellungen und Citrix Receiver.

Führen Sie in den Citrix Richtlinieneinstellungen folgende Schritte aus:

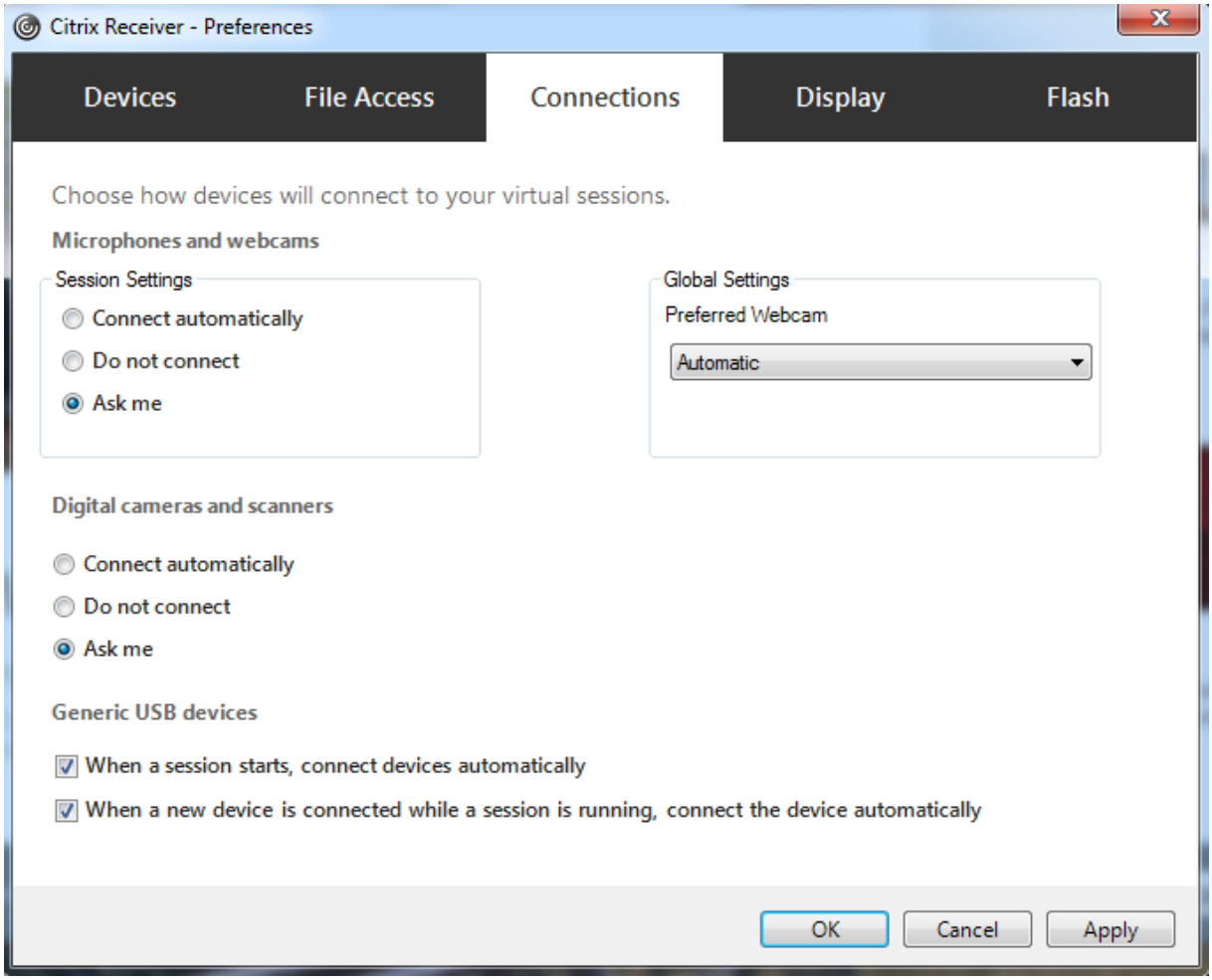
1. Fügen Sie die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie den Wert auf **Zugelassen** ein.



2. Optional: Zum Aktualisieren der Liste der zur Umleitung verfügbaren USB-Geräte fügen Sie die Einstellung Regeln für die Client-USB-Geräteumleitung einer Richtlinie hinzu und stellen Sie die USB-Richtlinienregeln ein.

   Gehen Sie in Citrix Receiver folgendermaßen vor:

3. Aktivieren Sie die USB-Unterstützung, wenn Sie Citrix Receiver auf Benutzergeräten installieren. Sie können eine administrative Vorlage verwenden oder die Einstellung unter “Citrix Receiver für Windows > Einstellungen > Verbindungen”festlegen.



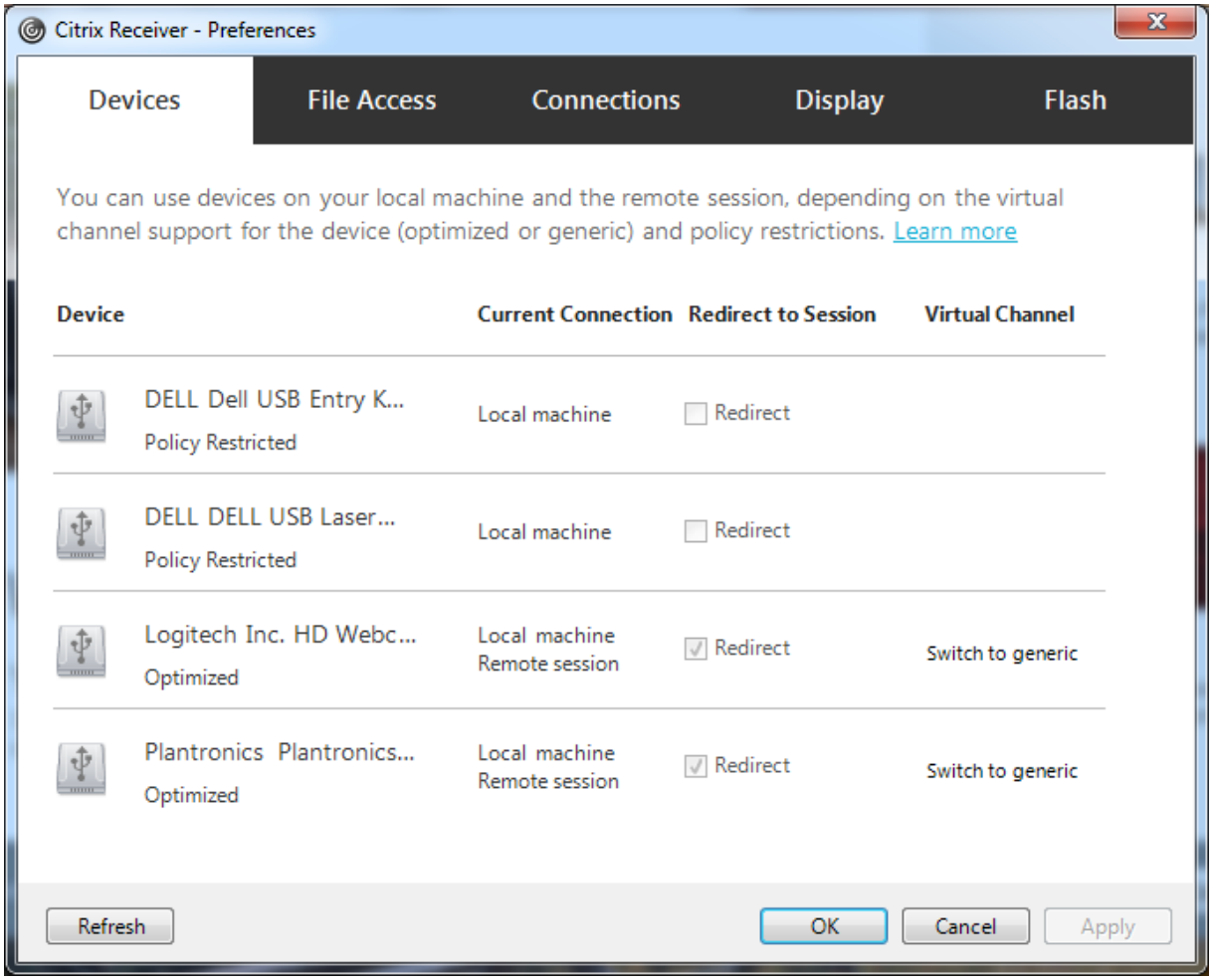
Wenn Sie im vorigen Schritt die USB-Richtlinienregeln für den VDA festgelegt haben, geben Sie nun die gleichen Richtlinienregeln für Citrix Receiver ein.

Informationen zur USB-Unterstützung Für Thin Clients und die erforderliche Konfiguration erhalten Sie vom Hersteller.

Konfigurieren der für die generische USB-Umleitung verfügbaren USB-Gerätetypen

USB-Geräte werden automatisch umgeleitet, wenn die USB-Unterstützung aktiviert ist und die USB-Einstellungen für eine automatische Verbindung der USB-Geräte konfiguriert wurden. USB-Geräte werden auch automatisch umgeleitet, wenn das Gerät im Modus “Desktop Appliance”ist und der Verbindungsbalken nicht angezeigt wird.

Die Benutzer können Geräte, die nicht automatisch umgeleitet werden, explizit umleiten, indem sie sie aus der USB-Geräteliste auswählen. Eine Anleitung hierzu enthält der Artikel zum Anzeigen von Geräten in Desktop Viewer in der Hilfe für Citrix Receiver für Windows.



Verwendung der generischen USB-Umleitung anstelle der optimierten Unterstützung:

- Wählen Sie in Citrix Receiver das USB-Gerät für die generische USB-Umleitung manuell aus und wählen Sie im Dialogfeld "Einstellungen"auf der Registerkarte "Geräte"die Option **Zu allgemein wechseln**.
- Wählen Sie das USB-Gerät für die generische USB-Umleitung automatisch, indem Sie die automatische Umleitung für den entsprechenden USB-Gerätetyp konfigurieren (z. B. AutoRedirectStorage=1) und die USB-Benutzereinstellung auf die automatische Verbindung der USB-Geräte festlegen. Weitere Informationen finden Sie unter CTX123015.

> **Hinweis:**
>
> Konfigurieren Sie die generische USB-Umleitung für Webcams nur dann, wenn die Webcam nicht mit der HDX-Multimediaumleitung kompatibel ist.

Um zu verhindern, dass USB-Geräte je aufgeführt oder umgeleitet werden, können Sie für Citrix Receiver und den VDA spezifische Regeln festlegen.

Für die generische USB-Umleitung benötigen Sie mindestens die USB-Geräteklasse und die Unterk-

lasse. Nicht für alle USB-Geräte wird die Geräteklasse bzw. Unterklasse verwendet, die man vermuten würde. Beispiel:

- Für Stifte wird die Klasse "Maus"verwendet.
- Für Smartcardleser kann eine vom Hersteller definierte Klasse oder die Klasse "HID-Geräte"gelten.

Zur präziseren Steuerung müssen Sie außerdem die Hersteller-, Produkt- und Release-ID kennen. Sie erhalten diese Informationen beim Vertreiber des Geräts.

> **Wichtig**
>
> Manipulierte USB-Geräte können USB-Gerätemerkmale präsentieren, die nicht ihrer beabsichtigten Nutzung entsprechen. Geräteregeln sind nicht zur Verhinderung solcher Fälle vorgesehen.

Die für die generische USB-Umleitung verfügbaren USB-Geräte legen Sie über Regeln für die Client-USB-Geräteumleitung für den VDA und Citrix Receiver fest, welche die USB-Standardrichtlinienregeln außer Kraft setzen.

VDA:

- Bearbeiten Sie die Administrator-Überschreibungsregeln der Serverbetriebssystemmaschinen mit den Gruppenrichtlinienregeln. Die Gruppenrichtlinien-Verwaltungskonsole ist auf dem Installationsmedium enthalten:
  - Für x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Für x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Citrix Receiver für Windows:

- Bearbeiten Sie die Benutzergeräteregistrierung. Eine administrative Vorlage (ADM-Datei) ist auf dem Installationsmedium enthalten, sodass Sie das Gerät über die Active Directory-Gruppenrichtlinie ändern können:
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Die Produktstandardregeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. Ändern Sie diese Produktstandardregeln nicht. Verwenden Sie sie als Anleitung zum Erstellen von Administrator-Überschreibungsregeln, wie nachfolgend beschrieben. Die GPO-Überschreibungen werden ausgewertet, bevor die Produktstandardregeln angewendet werden.

Die Administrator-Override-Regeln sind in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules gespeichert. GPO-Richtlinienregeln haben das Format **{Allow:|Deny:}** gefolgt von *Tag=Wert*-Ausdrücken, die durch Leerzeichen getrennt sind.

Die folgenden Tags werden unterstützt:

Tag	Beschreibung
VID	Vendor-ID vom Gerätedeskriptor
PID	Produkt-ID vom Gerätedeskriptor
REL	Release-ID vom Gerätedeskriptor
Klasse	Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor; verfügbare USB-Klassencodes finden Sie auf der USB-Website unter https://www.usb.org/.
SubClass	Unterklasse vom Gerätedeskriptor oder ein Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder ein Schnittstellendeskriptor

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird. Ein Trennzeichen ist nicht erforderlich, der Kommentar wird beim Abgleichen ignoriert.
- Leere Zeilen und Kommentare werden ignoriert.
- Leerzeichen dienen als Trennzeichen, sie können nicht in einer Zahl oder Kennung verwendet werden. Beispielsweise ist Deny: Class = 08 SubClass=05 eine gültige Regel, Deny: Class=0 Sub Class=05 hingegen nicht.
- Tags müssen den Übereinstimmungsoperator = verwenden. Beispielsweise VID=1230.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.

> **Hinweis:**
>
> Wenn Sie die ADM-Vorlagendatei verwenden, müssen Sie die Regeln in einer einzigen Zeile mit

> Semikolons getrennt eingeben.

Beispiele:

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für Hersteller- und Produkt-IDs:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
                Deny: VID=046D # Deny all Logitech products
<!--NeedCopy-->
```

- Das folgende Beispiel zeigt eine vom Administrator definierte USB-Richtlinienregel für eine definierte Klasse, Unterklasse und ein Protokoll:

```
 Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
          Allow: Class=EF SubClass=01 # Allow Sync devices
          Allow: Class=EF # Allow all USB-Miscellaneous devices
<!--NeedCopy-->
```

Verwenden und Entfernen von USB-Geräten

Benutzer können ein USB-Gerät vor oder nach dem Starten einer virtuellen Sitzung anschließen.

Wenn Sie mit Citrix Receiver für Windows arbeiten, gilt Folgendes:

- Geräte, die nach dem Sitzungsbeginn angeschlossen werden, werden unmittelbar im USB-Menü von Desktop Viewer angezeigt.
- Wenn ein USB-Gerät nicht richtig umgeleitet wird, können Sie das Problem u. U. beheben, indem Sie das Gerät erst nach dem Beginn der virtuellen Sitzung anschließen.
- Um Datenverlust zu verhindern, verwenden Sie das Windows-Symbol "Hardware sicher entfernen", bevor Sie das USB-Gerät entfernen.

Steuerung der Sicherheit für USB-Massenspeichergeräte

Die optimierte Unterstützung steht für USB-Massenspeichergeräte zur Verfügung. Sie ist Teil der XenApp- und XenDesktop-Clientlaufwerkzuordnung. Laufwerke auf Benutzergeräten werden automatisch Laufwerksbuchstaben auf dem virtuellen Desktop zugeordneten, wenn Benutzer sich anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt. Um Clientlaufwerkzuordnung zu konfigurieren, verwenden Sie die Einstellung **Clientwechseldatenträger** im Abschnitt Dateiumleitung der ICA-Richtlinieneinstellungen.

Für USB-Massenspeichergeräte können Sie die Clientlaufwerkzuordnung, die generische USB-Umleitung oder beides über Citrix Richtlinien verwenden. Die Hauptunterschiede sind folgende:

Feature	Clientlaufwerkszuordnung	Generische USB-Umleitung
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Nein
Konfigurierbare Leserechte	Ja	Nein
Verschlüsselter Gerätezugriff	Ja, wenn die Verschlüsselung vor dem Zugriff auf das Gerät entsperrt wird	Nein
Sicheres Entfernen des Geräts in einer Sitzung	Nein	Ja, unter der Voraussetzung, dass Benutzer den Empfehlungen des Betriebssystems zum sicheren Entfernen von Geräten folgen.

Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind und ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der Clientlaufwerkzuordnung umgeleitet. Wenn die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktiviert sind, für ein Gerät die automatische Umleitung konfiguriert wurde (siehe https://support.citrix.com/article/CTX123015) und ein Massenspeichergerät vor oder nach dem Sitzungsstart angeschlossen wird, wird es mit der generischen USB-Umleitung umgeleitet.

> **Hinweis:**
>
> Die USB-Umleitung wird für Verbindungen mit geringer Bandbreite (z. B. 50 KBit/s) unterstützt, das Kopieren großer Dateien funktioniert jedoch nicht.

Steuerung des Dateizugriffs bei der Clientlaufwerkzuordnung

Sie können steuern, ob Benutzer Dateien von ihren virtuellen Umgebungen auf ihre Benutzergeräte kopieren können. Standardmäßig ist in der Sitzung Lese-/Schreibzugriff auf Dateien und Ordner auf zugeordneten Clientlaufwerken möglich.

Um zu verhindern, dass Benutzer Dateien und Ordner auf zugeordneten Clientlaufwerken hinzufügen oder ändern, aktivieren Sie die Richtlinieneinstellung **Schreibgeschützter Zugriff auf Clientlaufwerke**. Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie die Einstellung **Clientlaufwerkumleitung** auf **Zugelassen** festlegen und zur Richtlinie hinzufügen.

Drucken

August 18, 2021

Die Druckerverwaltung in Ihrer Umgebung umfasst verschiedene Stufen:

1. Machen Sie sich, falls erforderlich, mit den Druckkonzepten vertraut.
2. Planen der Druckarchitektur. Dazu gehört die Analyse folgender Faktoren: Unternehmensanforderungen, vorhandene Druckinfrastruktur, derzeitige Interaktion von Benutzern und Anwendungen mit Druckvorgängen und das für Ihre Umgebung am besten geeignete Druckverwaltungsmodell.
3. Konfigurieren Sie die Druckumgebung, indem Sie eine Druckerbereitstellungsmethode auswählen und dann Richtlinien zur Bereitstellung Ihres Druckkonzepts erstellen. Aktualisieren Sie Richtlinien, wenn neue Mitarbeiter oder Server hinzugefügt werden.
4. Testen einer Druckkonfiguration, bevor sie den Benutzern bereitgestellt wird.
5. Pflegen Sie die Citrix Druckumgebung durch Verwalten von Druckertreibern und Optimieren der Druckleistung.
6. Beseitigen Sie evtl. auftretende Probleme.

Druckkonzepte

Bevor Sie die Bereitstellung planen, sollten Sie mit folgenden Hauptkonzepten des Druckens vertraut sein:

- Arten der Druckerbereitstellung
- Wie Druckaufträge weitergeleitet werden
- Grundlagen der Druckertreiberverwaltung

Die Druckkonzepte bauen auf denen von Windows auf. Um das Drucken in Ihrer Umgebung zu konfigurieren und erfolgreich zu verwalten, müssen Sie verstehen, wie das Netzwerk- und Clientdrucken in Windows funktioniert und wie das Druckverhalten in dieser Umgebung umgesetzt wird.

Ablauf des Druckprozesses

In dieser Umgebung werden alle Druckvorgänge (durch den Benutzer) auf Maschinen initiiert, auf denen Anwendungen gehostet werden. Druckaufträge werden über den Netzwerkdruckserver oder das Benutzergerät an das Druckgerät weitergeleitet.

Für Benutzer von virtuellen Desktops und Anwendungen gibt es keinen persistenten Arbeitsbereich. Bei Sitzungsende wird der Arbeitsbereich des Benutzers gelöscht, demnach müssen alle Einstellun-

gen zu Beginn jeder Sitzung neu erstellt werden. Bei jedem Start einer neuen Sitzung muss daher die Neuerstellung des Arbeitsbereichs durch das System erfolgen.

Wenn ein Benutzer druckt, übernimmt das System folgende Aufgaben:

- Entscheidung darüber, welche Drucker dem Benutzer bereitgestellt werden. Dies wird als Druckerprovisioning bezeichnet.
- Wiederherstellen der Druckeinstellungen des Benutzers.
- Ermitteln des Standarddruckers für die Sitzung.

Sie können festlegen, wie diese Aufgaben durchgeführt werden, indem Sie die Optionen für das Druckerprovisioning, die Weiterleitung von Druckaufträgen, das Speichern von Druckereigenschaften und die Treiberverwaltung konfigurieren. Bedenken Sie dabei, wie die verschiedenen Einstellungen möglicherweise die Druckleistung in der Umgebung und die Benutzererfahrung beeinflussen.

Druckerprovisioning

Der Prozess, durch den Drucker in einer Sitzung verfügbar gemacht werden, wird als Provisioning bezeichnet. Das Druckerprovisioning wird normalerweise dynamisch abgewickelt. Das heißt, die in einer Sitzung angezeigten Drucker sind nicht vordefiniert und gespeichert. Stattdessen werden die Drucker gemäß der Richtlinien beim Entstehen der Sitzung während der Anmeldung und Wiederverbindung zusammengestellt. Folglich können sich die Drucker je nach Richtlinie, Benutzerort und Netzwerkänderungen ändern, vorausgesetzt, dies spiegelt sich in den Richtlinien wider. Benutzer, die an einen anderen Ort wechseln, bemerken daher möglicherweise Änderungen in ihrem Arbeitsbereich.

Das System überwacht auch clientseitige Drucker und passt automatisch erstellte Drucker in Sitzungen dynamisch an, je nachdem, welche Hinzufügungen, Löschungen und Änderungen an den clientseitigen Druckern vorgenommen werden. Von dieser dynamischen Druckerermittlung profitieren mobile Benutzer, wenn sie über verschiedene Geräte eine Verbindung herstellen.

Die gängigsten Methoden der Druckerbereitstellung sind folgende:

- **Universeller Druckserver** - Der universelle Druckserver von Citrix bietet universelle Druckunterstützung für Netzwerkdrucker. Der universelle Druckserver verwendet den universellen Druckertreiber. Diese Lösung ermöglicht die Verwendung eines einzelnen Treibers auf einer Serverbetriebssystemmaschine und damit den Netzwerkdruck von jedem Gerät aus.

Citrix empfiehlt den Einsatz des universellen Druckservers für Szenarios mit Remote-Druckerservern. Der universelle Druckserver überträgt den Druckauftrag über das Netzwerk in einem optimierten und komprimierten Format, wodurch der Netzwerkverkehr reduziert und die Benutzererfahrung verbessert wird.

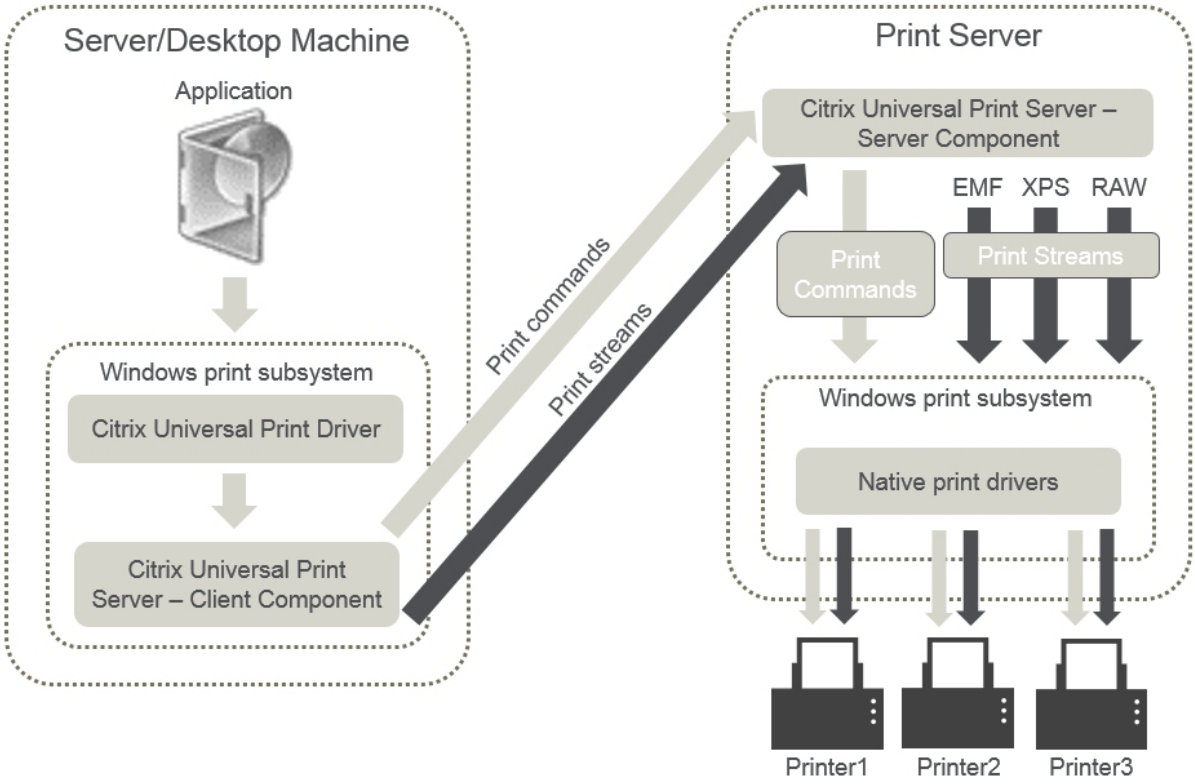
Der universelle Druckserver umfasst als Feature die folgenden Komponenten:

Eine Clientkomponente, **UPClient** - Aktivieren Sie UPClient auf jeder Serverbetriebssystemmaschine, die Sitzungsnetzwerkdrucker bereitstellt und den universellen Druckertreiber verwendet.

Eine Serverkomponente, **UPServer** - Installieren Sie UPServer auf jedem Druckserver, der Sitzungsnetzwerkdrucker bereitstellt, und den universellen Druckertreiber für die Sitzungsdrucker verwendet (unabhängig davon, ob Sitzungsdrucker zentral bereitgestellt werden).

Informationen zu den Anforderungen und zum Setup des universellen Druckservers finden Sie in den Artikeln Systemanforderungen und Installation.

Die folgende Abbildung zeigt den typischen Workflow eines Netzwerkdruckers in einer Umgebung mit universellem Druckserver.



Wenn Sie das Citrix Feature “Universeller Druckserver”aktivieren, wird es von allen verbundenen Netzwerkdruckern automatisch über Autodiscovery genutzt.

> **Hinweis:**
> Der universelle Druckserver wird auch für VDI-in-a-Box 5.3 unterstützt. Informationen zur Installation des universellen Druckservers mit VDI-in-a-Box finden Sie in der Dokumentation zu VDI-in-a-Box.

- **Automatische Erstellung**: *Automatische Erstellung*bezieht sich auf Drucker, die automatisch zu Beginn jeder Sitzung erstellt werden. Sowohl Remotedrucker als auch lokal angeschlossene Drucker können automatisch erstellt werden. Bei Umgebungen mit einer großen Anzahl von Druckern pro Benutzer ist es u. U. besser, nur den Standarddrucker automatisch zu erstellen.

Wenn weniger Drucker automatisch erstellt werden, entsteht auf den Serverbetriebssystemmaschinen weniger Mehraufwand (Arbeitsspeicher und CPU). Eine reduzierte Anzahl an automatisch erstellten Druckern kann auch die Anmeldedauer der Benutzer verkürzen.

Automatisch erstellte Drucker basieren auf:

- Den auf dem Benutzergerät installierten Druckern.
- Den auf die Sitzung angewendeten Richtlinien.

  Durch Richtlinieneinstellungen für die automatische Erstellung können Sie Anzahl oder Art der automatisch erstellten Drucker beschränken. Standardmäßig sind die Drucker in Sitzungen verfügbar, wenn alle Drucker auf dem Benutzergerät automatisch konfiguriert werden, einschließlich der lokal angeschlossenen und der Netzwerkdrucker.

Nachdem der Benutzer die Sitzung beendet, werden die Drucker für diese Sitzung gelöscht.

Mit der automatischen Erstellung von Client- und Netzwerkdruckern sind Wartungsarbeiten verbunden. Bei Hinzufügen eines Druckers muss beispielsweise auch Folgendes durchgeführt werden:

- Aktualisieren der Richtlinieneinstellung Sitzungsdrucker
- Hinzufügen des Treibers zu allen Serverbetriebssystemmaschinen über die Richtlinieneinstellung Druckertreiberzuordnung und -kompatibilität

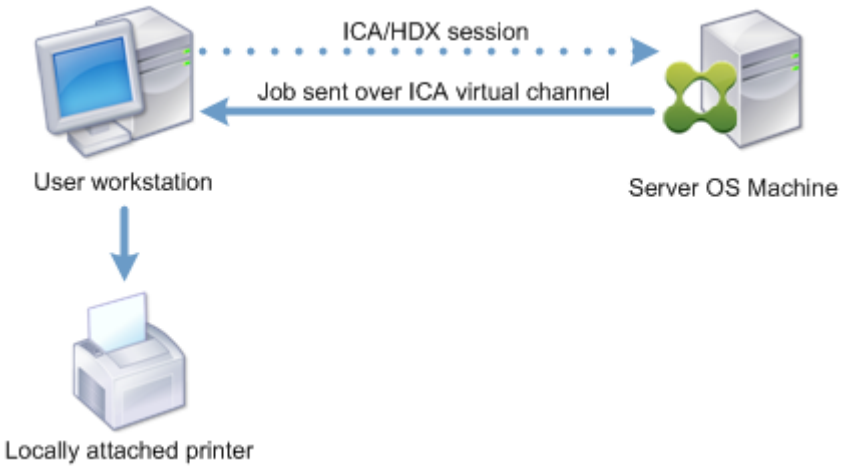
Weiterleiten von Druckaufträgen

Der Begriff Druckpfad umfasst den Pfad, über den Druckaufträge weitergeleitet werden, und den Speicherort, an dem Druckaufträge gespoolt werden. Beide Aspekte dieses Konzepts sind wichtig. Die Weiterleitung wirkt sich auf den Netzwerk-Datenverkehr aus. Das Spooling wirkt sich auf die Auslastung der lokalen Ressourcen an dem Gerät, das den Auftrag verarbeitet, aus.

In dieser Umgebung können Druckaufträge auf zwei Wegen zu einem Druckgerät gelangen: über den Client oder über einen Netzwerkdruckserver. Dafür werden die Bezeichnungen Clientdruckpfad und Netzwerkdruckpfad verwendet. Welcher Pfad standardmäßig ausgewählt wird, hängt vom verwendeten Drucker ab.

Lokal angeschlossene Drucker

Das System leitet Aufträge von der Serverbetriebssystemmaschine über den Client an den Drucker. Der Druckdatenverkehr wird über das ICA-Protokoll optimiert und komprimiert. Wenn ein Druckgerät lokal an das Benutzergerät angeschlossen ist, werden Druckaufträge über den virtuellen ICA-Kanal weitergeleitet.



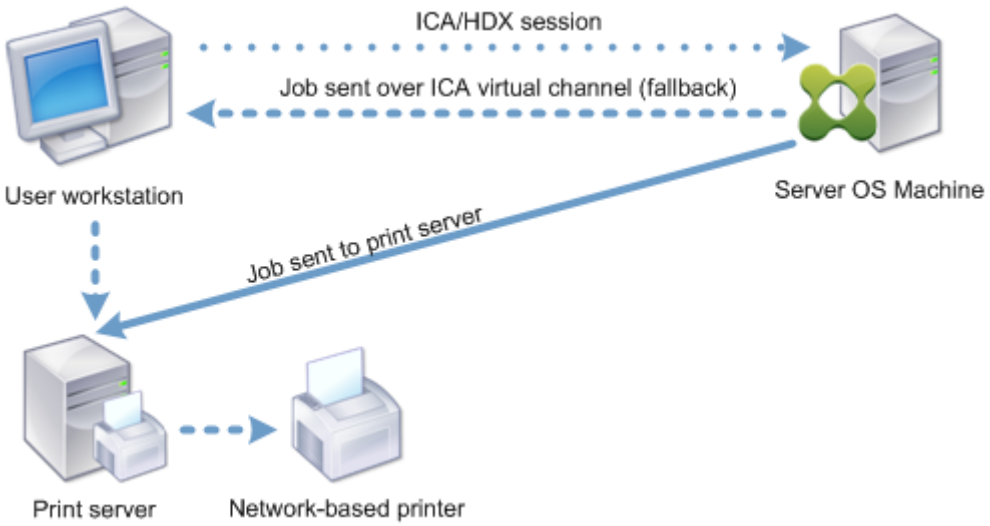
Netzwerkbasierte Drucker

Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Serverbetriebssystemmaschine über das Netzwerk direkt an den Druckserver weitergeleitet. In folgenden Situationen werden jedoch Druckaufträge automatisch über die ICA-Verbindung geleitet:

- Wenn der virtuelle Desktop oder die Anwendung keine Verbindung mit dem Druckserver herstellen kann.
- Wenn der systemeigene Druckertreiber auf der Serverbetriebssystemmaschine nicht verfügbar ist.

Wenn der universelle Druckserver nicht aktiviert ist, empfiehlt sich die Konfiguration des Clientdruckpfads für den Netzwerkdruck bei Verbindungen mit geringer Bandbreite, z. B. WANs, die von der Optimierung und Komprimierung des Datenverkehrs beim Senden von Aufträgen über die ICA-Verbindung profitieren.

Der Clientdruckpfad ermöglicht auch die Begrenzung des Datenverkehrs oder der für Druckaufträge zugeordneten Bandbreite. Wenn die Auftragsleitung über das Benutzergerät nicht möglich ist, z. B. bei Thin Clients ohne Druckerfunktionen, muss die Servicequalität so konfiguriert werden, dass ICA/HDX-Verkehr Vorrang hat und eine gute Benutzererfahrung bei der Sitzung gewährleistet ist.



Druckertreiberverwaltung

Der universelle Citrix Druckertreiber (UPD) ist ein geräteunabhängiger, mit den meisten Druckern kompatibler Druckertreiber. Der Citrix UDP besteht aus zwei Komponenten:

Serverkomponente. Der Citrix UPD wird als Teil des XenApp- oder XenDesktop-VDAs installiert. Mit dem VDA werden die folgenden Citrix UPD-Treiber installiert: Citrix Universeller Drucker (EMF-Treiber) und Citrix XPS Universeller Drucker (XPS-Treiber).

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

Wenn ein Druckauftrag initiiert wird, sendet der Treiber die Ausgabe der Anwendung ohne Änderung an das Endpunktgerät.

Clientkomponente. Der Citrix UPD wird als Teil von Citrix Receiver installiert. Er ruft den eingehenden Druckdatenstrom der XenApp- oder XenDesktop-Sitzung ab. Er leitet diesen dann an das lokale Drucksubsystem weiter, wo der Druckauftrag mit den gerätespezifischen Druckertreibern verarbeitet wird. Neben Citrix UPD kann der universelle Citrix PDF-Druckertreiber separat mit Citrix Receiver für HTML5 und Citrix Receiver für Chrome installiert werden.

Der Citrix UPD unterstützt die folgenden Druckformate:

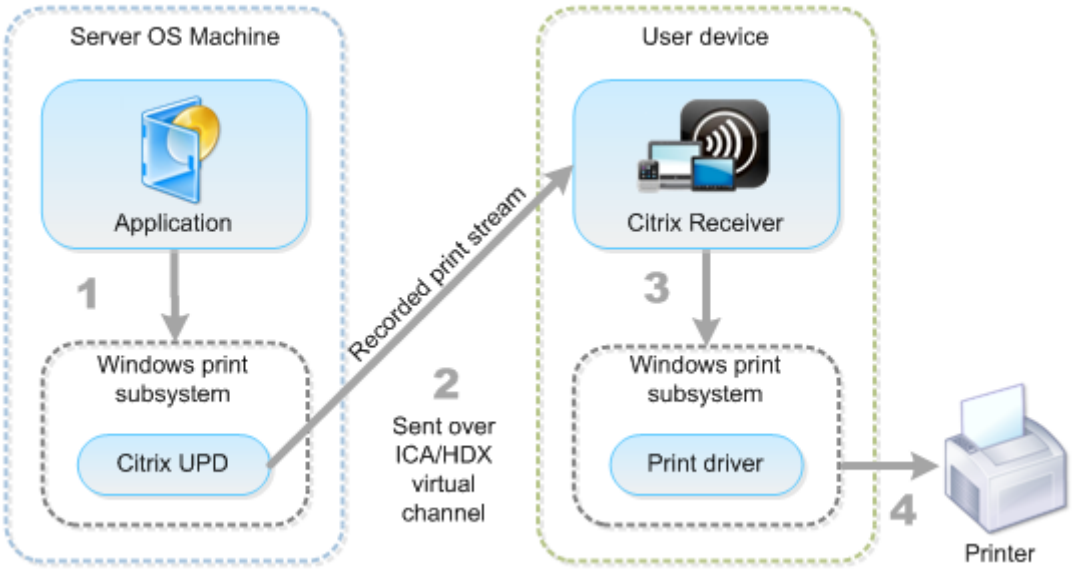
- Enhanced Metafile Format (**EMF**), Standard. EMF ist die 32-Bit-Version von Windows Metafile Format (WMF). Der EMF-Treiber kann nur von Windows-Clients verwendet werden.
- XML-Papierspezifikation (**XPS**). Der Windows XPS-Treiber verwendet XML zum Erstellen eines plattformunabhängigen elektronischen Dokuments, das mit dem Adobe PDF-Format vergleichbar ist.

- Printer Command Language (**PCL5c** und **PCL4**). PCL ist ein ursprünglich von Hewlett-Packard für Tintenstrahldrucker entwickeltes Druckprotokoll. Es wird für den Druck einfacher Text- und Grafikelemente verwendet und wird von vielen LaserJet- und Multifunktionsgeräten von HP unterstützt.
- PostScript (**PS**). PostScript ist eine Computersprache zum Drucken von Text und Vektorgrafiken. Der Treiber wird in vielen Druckern und Multifunktionsgeräten des unteren Preissegments verwendet.

Die PCL- und PS-Treiber sind am besten für nicht-Windows-Geräte, wie z. B. Mac- oder UNIX-Clients geeignet. Die Reihenfolge, in der der Citrix UPD die Verwendung der Treiber versucht, kann mit der Richtlinieneinstellung Priorität universeller Treiber geändert werden.

Der Citrix UDP (EMF- und XPS-Druckertreiber) unterstützt erweiterte Druckerfunktionen wie Heftung und Auswahl der Papierzufuhr. Die Funktionen sind verfügbar, wenn sie durch den nativen Treiber über Microsoft Print Capability zur Verfügung gestellt werden. Der native Treiber muss die standardisierten Druckschemastichwörter in der XML-Datei mit den Druckfunktionen verwenden. Werden nicht standardmäßige Stichwörter verwendet, stehen die erweiterten Druckfunktionen über den universellen Citrix Druckertreiber nicht zur Verfügung.

Die folgende Abbildung zeigt die universellen Druckertreiberkomponenten und einen typischen Workflow für ein lokal angeschlossenes Druckgerät.

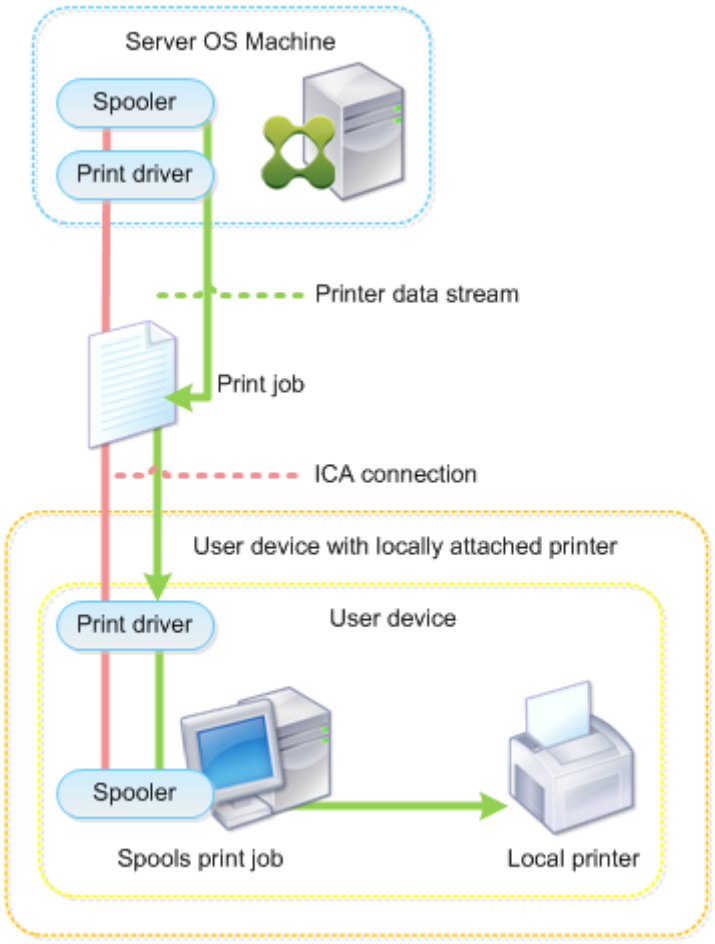


Legen Sie bei der Planung der Strategie zur Treiberverwaltung fest, ob Sie gerätespezifische Treiber, den universellen Druckertreiber oder beides unterstützen wollen. Wenn Sie Standardtreiber unterstützen, müssen Sie außerdem Folgendes festlegen:

Wenn das System während der automatischen Druckererstellung erkennt, dass ein neuer lokaler Drucker an einem Benutzergerät angeschlossen ist, wird die Serverbetriebssystemmaschine auf den

erforderlichen Druckertreiber hin überprüft. Ist kein Windows-systemeigener Treiber verfügbar, wird vom System standardmäßig der universelle Druckertreiber verwendet.

Der Druckvorgang kann nur dann erfolgreich ausgeführt werden, wenn der Druckertreiber auf der Serverbetriebssystemmaschine und der Treiber auf dem Benutzergerät übereinstimmen. In der folgenden Abbildung wird dargestellt, wie der Druckertreiber an zwei Orten für den Clientdruck verwendet wird.



- Zu unterstützende Treibertypen
- Aktivieren oder Deaktivieren der automatischen Installation der Druckertreiber (falls auf Serverbetriebssystemmaschinen nicht vorhanden)
- Erstellen der Treiberkompatibilitätslisten

Verwandter Inhalt

- Druckkonfigurationsbeispiele
- Bewährte Methoden, Überlegungen zur Sicherheit und Standardvorgänge
- Druckrichtlinien und Einstellungen

- Druckerprovisioning
- Pflegen der Druckumgebung

Druckkonfigurationsbeispiele

February 22, 2019

Die Auswahl der am besten geeigneten Druckkonfigurationsoptionen für die Anforderungen und die Umgebung kann die Verwaltung vereinfachen. Obwohl die Standarddruckkonfiguration für die meisten Umgebungen geeignet ist, gewährleisten die Standardwerte möglicherweise nicht die erwartete Benutzererfahrung oder die optimale Netzwerkverwendung und den gewünschten Verwaltungsaufwand für die Umgebung.

Die Druckkonfiguration hängt von folgenden Faktoren ab:

- Den Unternehmensanforderungen und der vorhandenen Druckinfrastruktur.

  Berücksichtigen Sie bei der Druckkonfiguration die Anforderungen der Organisation. Die vorhandene Druckimplementierung (ob Benutzer Drucker hinzufügen können, welche Benutzer Zugriff auf welche Drucker haben usw.) kann bei der Definition der Druckkonfiguration ein nützlicher Leitfaden sein.

- Ob in Ihrer Organisation Sicherheitsrichtlinien gelten, die Drucker für bestimmte Benutzer reservieren (z. B. Drucker für die Personalabteilung oder die Gehaltsabrechnung).
- Ob Benutzer drucken müssen, wenn sie nicht an ihrem primären Arbeitsort sind, z. B. Mitarbeiter, die verschiedene Arbeitsstationen verwenden oder auf Geschäftsreisen gehen.

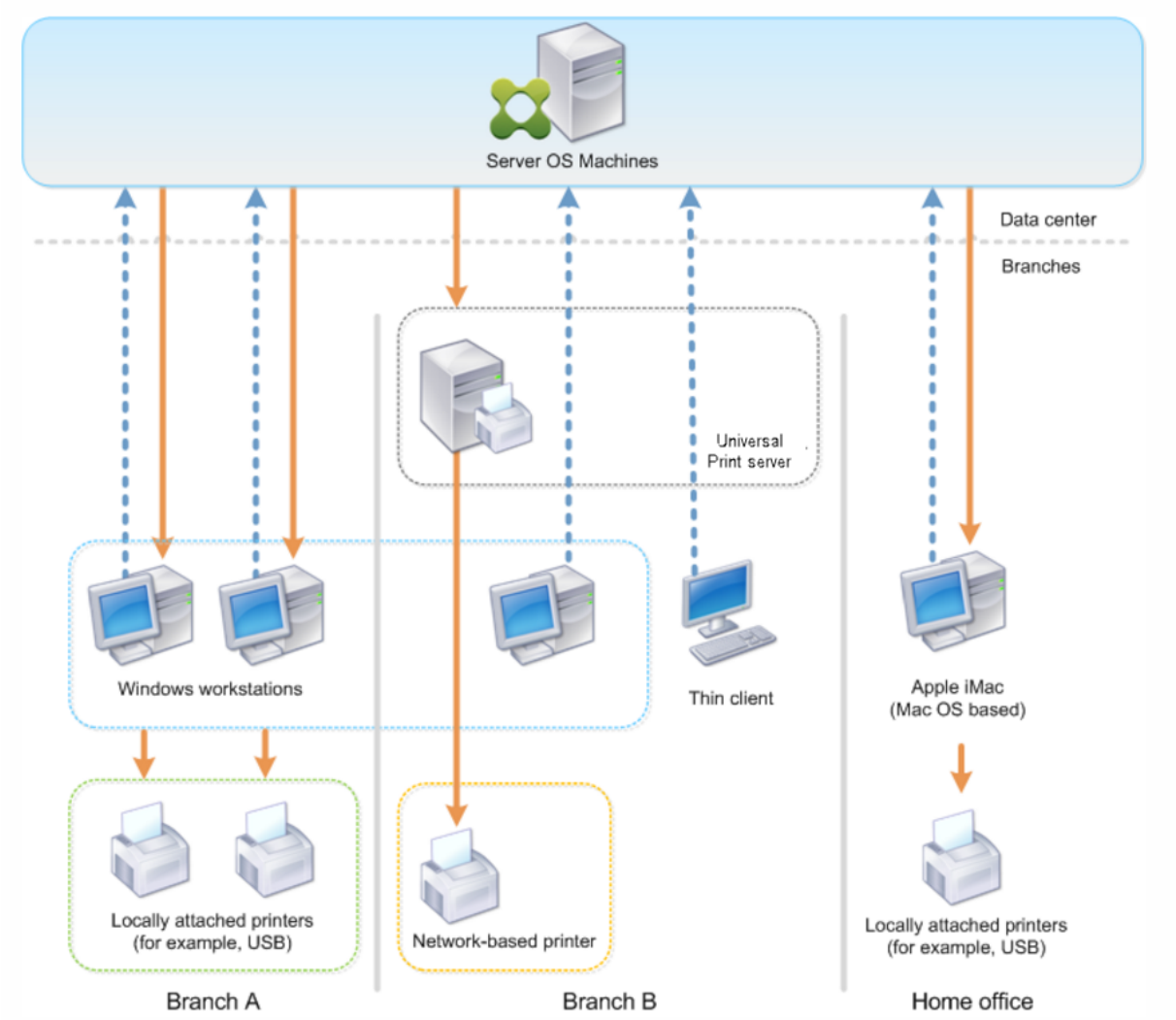
Achten Sie beim Entwerfen der Druckkonfiguration darauf, den Benutzern die gleiche Erfahrung in einer Sitzung zu bieten, wie sie es beim Drucken von lokalen Benutzergeräten aus gewohnt sind.

Beispiel einer Druckbereitstellung

Die folgende Abbildung zeigt die Bereitstellung dieser Anwendungsfälle:

- **Branch A:** kleine Auslandsniederlassung mit einigen Windows-Arbeitsstationen. Jede Benutzerarbeitsstation hat einen lokal angeschlossenen, privaten Drucker.
- **Branch B:** großes Zweigstellenbüro mit Thin Clients und Windows-Arbeitsstationen. Aus Effizienzgründen teilen sich die Benutzer dieser Zweigstelle die Netzwerkdrucker (einen pro Stockwerk). Die Druckwarteschlangen werden über Windows-Druckserver der Zweigstelle gesteuert.

- **Home office:** Büro im Haus eines Mitarbeiters mit einem Mac OS-Gerät, über das auf die Citrix Infrastruktur des Unternehmens zugegriffen wird. Das Benutzergerät hat einen lokal angeschlossenen Drucker.



In den folgenden Abschnitten werden Konfigurationen beschrieben, die die Komplexität der Umgebung minimieren und die Verwaltung vereinfachen.

Automatisch erstellte Clientdrucker und der universelle Citrix Druckertreiber

In Branch A arbeiten alle Benutzer auf Arbeitsstationen unter Windows und verwenden daher automatisch erstellte Clientdrucker und den universellen Druckertreiber. Dies bietet folgende Vorteile:

- Leistung: Druckaufträge werden über den ICA-Druckkanal geleitet, sodass die Druckdaten komprimiert werden können und Bandbreite eingespart wird.

  Um sicherzustellen, dass ein einzelner Benutzer durch den Druck eines großen Dokuments nicht

die Sitzungsleistung anderer Benutzer beeinträchtigt, wird eine Citrix Richtlinie für die maximale Druckbandbreite konfiguriert.

Eine andere Lösung wäre die Multistream-ICA-Verbindung, bei der der Druckverkehr innerhalb einer separaten TCP-Verbindung mit niedriger Priorität übertragen wird. Multistream-ICA kann verwendet werden, wenn Quality of Service (QoS) über die WAN-Verbindung nicht implementiert ist.

- Flexibilität: Der universelle Citrix Druckertreiber gewährleistet, dass alle mit dem Client verbundenen Drucker auch von virtuellen Desktop- oder Anwendungssitzungen verwendet werden können, ohne dass ein neuer Druckertreiber im Datencenter integriert werden muss.

Universeller Citrix Druckserver

In Branch B werden alle Netzwerkdrucker und ihre Warteschlangen auf einem Windows-Druckerserver verwaltet. Somit erweist sich der universelle Citrix Druckserver als die effizienteste Konfiguration.

Alle erforderlichen Druckertreiber werden von lokalen Administratoren auf dem Druckserver installiert und verwaltet. Das Zuordnen von Druckern in virtuellen Desktop- oder Anwendungssitzungen funktioniert wie folgt:

- Arbeitsstationen unter Windows: Das IT-Team vor Ort hilft den Benutzern beim Herstellen der Verbindung mit dem geeigneten Netzwerkdrucker auf ihren Windows-Arbeitsstationen. Dies ermöglicht Benutzern, über lokal installierte Anwendungen zu drucken.

  Bei virtuellen Desktop- oder Anwendungssitzungen werden die lokal konfigurierten Drucker über die automatische Erstellung aufgelistet. Der virtuelle Desktop oder die virtuelle Anwendung stellt dann eine Verbindung mit dem Druckserver her, falls möglich, als Direktnetzwerkverbindung.

  Die Komponenten des universellen Citrix Druckservers werden installiert und aktiviert, systemeigene Druckertreiber sind nicht erforderlich. Falls ein Treiber aktualisiert oder eine Druckerwarteschlange geändert wird, ist im Datencenter keine weitere Konfiguration nötig.

- Thin Clients: Für Thin Client-Benutzer müssen die Drucker in den virtuellen Desktop- oder Anwendungssitzungen angeschlossen werden. Um den Benutzern das Drucken so einfach wie möglich zu machen, konfigurieren die Administratoren eine einzige Citrix Sitzungsdruckerrichtlinie pro Stockwerk, damit der jeweilige Drucker als Standarddrucker festgelegt wird.

  Damit sichergestellt ist, dass die Benutzer stets mit dem richtigen Drucker verbunden sind, auch wenn sie in einem anderen Stockwerk sind, werden die Richtlinien nach Subnetz oder Thin Client-Namen gefiltert. Diese Konfiguration, die auch als “Proximitydrucken”bezeichnet wird, lässt die Wartung lokaler Druckertreiber zu (gemäß der delegierten Administration).

Wenn eine Druckerwarteschlange geändert oder hinzugefügt werden muss, müssen Citrix Administratoren die entsprechende Richtlinie für Sitzungsdrucker in der Umgebung ändern.

Da der Netzwerkdruckdatenverkehr außerhalb des virtuellen ICA-Kanals gesendet wird, wird QoS implementiert. Eingehende und ausgehende Netzwerkdaten an Ports für ICA/HDX-Datenverkehr haben Vorrang vor sonstigem Netzwerkdatenverkehr. Diese Konfiguration gewährleistet, dass Benutzersitzungen von großen Druckaufträgen nicht beeinträchtigt werden.

Automatisch erstellte Clientdrucker und der universelle Citrix Druckertreiber

Bei Heimbüros mit nicht standardmäßigen Arbeitsstationen und nicht verwalteten Druckgeräten ist es am einfachsten, automatisch erstellte Drucker und den universellen Druckertreiber zu verwenden.

Zusammenfassung der Bereitstellung

Zusammenfassend lässt sich die Konfiguration dieses Bereitstellungsbeispiels wie folgt beschreiben:

- Auf Serverbetriebssystemmaschinen werden keine Druckertreiber installiert. Es wird nur der universelle Citrix Druckertreiber verwendet. Fallback auf systemeigene Druckertreiber und die automatische Installation von Druckertreibern sind deaktiviert.
- Die automatische Erstellung von Clientdruckern für alle Benutzer wird über eine Richtlinie konfiguriert. Serverbetriebssystemmaschinen werden standardmäßig direkt mit dem Druckserver verbunden. Zur Konfiguration müssen lediglich die Komponenten des universellen Druckservers aktiviert werden.
- Eine Sitzungsdruckerrichtlinie wird für jedes Stockwerk von Branch B konfiguriert und gilt für alle Thin Clients des jeweiligen Stockwerks.
- Die Implementierung von QoS für Branch B gewährleistet eine hervorragende Benutzererfahrung.

Bewährte Methoden, Überlegungen zur Sicherheit und Standardvorgänge

August 18, 2021

Bewährte Methoden

Viele Faktoren bestimmen die beste Drucklösung für eine bestimmte Umgebung. Einige dieser bewährten Methoden sind möglicherweise für Ihre Site nicht geeignet.

- Verwenden Sie das Citrix Feature "universeller Druckserver".
- Verwenden Sie den universellen Druckertreiber oder Windows-systemeigene Treiber.
- Reduzieren Sie die Anzahl der installierten Druckertreiber auf den Serverbetriebssystemmaschinen auf das Minimum.
- Verwenden Sie Treiberzuordnung zu systemeigenen Treibern.
- Installieren Sie nie ungetestete Druckertreiber in einer Produktionssite.
- Vermeiden Sie Updates von Treibern. Versuchen Sie stets, einen Treiber zu deinstallieren, den Server neu zu starten und dann einen Ersatztreiber zu installieren.
- Deinstallieren Sie nicht verwendete Treiber oder verwenden Sie die Richtlinie Druckertreiberzuordnung und -kompatibilität, um zu verhindern, dass Drucker mit dem Treiber erstellt werden.
- Vermeiden Sie möglichst Kernelmodustreiber der Version 2.
- Wenden Sie sich an den Hersteller oder sehen Sie in der Citrix Ready-Produktdokumentation www.citrix.com/ready nach, ob ein Druckermodell unterstützt wird.

  Im Allgemeinen werden alle von Microsoft zur Verfügung gestellten Druckertreiber mit Terminaldiensten getestet und ihre Funktion unter Citrix gewährleistet. Vergewissern Sie sich jedoch vor Einsatz eines Druckertreibers eines Drittanbieters, dass der Treiber von Windows Hardware Quality Labs (WHQL) für Terminaldienste zertifiziert wurde. Citrix vergibt keine Zertifizierung für Druckertreiber.

Sicherheitsüberlegungen

Citrix Drucklösungen sind inhärent sicher.

- Der Citrix Druckmanagerdienst überwacht und reagiert fortlaufend auf Sitzungsereignisse wie An- und Abmeldung, Trennen, Wiederverbinden und Beenden der Sitzung. Er behandelt Anforderungen, indem er die Identität des Benutzers der aktuellen Sitzung übernimmt.
- Beim Citrix Drucken wird jedem Drucker ein eindeutiger Namespace in einer Sitzung zugewiesen.
- Citrix-Drucken richtet die Standardsicherheitsbeschreibung für automatisch erstellte Drucker ein, um sicherzustellen, dass die in einer Sitzung automatisch erstellten Clientdrucker für Benutzer in anderen Sitzungen nicht zugänglich sind. Standardmäßig können Administratoren nicht versehentlich auf einem Clientdrucker einer anderen Sitzung drucken, obwohl sie jeden Clientdrucker sehen und die Berechtigungen dafür manuell ändern können.

Standarddruckvorgänge

Wenn Sie keine Richtlinienregeln konfigurieren, zeigt sich standardmäßig das folgende Druckverhalten:

- Universeller Druckserver ist deaktiviert.
- Alle auf dem Benutzergerät konfigurierten Drucker werden automatisch zu Beginn jeder Sitzung konfiguriert.

  Dieses Verhalten entspricht der Citrix-Richtlinieneinstellung "Clientdrucker automatisch erstellen"mit der Option "Alle Clientdrucker automatisch erstellen".
- Das System leitet alle Druckaufträge, die in Warteschlangen für an Benutzergeräte lokal angeschlossene Drucker gestellt wurden, als Clientdruckaufträge weiter (d. h. über den ICA-Kanal und durch das Benutzergerät).
- Das System leitet alle Druckaufträge, die in Warteschlangen von Netzwerkdruckern gestellt wurden, direkt über Serverbetriebssystemmaschinen. Falls die Aufträge vom System nicht über das Netzwerk weitergeleitet werden können, werden sie als umgeleiteter Clientdruckauftrag über das Benutzergerät weitergeleitet.

  Dieses Verhalten entspricht dem Deaktivieren der Citrix Richtlinieneinstellung Direkte Verbindungen zu Druckservern.
- Standardmäßig versucht das System, die Druckeigenschaften (eine Kombination aus den Druckeinstellungen des Benutzers und den gerätespezifischen Druckeinstellungen) auf dem Benutzergerät zu speichern. Wenn der Client diesen Vorgang nicht unterstützt, werden die Druckeigenschaften vom System in Benutzerprofilen auf der Serverbetriebssystemmaschine gespeichert.

  Dieses Verhalten entspricht der Citrix Richtlinieneinstellung Speicherung von Druckereigenschaften mit der Option Nur im Profil speichern, wenn sie nicht auf dem Client gespeichert sind.
- Das System verwendet die Windows-Version des Druckertreibers, falls sie auf der Serverbetriebssystemmaschine verfügbar ist. Ist der Druckertreiber nicht verfügbar, versucht das System, den Treiber vom Windows-Betriebssystem zu installieren. Ist der Treiber in Windows nicht verfügbar, wird ein universeller Citrix Druckertreiber verwendet.

  Dieses Verhalten entspricht dem Aktivieren der Citrix Richtlinieneinstellung "Automatische Installation von mitgelieferten Druckertreibern"und Konfigurieren der Einstellung "Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist".

  Das Aktivieren von Automatische Installation von mitgelieferten Druckertreibern kann dazu führen, dass eine große Anzahl systemeigener Druckertreiber installiert wird.

Hinweis: Wenn Sie nicht sicher sind, welche Standardwerte voreingestellt sind, zeigen Sie sie an, indem Sie eine neue Richtlinie erstellen und alle Druckrichtlinienregeln aktivieren. Die angezeigte Option ist die Standardoption.

Immer aktive Protokollierung

Eine Always-On-Protokollierung ist für den Druckserver und das Drucksubsystem auf dem VDA verfügbar.

Zum Sortieren der Protokolle als ZIP-Datei für den E-Mail-Versand bzw. für den automatischen Upload an Citrix Insight Services verwenden Sie das PowerShell-Cmdlet **Start-TelemetryUpload**.

Druckrichtlinien und Einstellungen

August 18, 2021

Wenn Benutzer von veröffentlichten Anwendungen aus auf Drucker zugreifen, können Sie über Citrix Richtlinien Folgendes konfigurieren:

- Wie das Drucker-Provisioning erfolgt (bzw. wie Drucker zu Sitzungen hinzugefügt werden)
- Wie Druckaufträge weitergeleitet werden
- Wie Druckertreiber verwaltet werden

Sie können verschiedene Druckkonfigurationen für unterschiedliche Benutzergeräte, Benutzer oder beliebige andere Objekte haben, nach denen Richtlinien gefiltert werden.

Die meisten Druckfunktionen werden über die Citrix Druckrichtlinieneinstellungen konfiguriert. Druckeinstellungen folgen dem Standardverhalten für Citrix Richtlinien.

Druckereinstellungen können vom System am Ende einer Sitzung in das Druckerobjekt oder das Clientdruckgerät geschrieben werden, sofern das Netzwerkkonto des Benutzers ausreichende Berechtigungen hat. Standardmäßig verwendet Citrix Receiver die Einstellungen, die im Druckerobjekt in der Sitzung gespeichert wurden, bevor an anderen Orten nach Einstellungen gesucht wird.

Standardmäßig werden die Druckereigenschaften auf dem Benutzergerät (falls vom Gerät unterstützt) oder im Benutzerprofil auf der Serverbetriebssystemmaschine gespeichert oder beibehalten. Wenn die Druckereigenschaften während einer Sitzung vom Benutzer geändert werden, werden diese Änderungen im Benutzerprofil auf der Maschine aktualisiert. Wenn sich der Benutzer das nächste Mal anmeldet oder eine neue Verbindung herstellt, übernimmt das Benutzergerät die beibehaltenen Einstellungen. Das heißt, auf dem Benutzergerät geänderte Druckereigenschaften wirken sich nicht auf die aktuelle Sitzung aus bis zum Ab- und Neuanmelden des Benutzers.

Speicherorte für Druckeinstellungen

In Windows-Druckumgebungen können die an den Druckvoreinstellungen vorgenommenen Änderungen auf dem lokalen Computer oder in einem Dokument gespeichert werden. Wenn Benutzer in dieser Umgebung Druckeinstellungen ändern, können diese Änderungen an folgenden Positionen gespeichert werden:

- **Auf dem Benutzergerät:** Windows-Benutzer können Geräteeinstellungen auf dem Benutzergerät ändern, indem sie mit der rechten Maustaste auf die Drucker in der Systemsteuerung klicken und "Druckeinstellungen"wählen. Wenn beispielsweise "Querformat"als Seitenausrichtung ausgewählt wird, gilt Querformat als Standard-Seitenausrichtung für diesen Drucker.
- **In einem Dokument:** Bei Textverarbeitungs- und Desktop-Publishing-Programmen werden Dokumenteinstellungen, z. B. die Seitenausrichtung, häufig in Dokumenten gespeichert. Wenn Sie beispielsweise ein zu druckendes Dokument in eine Warteschlange setzen, speichert Microsoft Word die von Ihnen angegebenen Druckvoreinstellungen wie Seitenausrichtung und Druckername im Dokument selbst. Diese Einstellungen erscheinen standardmäßig, wenn Sie dieses Dokument das nächste Mal drucken.
- **Benutzerseitige Änderungen in einer Sitzung:** Das System übernimmt Änderungen an den Druckeinstellungen eines automatisch erstellten Druckers nur, wenn diese in der Systemsteuerung der Sitzung, also auf der Serverbetriebssystemmaschine, vorgenommen wurden.
- **Auf der Serverbetriebssystemmaschine:** Dies sind die Standardeinstellungen, die einem bestimmten Druckertreiber auf der Maschine zugeordnet sind.

Die in einer Windows-Umgebung gespeicherten Einstellungen sind abhängig von der Stelle, an der die Einstellungen vom Benutzer vorgenommen wurden. Das bedeutet außerdem, dass die an einer Stelle wie einer Tabellenkalkulation angezeigten Druckeinstellungen sich von den Einstellungen an anderen Stellen, beispielsweise in Dokumenten, unterscheiden können. Die auf einen bestimmten Drucker angewendeten Druckeinstellungen variieren daher innerhalb einer Sitzung.

Hierarchie der Benutzerdruckeinstellungen

Da die Druckeinstellungen an verschiedenen Stellen gespeichert werden können, verarbeitet das System sie gemäß einer bestimmten Priorität. Sie dürfen auch nicht vergessen, dass Geräteeinstellungen anders behandelt werden als Dokumenteinstellungen und normalerweise Vorrang vor diesen haben.

Standardmäßig wendet das System immer alle Druckeinstellungen an, die ein Benutzer während einer Sitzung geändert hat, d. h. alle beibehaltenen Einstellungen, bevor andere Einstellungen berücksichtigt werden. Wenn der Benutzer druckt, führt das System die auf der Serverbetriebssystemmaschine gespeicherten Standarddruckereinstellungen mit allen beibehaltenen Einstellungen oder Clientdruckeinstellungen zusammen und wendet sie an.

Speichern der Druckeinstellungen des Benutzers

Citrix empfiehlt, dass Sie den Speicherort der Druckereigenschaften nicht ändern. Am einfachsten können Sie konsistente Druckereigenschaften sicherstellen, indem Sie die Standardeinstellung beibehalten, wonach die Druckereigenschaften auf dem Benutzergerät gespeichert werden. Wenn das System die Eigenschaften auf dem Benutzergerät nicht speichern kann, wird automatisch auf das Benutzerprofil auf der Serverbetriebssystemmaschine zurückgegriffen.

Überprüfen Sie die Richtlinieneinstellung Speicherung von Druckereigenschaften, wenn diese Szenarios zutreffen:

- Verwendung von älteren Plug-Ins, durch die das Speichern der Druckereigenschaften durch die Benutzer auf einem Benutzergerät unterbunden wird
- Verwendung verbindlicher Profile im Windows-Netzwerk, wobei die Druckereigenschaften der Benutzer beibehalten werden sollen

Druckerprovisioning

August 18, 2021

Universeller Citrix Druckserver

Bei der Wahl der besten Drucklösung für Ihre Umgebung sollten Sie Folgendes berücksichtigen:

- Der universelle Druckserver bietet Features, die beim Windows-Druckanbieter nicht verfügbar sind: Zwischenspeichern von Bildern und Schriftarten, erweiterte Komprimierung, Optimierung und Unterstützung für QoS.
- Der universelle Druckertreiber unterstützt die von Microsoft definierten, öffentlichen geräteunabhängigen Einstellungen. Wenn Benutzer Zugriff auf die Geräteeinstellungen des Druckertreibers eines bestimmten Herstellers benötigen, stellt der universelle Druckserver gepaart mit einem Windows-systemeigenen Treiber die beste Lösung dar. In dieser Konfiguration bleiben die Vorteile des universellen Druckservers erhalten und die Benutzer können zugleich auf bestimmte Druckerfunktionen zugreifen. Allerdings ist zu bedenken, dass Windows-systemeigene Treiber wartungsbedürftig sind.
- Der universelle Druckserver von Citrix bietet universelle Druckunterstützung für Netzwerkdrucker. Der universelle Druckserver verwendet den universellen Druckertreiber, einen einzelnen Treiber auf der Serverbetriebssystemmaschine, mit dem von jedem Gerät aus, einschließlich Thin Clients und Tablets, auf lokalen oder Netzwerkdruckern gedruckt werden kann.

Um den universellen Druckserver mit einem Windows-systemeigenen Treiber zu verwenden, aktivieren Sie den universellen Druckserver. Wenn der Windows-systemeigene Treiber verfügbar ist, wird er standardmäßig verwendet. Andernfalls wird der universelle Druckertreiber verwendet. Um dieses Verhalten zu ändern, beispielsweise zur ausschließlichen Verwendung des Windows-systemeigenen Treibers oder des universellen Druckertreibers, müssen Sie die Richtlinieneinstellung Verwendung universeller Druckertreiber aktualisieren.

Installieren des universellen Druckservers

Zum Verwenden des universellen Druckservers installieren Sie die UpsServer-Komponente, wie in den Dokumenten zur Installation beschrieben, auf den Druckservern und konfigurieren Sie sie. Weitere Informationen finden Sie unter Installieren von Kernkomponenten und Installieren über die Befehlszeile.

In Umgebungen, in denen Sie die UPClient-Komponente separat bereitstellen, z. B. mit **XenApp 6.5**:

1. Laden Sie das eigenständige Paket für den XenApp und XenDesktop Virtual Delivery Agent (VDA) für Windows-Desktopbetriebssysteme oder Windows-Serverbetriebssysteme herunter.
2. Extrahieren Sie den VDA anhand der Anweisungen unter Installieren über die Befehlszeile.
3. Installieren Sie die Voraussetzungen aus \Image-Full\Support\VcRedist_2013_RTM
    - Vcredist_x64 / vcredist_x86
        - Führen Sie x86 nur bei 32-Bit-Bereitstellungen aus und beide bei 64-Bit-Bereitstellungen
4. Installieren Sie die CDF-Voraussetzung aus \Image-Full\x64\Virtual Desktop Components oder \Image-Full\x86\Virtual Desktop Components.
    - Cdf_x64 / Cdf_x86
        - x86 für 32 Bit, x64 für 64 Bit
5. Navigieren Sie zur UPClient-Komponente in \Image-Full\x64\Virtual Desktop Components oder in \Image-Full\x86\Virtual Desktop Components.
6. Installieren Sie die UPClient-Komponente, indem Sie die MSI der Komponente extrahieren und starten.
7. Nach der Installation der UPClient-Komponente ist ein Neustart erforderlich.

Deaktivieren der Teilnahme am CEIP für den universellen Druckserver

Bei der Installation des universellen Druckservers werden Sie automatisch für das Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) registriert. Der erste Upload von Daten erfolgt sieben Tage nach der Installation.

Zum Deaktivieren der Teilnahme am CEIP legen Sie den **DWORD**-Wert des Registrierungsschlüssels **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** auf **0** fest.

Wenn Sie anschließend wieder teilnehmen möchten, legen Sie den DWORD-Wert auf 1 fest.

> **Achtung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Weitere Informationen finden Sie unter Citrix Insight Services.

Konfigurieren des universellen Druckservers

Verwenden Sie die folgenden Citrix Richtlinieneinstellungen zum Konfigurieren des universellen Druckservers. Weitere Informationen finden Sie in der Onlinehilfe zu Richtlinieneinstellungen.

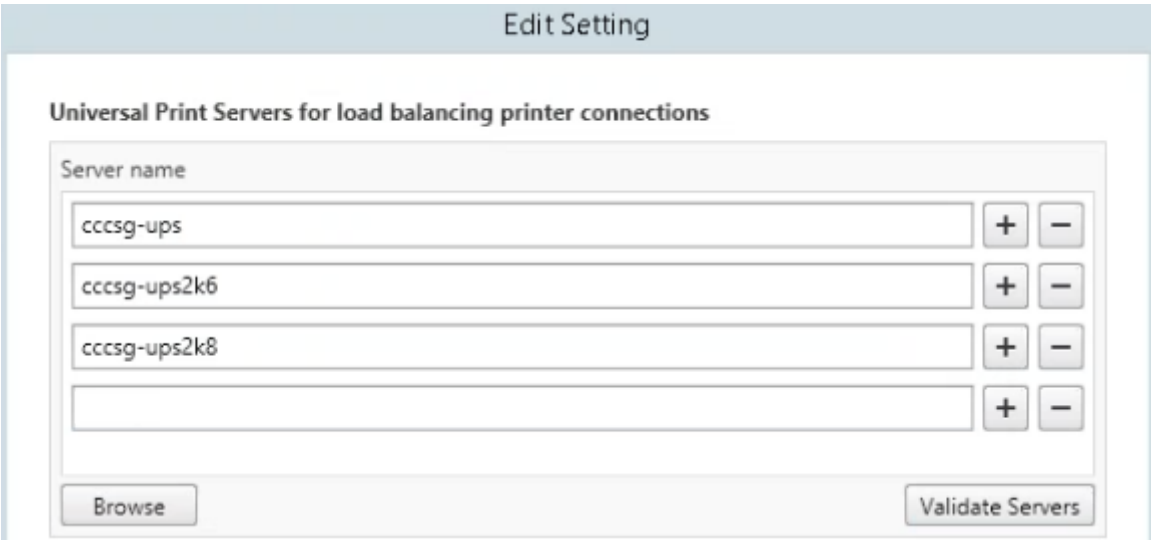
- **Universellen Druckserver aktivieren**: Der universelle Druckserver ist standardmäßig deaktiviert. Wenn Sie ihn aktivieren, müssen Sie festlegen, ob der Windows-Druckanbieter verwendet werden soll, wenn der universelle Druckserver nicht verfügbar ist. Nachdem der universelle Druckserver aktiviert wurde, können Benutzer Netzwerkdrucker über die Windows-Druckanbieter- und Citrix Anbieteroberflächen hinzufügen und auflisten.
- **Port für Druckdatenstrom des universellen Druckservers (CGP)**: Gibt die Nummer des TCP-Ports an, die vom Druckdatenstrom-Listener (CGP) des universellen Druckservers verwendet wird. Standardwert ist **7229**.
- **Port für universellen Druckserverwebdienst (HTTP/SOAP)**: Gibt die Nummer des TCP-Ports an, der vom Listener des universellen Druckservers für eingehende HTTP/SOAP-Anforderungen verwendet wird. Standardwert: **8080**.

Zum Ändern des HTTP-Standardports 8080 für die Kommunikation zwischen universellem Druckserver und XenApp- bzw. XenDesktop-VDAs müssen Sie außerdem auf Computern mit dem universeller Druckserver den folgenden Registrierungsschlüssel erstellen und die Portnummer ändern:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies
“UpsHttpPort”=DWORD:<Portnummer>

Diese Portnummer muss mit dem Port für den universellen Druckserverwebdienst (HTTP/SOAP) der HDX-Richtlinie in Studio übereinstimmen.

- **Universeller Druckserver - Eingabebandbreitenlimit für Druckdatenstrom (KBit/s)**: Gibt das obere Limit (in Kilobit pro Sekunde) für die Übertragungsrate der Druckdaten an, die von jedem Druckauftrag mit CGP an den universellen Druckserver übergeben werden. Standardwert: 0 (unbegrenzt).
- **Universelle Druckserver für den Lastausgleich**: Mit dieser Einstellung werden die universellen Druckserver aufgelistet, die zum Lastausgleich für am Sitzungsstart erstellte Druckerverbindungen verwendet werden, nachdem andere Citrix Druckrichtlinieneinstellungen bewertet wurden. Zum Optimieren der Erstellungszeit von Druckern empfiehlt Citrix, dass alle Druckserver über denselben Satz freigegebener Drucker verfügen.



- **Außer-Betrieb-Schwellenwert für universelle Druckserver**: Gibt an, wie lange der Load Balancer auf die Wiederherstellung eines nicht verfügbaren Druckservers warten muss, bevor er den Server als bleibend offline einstuft und dessen Last auf andere verfügbare Druckserver verteilt. Standardwert ist 180 (Sekunden).

Nach Ändern von Druckrichtlinien auf dem Delivery Controller kann es einige Minuten dauern, bis die Änderungen auf die VDAs angewendet werden.

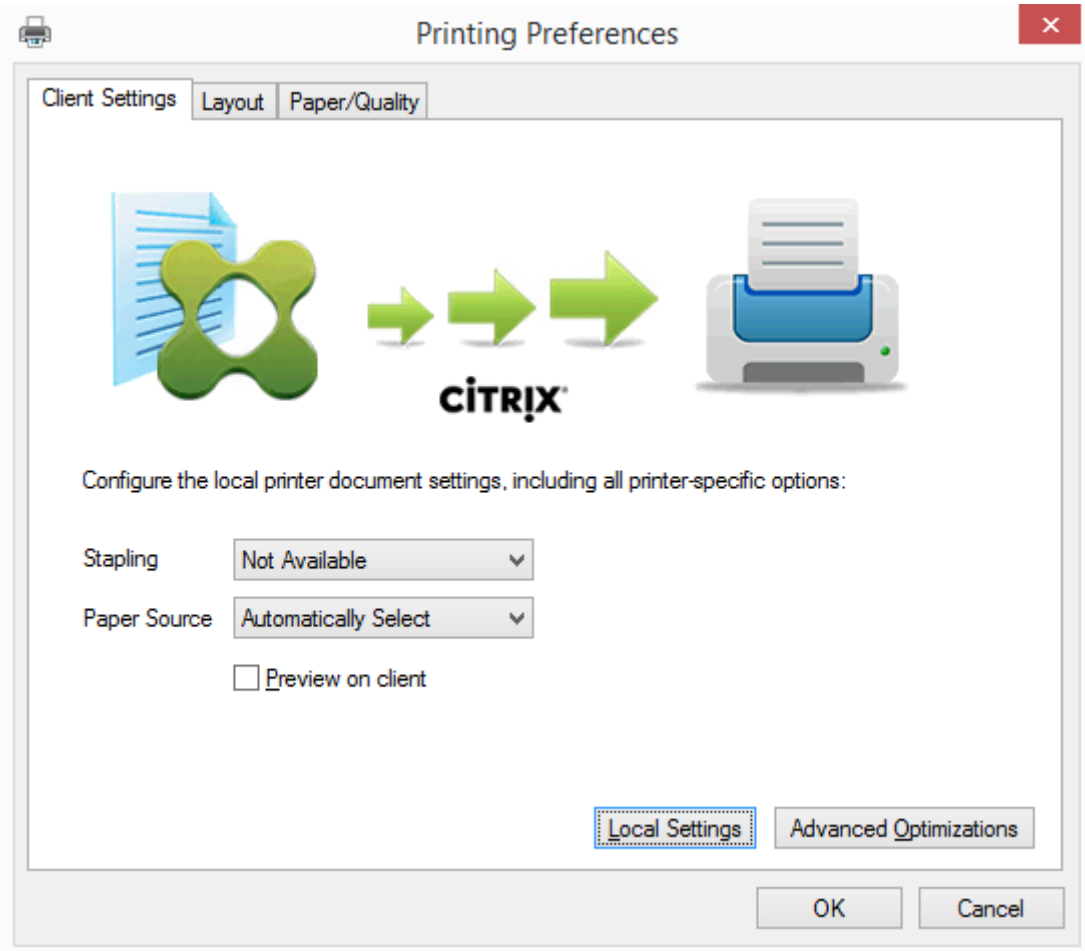
Interaktion mit anderen Richtlinieneinstellungen: Der universelle Druckserver berücksichtigt andere Citrix Druckrichtlinieneinstellungen und interagiert mit diesen (siehe folgende Tabelle). Die Angaben basieren auf folgender Annahme: Die Richtlinieneinstellung “Universeller Druckserver”ist aktiviert, die Komponenten des universellen Druckservers sind installiert und die Richtlinieneinstellungen werden angewendet.

Richtlinieneinstellung	Interaktion
Clientdruckerumleitung, automatisches Erstellen von Clientdruckern	Wenn der universelle Druckserver aktiviert ist, werden Clientnetzwerkdrucker mit dem universellen Druckertreiber statt den systemeigenen Treibern erstellt. Den Benutzern wird der gleiche Druckername wie zuvor angezeigt.
Sitzungsdrucker	Wenn Sie die Citrix Lösung des universellen Druckservers einsetzen, werden die Richtlinieneinstellungen für universelle Druckertreiber berücksichtigt.
Direkte Verbindungen zu Druckserver	Wenn der universelle Druckserver aktiviert ist und die Einstellung für die Richtlinie "Verwendung universeller Druckertreiber"für die ausschließliche Verwendung des universellen Druckens konfiguriert ist, kann mit dem universellen Druckertreiber eine direkte Netzwerkdruckerverbindung mit dem Druckserver erstellt werden.
UPD-Präferenz	Unterstützt EMF- und XPS-Treiber.

Auswirkungen auf Benutzeroberflächen: Der vom universellen Druckserver verwendete universelle Citrix Druckertreiber deaktiviert die folgenden Steuerelemente der Benutzeroberfläche:

- Schaltfläche für die lokalen Druckereinstellungen im Druckereigenschaften-Dialogfeld
- Schaltflächen für die lokalen Druckereinstellungen und die Vorschau im Dokumenteigenschaften-Dialogfeld

Der universelle Citrix Druckertreiber (EMF- und XPS-Druckertreiber) unterstützt erweiterte Druckerfunktionen wie Heftung und Auswahl der Papierzufuhr. Die Benutzer können die Optionen für Heften und Druckmaterialquelle im benutzerdefinierten UPD-Druckdialogfeld wählen, wenn die dem UPD für die Sitzung zugewiesenen Client- bzw. Netzwerkdrucker die Features unterstützen.



Zum Festlegen nicht standardmäßiger Druckereinstellungen wie z. B. Heftung und PIN-Schutz für einen dem Client zugeordneten Drucker, für den der Citrix UPD EMF- oder XPS-Treiber verwendet wird, klicken Sie im UPD-Dialogfeld auf **Lokale Einstellungen**. Das Dialogfeld **Druckeinstellungen** des zugeordneten Druckers wird außerhalb der Sitzung auf dem Client angezeigt, sodass der Benutzer beliebige Druckeroptionen ändern kann und die geänderten Einstellungen in der aktiven Sitzung beim Drucken verwendet werden.

Die Funktionen sind verfügbar, wenn sie durch den nativen Treiber über Microsoft Print Capability zur Verfügung gestellt werden. Der native Treiber muss die standardisierten Druckschemastichwörter in der XML-Datei mit den Druckfunktionen verwenden. Werden nicht standardmäßige Stichwörter verwendet, stehen die erweiterten Druckfunktionen über den universellen Citrix Druckertreiber nicht zur Verfügung.

Beim universellen Druckserver gleicht der Assistent für die Druckerinstallation des Citrix Druckanbieters dem für den Windows-Druckanbieter mit den folgenden Ausnahmen:

- Beim Hinzufügen eines Druckers mit dem Namen oder einer Adresse können Sie eine HTTP/SOAP-Portnummer für den Druckserver angeben. Die Portnummer wird Teil des Druckernamens und wird angezeigt.

- Wenn in der Einstellung für die Citrix-Richtlinie "Verwendung universeller Druckertreiber"festgelegt ist, dass universelles Drucken verwendet werden muss, wird der Name des universellen Druckertreibers bei der Auswahl des Druckers angezeigt. Der Windows-Druckanbieter kann den universellen Druckertreiber nicht verwenden.

Der Citrix Druckanbieter unterstützt kein clientseitiges Rendering.

Weitere Informationen zum universellen Druckserver finden Sie unter CTX200328.

Automatisch erstellte Clientdrucker

Die folgenden universellen Drucklösungen sind für Clientdrucker verfügbar:

- **Citrix Universeller Drucker** - ein generischer Drucker, der zu Beginn einer Sitzung erstellt wird und nicht an ein Druckgerät gebunden ist. Der Citrix Universelle Drucker muss die verfügbaren Clientdrucker bei der Anmeldung nicht auflisten, wodurch sich der Ressourceneinsatz erheblich reduziert und die Anmeldedauer für die Benutzer verringert wird. Mit dem Citrix Universellen Drucker kann auf jedem clientseitigen Druckgerät gedruckt werden.

  Der Citrix Universelle Drucker funktioniert allerdings möglicherweise nicht für alle Benutzergeräte oder Citrix Receiver in Ihrer Umgebung. Der Citrix Universelle Drucker erfordert eine Windows-Umgebung und unterstützt nicht das Citrix Offline Plug-In oder Anwendungen, die an Clients gestreamt werden. Verwenden Sie für solche Umgebungen automatisch erstellte Drucker und den universellen Druckertreiber.

  Wenn Sie eine universelle Drucklösung für Citrix Receiver benötigen, die nicht unter Windows ausgeführt werden, verwenden Sie einen der anderen universellen PostScript/PCL-Druckertreiber, die automatisch installiert werden.

- **Citrix Universeller Druckertreiber** - ein geräteunabhängiger Druckertreiber. Wenn Sie einen universellen Citrix Druckertreiber einrichten, verwendet das System standardmäßig den auf EMF basierenden universellen Druckertreiber.

  Der universelle Citrix Druckertreiber kann auch kleinere Druckaufträge erstellen als ältere oder weniger umfangreiche Druckertreiber. Für Spezialdrucker wird jedoch u. U. ein gerätespezifischer Treiber benötigt, um die Druckaufträge optimal zu verarbeiten.

Konfigurieren von Universal Printing: Verwenden Sie die folgenden Citrix Richtlinieneinstellungen zum Konfigurieren von Universal Printing. Weitere Informationen finden Sie in der Onlinehilfe zu Richtlinieneinstellungen.

- Verwenden universeller Druckertreiber: Mit dieser Einstellung legen Sie fest, wann das universelle Drucken verwendet wird.

- Automatisch generischen universellen Drucker erstellen: Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Erstellung des generischen universellen Citrix Druckerobjekts für Sitzungen mit einem Benutzergerät, das mit Universal Printing kompatibel ist. Standardmäßig werden generische universelle Drucker nicht automatisch erstellt.
- Priorität universeller Treiber: Mit dieser Einstellung geben Sie an, in welcher Reihenfolge das System die universellen Druckertreiber verwendet, angefangen mit dem ersten Eintrag in der Liste. Sie können Treiber hinzufügen, bearbeiten oder entfernen und die Reihenfolge der Treiber in der Liste ändern.
- Universelles Drucken - Vorschaueinstellung Mit dieser Einstellung geben Sie an, ob die Druckvorschau für automatisch erstellte oder universelle Drucker verwendet werden soll.
- Universelles Drucken - EMF-Verarbeitungsmodus Mit dieser Einstellung steuern Sie die Verarbeitungsmethode für die EMF-Spooldatei auf dem Windows-Benutzergerät. Standardmäßig werden EMF-Datensätze direkt zum Drucker gespoolt. Direktes Spoolen an den Drucker ermöglicht eine schnellere Verarbeitung der Datensätze durch den Spooler und beansprucht weniger CPU-Ressourcen.

Weitere Richtlinien finden Sie unter Optimieren der Druckleistung. Informationen zum Ändern der Standardeinstellungen (Papierformat, Druckqualität, Farbe, Seitenaufdruck und Auflage) finden Sie unter CTX113148.

Drucker automatisch über das Benutzergerät erstellen: Zu Beginn einer Sitzung erstellt das System standardmäßig alle Drucker auf dem Benutzergerät automatisch. Sie können steuern, welche Typen der Drucker ggf. den Benutzern bereitgestellt werden und somit ein automatisches Erstellen verhindern.

Verwenden Sie die Citrix Richtlinieneinstellung
“Clientdrucker automatisch erstellen”, um das automatische Erstellen zu steuern. Sie können Folgendes festlegen:

- Alle für das Benutzergerät sichtbaren Drucker, einschließlich der Netzwerkdrucker und der lokal angeschlossenen Drucker, werden zu Beginn einer Sitzung automatisch erstellt (Standardeinstellung)
- Alle lokalen Drucker, die physisch an das Benutzergerät angeschlossen sind, werden automatisch erstellt
- Nur der Standarddrucker für das Benutzergerät wird automatisch erstellt
- Automatische Erstellung ist für alle Clientdrucker deaktiviert

Die Einstellung Clientdrucker automatisch erstellen erfordert, dass für die Einstellung Clientdruckerumleitung die Option Zugelassen (Standardeinstellung) festgelegt ist.

Zuweisen von Netzwerkdruckern an Benutzer

Standardmäßig werden die Netzwerkdrucker auf dem Benutzergerät automatisch zu Beginn jeder Sitzung konfiguriert. Sie können die Anzahl der aufgelisteten und zugeordneten Netzwerkdrucker reduzieren, indem Sie festlegen, welche Netzwerkdrucker in jeder Sitzung erstellt werden sollen. Diese Drucker werden als Sitzungsdrucker bezeichnet.

Sie können die Sitzungsdruckerrichtlinien nach IP-Adressen filtern, um das Proximitydrucken (auf dem nächstgelegenen Drucker) zu gewährleisten. Das Drucken auf dem nächstgelegenen Drucker ermöglicht den Benutzern innerhalb eines angegebenen IP-Adressbereichs den automatischen Zugriff auf Netzwerkdruckgeräte, die im gleichen Bereich liegen. Proximitydrucken wird von der Funktion Citrix Universeller Druckserver umgesetzt; die hier beschriebene Konfiguration ist dazu nicht erforderlich.

Proximitydrucken kann folgende Szenarios umfassen:

- Das interne Unternehmensnetzwerk nutzt einen DHCP-Server, der automatisch IP-Adressen für Benutzer zuweist.
- Alle Abteilungen im Unternehmen haben eindeutige zugeordnete IP-Adressbereiche.
- In den IP-Adressbereichen jeder Abteilung gibt es Netzwerkdrucker.

Wenn Proximitydrucken konfiguriert ist und ein Mitarbeiter einer Abteilung in eine andere wechselt, ist keine zusätzliche Druckgerätekonfiguration erforderlich. Sobald das Benutzergerät im IP-Adressbereich der neuen Abteilung erkannt wird, erhält es Zugriff auf alle Netzwerkdrucker in diesem Bereich.

Konfigurieren bestimmter Drucker für die Umleitung in Sitzungen - zum Erstellen von durch Administratoren zugewiesenen Druckern konfigurieren Sie
die Citrix Richtlinieneinstellung “Sitzungsdrucker”. Verwenden Sie zum Hinzufügen eines Netzwerkdruckers zu dieser Richtlinie eine der folgenden Methoden:

- Geben Sie den UNC-Pfad im Format \\servername\printername ein.
- Navigieren Sie zu einem Drucker im Netzwerk.
- Navigieren Sie zu Druckern auf einem bestimmten Server. Geben Sie den Servernamen im Format \\servername an und klicken Sie auf Durchsuchen.

> **Wichtig:**
>
> Der Server führt alle aktivierten Einstellungen für Sitzungsdrucker für alle angewendeten Richtlinien zusammen, angefangen von der höchsten bis zur niedrigsten Priorität. Ist ein Drucker in mehreren Richtlinienobjekten konfiguriert, werden angepasste Standardeinstellungen nur aus dem Richtlinienobjekt mit der höchsten Priorität verwendet, in dem der Drucker konfiguriert ist.

Welche Netzwerkdrucker über die Einstellung Sitzungsdrucker erstellt werden, kann je nachdem, wo die Sitzung gestartet wurde, durch Filtern, beispielsweise nach Subnetzen, variieren.

Festlegen eines Standardnetzwerkdruckers für eine Sitzung: Standardmäßig wird der Hauptdrucker des Benutzers als Standarddrucker für eine Sitzung verwendet. Verwenden Sie die Citrix Richtlinieneinstellung Standarddrucker, um die Auswahl des Standarddruckers auf dem Benutzergerät in einer Sitzung zu ändern.

1. Wählen Sie unter Standarddrucker eine Einstellung für Standarddrucker des Clients wählen:
    - Netzwerkdruckername: Drucker, die mit der Richtlinieneinstellung Sitzungsdrucker hinzugefügt wurden, werden in diesem Menü angezeigt. Wählen Sie den als Standard für diese Richtlinie zu verwendenden Netzwerkdrucker aus.
    - Standarddrucker des Benutzers nicht anpassen: Verwendet die Einstellung der Terminaldienste oder des aktuellen Benutzerprofils für den Standarddrucker. Weitere Informationen finden Sie in der Onlinehilfe zu Richtlinieneinstellungen.
2. Wenden Sie die Richtlinie auf die Benutzergruppe (oder andere gefilterte Objekte) an, auf die sich auswirken soll.

Konfigurieren von Proximitydrucken: Das Proximitydrucken (Drucken auf dem nächstgelegenen Drucker) wird ebenfalls über den universellen Druckserver von Citrix bereitgestellt. Dieser erfordert nicht die hier beschriebene Konfiguration.

1. Erstellen Sie eine separate Richtlinie für jedes Subnetz (oder entsprechend dem Druckerstandort).
2. Fügen Sie in jeder Richtlinie der Einstellung Sitzungsdrucker die Drucker an dem geografischen Standort des Subnetzes hinzu.
3. Setzen Sie die Einstellung Standarddrucker auf Standarddrucker des Benutzers nicht anpassen.
4. Filtern Sie die Richtlinien nach Client-IP-Adresse. Aktualisieren Sie diese Richtlinien, um Änderungen der DHCP-IP-Adressbereiche zu berücksichtigen.

Pflegen der Druckumgebung

August 18, 2021

Zur Pflege der Druckumgebung gehört Folgendes:

- Verwalten von Druckertreibern
- Optimieren der Druckleistung
- Anzeigen von Druckern und Verwalten von Druckwarteschlangen

Verwalten von Druckertreibern

Citrix empfiehlt die Verwendung des universellen Citrix Druckertreibers, um den Verwaltungsaufwand und mögliche Probleme mit Druckertreibern gering zu halten.

Wenn die automatische Erstellung fehlschlägt, installiert das System standardmäßig einen bei Windows integrierten systemeigenen Druckertreiber. Falls kein Treiber verfügbar ist, greift das System automatisch auf den universellen Druckertreiber zurück. Weitere Informationen über Druckertreiber-Standardwerte finden Sie unter Bewährte Methoden, Sicherheitsüberlegungen und Standardvorgänge.

Wenn der universelle Druckertreiber von Citrix nicht für alle Szenarios geeignet ist, reduzieren Sie die Anzahl installierter Treiber auf Serverbetriebssystemmaschinen mit von Druckertreiberzuordnungen. Außerdem bietet die Zuordnung von Druckertreibern folgende Optionen:

- Beschränken bestimmter Drucker auf die ausschließliche Verwendung des universellen Citrix Druckertreibers
- Zulassen oder Verhindern der Erstellung von Druckern mit einem bestimmten Treiber
- Ersetzen veralteter oder beschädigter Treiber durch gewünschte Druckertreiber
- Ersetzen von Clienttreibernamen durch einen unter Windows Server verfügbaren Treiber

Automatische Installation von Druckertreibern verhindern: Die automatische Installation von Druckertreibern muss deaktiviert sein, damit Konsistenz zwischen Serverbetriebssystemmaschinen gewährleistet ist. Dies kann über Citrix Richtlinien und/oder Microsoft-Richtlinien erreicht werden. Zum Verhindern der automatischen Installation Windows-systemeigener Druckertreiber deaktivieren Sie die Citrix Richtlinieneinstellung Automatische Installation von mitgelieferten Druckertreibern.

Zuordnen von Clientdruckertreibern: Jeder Client liefert bei der Anmeldung Informationen zu den clientseitigen Druckern, einschließlich dem Namen des Druckermodells. Bei der automatischen Erstellung der Clientdrucker werden die Namen der Druckertreiber auf dem Windows-Server ausgewählt, die den Namen der Druckermodelle entsprechen, die der Client bereitgestellt hat. Beim automatischen Erstellen werden mit diesen identifizierten verfügbaren Druckertreibern umgeleitete Clientdruckwarteschlangen erstellt.

Gehen Sie bei der Erstellung von Regeln für die Treiberersetzung und der Bearbeitung der Druckeinstellungen für zugeordnete Clientdruckertreiber grundsätzlich folgendermaßen vor:

1. Legen Sie die Regeln für die Treiberersetzung für automatisch erstellte Drucker fest, indem Sie die Citrix Richtlinieneinstellung Druckertreiberzuordnung und -kompatibilität konfigurieren. Fügen Sie dabei den Namen des Clientdruckertreibers hinzu und wählen Sie über das Menü Druckertreiber suchen den Servertreiber aus, durch den Sie den Clientdruckertreiber ersetzen möchten. Sie können in dieser Einstellung Platzhalter verwenden. Damit beispielsweise alle HP-Drucker einen bestimmten Treiber verwenden, geben Sie in der Richtlinieneinstellung HP* an.

2. Zum Ausschließen eines Druckertreibers wählen Sie den Namen des Treibers aus und aktivieren Sie die Einstellung Nicht erstellen.
3. Sie können bei Bedarf eine Treiberzuordnung bearbeiten, eine Zuordnung löschen oder die Reihenfolge der Treibereinträge in der Liste ändern.
4. Zum Bearbeiten der Druckeinstellungen für zugeordnete Clientdruckertreiber wählen Sie den Druckertreiber aus, klicken Sie auf Einstellungen und geben Sie die Einstellungen wie Druckqualität, Ausrichtung und Farbe an. Wenn Sie eine Druckoption angeben, die der Druckertreiber nicht unterstützt, hat die Option keine Auswirkung. Mit dieser Einstellung werden die gespeicherten Druckereinstellungen überschrieben, die der Benutzer in einer vorherigen Sitzung festgelegt hat.
5. Citrix empfiehlt, das Verhalten der Drucker nach der Zuordnung von Treibern ausführlich zu testen, da einige Druckfunktionen möglicherweise nur über einen bestimmten Treiber zur Verfügung stehen.

Bei der Benutzeranmeldung wird die Clientdruckerkompatibilitätsliste vom System überprüft, bevor die Clientdrucker eingerichtet werden.

Optimieren der Druckleistung

Verwenden Sie den universellen Druckserver und den universellen Druckertreiber, um die Leistung zu optimieren. Die folgenden Richtlinien steuern die Druckoptimierung und Komprimierung:

- Universelles Drucken - Optimierungsstandards. Gibt die Standardeinstellungen für den universellen Drucker an, wenn er für eine Sitzung erstellt wird:
  - Mit Gewünschte Bildqualität geben Sie das standardmäßige Bildkomprimierungslimit an, das auf universelles Drucken angewendet wird. In der Standardeinstellung ist Standardqualität aktiviert, d. h. Benutzer können Bilder nur mit der Standardqualitäts- oder geringeren Qualitätskomprimierung drucken.
  - Mit “Heavyweight-Komprimierung aktivieren”aktivieren oder deaktivieren Sie das Verringern der Bandbreite unter den Komprimierungsgrad, der von Gewünschte Bildqualität festgelegt ist; Bildqualität geht nicht verloren. Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.
  - Mit den Einstellungen Zwischenspeichern von Bildern und Schriftarten legen Sie fest, ob Bilder und Schriftarten, die mehrmals im Druckdatenstrom vorhanden sind, zwischengespeichert werden. Sie stellen damit sicher, dass jedes eindeutige Bild oder jede Schriftart nur einmal zum Drucker gesendet wird. Standardmäßig werden eingebettete Bilder und Schriftarten zwischengespeichert.
  - Mit Nicht-Administratoren können diese Einstellungen ändern legen Sie fest, ob Benutzer die Standardeinstellungen für die Druckoptimierung in einer Sitzung ändern können. Standardmäßig können Benutzer die Standardeinstellungen für die Druckoptimierung nicht

ändern.

- Universelles Drucken - Bildkomprimierungslimit. Definiert die maximale Qualität und die minimale Komprimierung für Bilder, die mit dem universellen Druckertreiber gedruckt werden. Das Limit für Bildkomprimierung ist standardmäßig auf "Beste Qualität"(verlustfreie Komprimierung) gesetzt.
- Universelles Drucken - Druckqualitätslimit. Der Höchstwert für Punkte pro Zoll (dpi) zum Erstellen von Ausdrucken in einer Sitzung. In der Standardeinstellung ist kein Limit angegeben.

Standardmäßig werden alle für Netzwerkdrucker bestimmten Druckaufträge von der Serverbetriebssystemmaschine über das Netzwerk direkt an den Druckserver weitergeleitet. Erwägen Sie, Druckaufträge über die ICA-Verbindung zu leiten, wenn das Netzwerk hohe Latenz oder beschränkte Bandbreite aufweist. Deaktivieren Sie hierzu die Citrix Richtlinieneinstellung Direkte Verbindungen zu Druckservern. Bei einer ICA-Verbindung werden die Daten komprimiert gesendet, es wird somit weniger Bandbreite bei der Übertragung der Daten über das WAN gebraucht.

Verbessern der Sitzungsleistung durch Limitierung der Druckbandbreite: Beim Drucken von Dateien von Serverbetriebssystemmaschinen auf Benutzerdruckern, können bei anderen virtuellen Kanälen (z. B. Video) aufgrund des Wettbewerbs um die Bandbreite Leistungsverringerungen entstehen, insbesondere dann, wenn Benutzer über langsamere Netze auf Server zugreifen. Um dies zu verhindern, können Sie die für das Drucken verwendete Bandbreite beschränken. Indem Sie die Datenübertragungsrate für den Druck einschränken, stellen Sie im HDX-Datenstrom eine größere Bandbreite für die Übertragung von Video, Tastatureingaben und Mausdaten zur Verfügung.

Wichtig: Das Druckerbandbreitenlimit wird immer eingehalten, auch wenn keine anderen Kanäle verwendet werden.

Verwenden Sie die nachfolgenden Einstellungen der Citrix Richtlinie
"Bandbreite", um die Druckerbandbreitenlimits für die Sitzung zu beschränken. Führen Sie diese Aufgabe mit Studio aus, um die Limits für die Site festzulegen. Wenn Sie Limits für einzelne Server festlegen möchten, führen Sie diese Aufgabe über die Gruppenrichtlinien-Verwaltungskonsole in Windows lokal auf jeder Serverbetriebssystemmaschine aus.

- Die Einstellung Bandbreitenlimit für Druckerumleitung dient zur Angabe der zum Drucken verfügbaren Bandbreite in Kilobits pro Sekunde (KBit/s).
- Die Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) begrenzt die zum Drucken verfügbare Bandbreite auf einen Prozentanteil der insgesamt verfügbaren Bandbreite.

  Hinweis: Zur Verwendung der Einstellung
  "Bandbreitenlimit für Druckerumleitung (Prozent)"müssen Sie auch die Einstellung
  "Bandbreitenlimit für Sitzung insgesamt"aktivieren.

  Wenn Sie Werte für beide Einstellungen eingeben, wird die strengste Einstellung (mit dem niedrigeren Wert) angewendet.

Zum Abrufen von Echtzeitinformationen zur Druckbandbreite verwenden Sie Citrix Director.

Lastausgleich bei universellen Druckservern

Die universelle Druckserverlösung kann skaliert werden, indem Sie der Lastausgleichslösung weitere Druckserver hinzufügen. Es gibt keine einzelne Fehlerquelle, da jeder VDA seinen eigenen Load Balancer hat, um die Drucklast auf alle Druckserver zu verteilen.

Verwenden Sie die Richtlinieneinstellungen Universelle Druckserver für den Lastausgleich und Außer-Betrieb-Schwellenwert für universelle Druckserver, um die Drucklast in einer Lastausgleichslösung auf alle Druckserver zu verteilen.

Wenn ein Druckerserver unvorhergesehen ausfällt, werden die Druckerverbindungen des ausgefallenen Druckservers durch den Failovermechanismus des Load Balancers eines VDAs automatisch auf die anderen verfügbaren Druckerserver verteilt, sodass alle vorhandenen und eingehenden Sitzungen normal funktionieren, ohne dass die Benutzererfahrung betroffen oder ein Eingreifen des Administrators nötig ist.

Administratoren können die Aktivitäten der Lastausgleichsdruckserver mit einer Reihe von Leistungsindikatoren überwachen und Folgendes auf dem VDA verfolgen:

- Liste der Lastausgleichsdruckserver auf dem VDA und deren Zustand (verfügbar, nicht verfügbar)
- Anzahl der akzeptierten Druckerverbindungen pro Druckserver
- Anzahl der fehlgeschlagenen Druckerverbindungen pro Druckserver
- Anzahl der aktiven Druckerverbindung pro Druckserver
- Anzahl ausstehender Druckerverbindungen pro Druckserver

Anzeigen und Verwalten der Druckwarteschlangen

In der folgenden Tabelle wird aufgeführt, wo Sie in Ihrer Umgebung Drucker anzeigen und die Druckwarteschlangen verwalten können.

		Druckmodell
Clientdrucker (an das Benutzergerät angeschlossene Drucker)	Clientdruckmodell	UAC aktiviert: Druckverwaltungs-Snap-In in der Microsoft Management Console; UAC deaktiviert: vor Windows 8 –Systemsteuerung, Windows 8 – Druckverwaltungs-Snap-In
Netzwerkdrucker (Drucker auf einem Netzwerkdruckserver)	Netzwerkdruckmodell	UAC aktiviert: Druckserver > Druckverwaltungs-Snap-In in der Microsoft Management Console; UAC deaktiviert: Druckserver > Systemsteuerung
Netzwerkdrucker (Drucker auf einem Netzwerkdruckserver)	Clientdruckmodell	UAC aktiviert: Druckserver > Druckverwaltungs-Snap-In in der Microsoft Management Console; UAC deaktiviert: vor Windows 8 –Systemsteuerung, Windows 8 – Druckverwaltungs-Snap-In
Lokale Netzwerkserverdrucker (Drucker von einem Netzwerkdruckserver, die einer Serverbetriebssystemmaschine hinzugefügt werden)	Netzwerkdruckmodell	UAC aktiviert: Druckserver > Systemsteuerung; UAC deaktiviert: Druckserver > Systemsteuerung

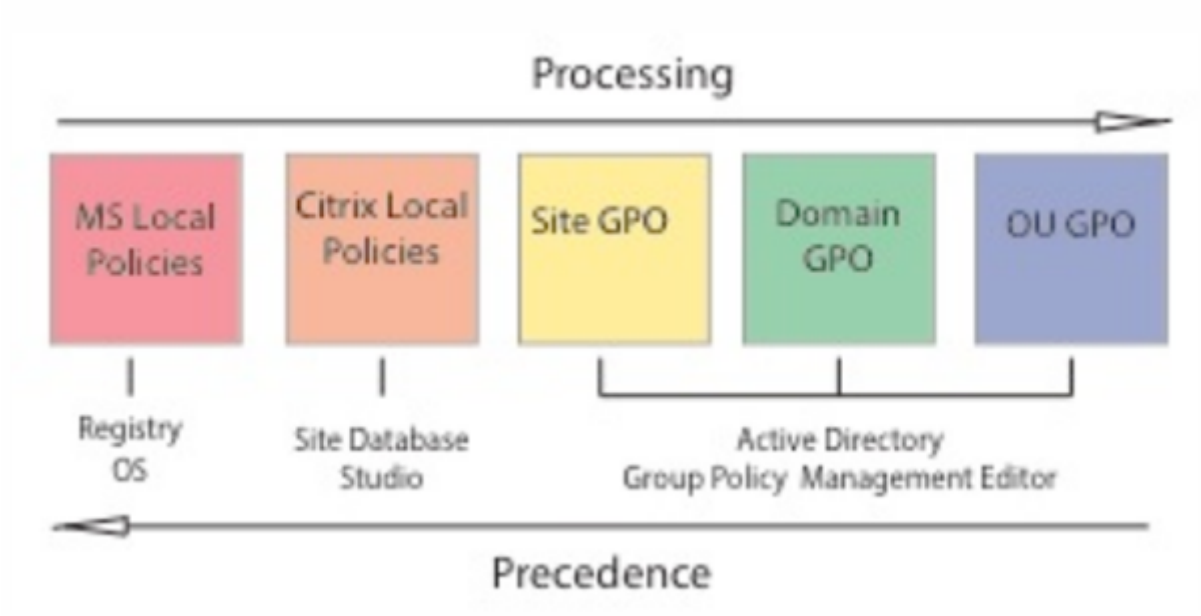
> **Hinweis:**
>
> Druckwarteschlangen für Netzwerkdrucker, die das Netzwerkdruckmodell verwenden, sind privat und können nicht über das System verwaltet werden.

Richtlinien

February 4, 2020

Richtlinien sind eine Sammlung von Einstellungen, die definieren, wie Sitzungen, Bandbreite und Sicherheit für eine Gruppe von Benutzern, Geräten oder Verbindungstypen verwaltet werden.

Richtlinieneinstellungen können auf physische und virtuelle Maschinen oder auf Benutzer angewendet werden. Sie können Einstellungen auf einzelne Benutzer auf lokaler Ebene oder auf Sicherheitsgruppen in Active Directory anwenden. Die Konfigurationen definieren spezifische Kriterien und Regeln. Wenn Sie die Richtlinien nicht ausdrücklich zuweisen, gelten die Einstellungen für alle Verbindungen.



Sie können Richtlinien auf unterschiedliche Ebenen des Netzwerks zuweisen. Richtlinieneinstellungen, die auf der GPO-Ebene der Organisationseinheit zugewiesen werden, haben die höchste Priorität im Netzwerk. Richtlinien auf der Domänen-GPO-Ebene überschreiben Richtlinien auf der Ebene der Sitegruppenrichtlinienobjekte, die wiederum alle lokalen Richtlinien von Microsoft und Citrix überschreiben, die mit ihnen in Konflikt stehen.

Alle lokalen Citrix Richtlinien werden in der Citrix Studio-Konsole erstellt und verwaltet und in der Sitedatenbank gespeichert. Gruppenrichtlinien werden mithilfe der Microsoft-Gruppenrichtlinien-Verwaltungskonsole erstellt und verwaltet und in Active Directory gespeichert. Lokale Microsoft-Richtlinien werden im Windows-Betriebssystem erstellt und in der Registrierung gespeichert.

Studio verwendet einen Modellierungsassistenten, mit dem Administratoren Konfigurationseinstellungen in Vorlagen und Richtlinien vergleichen können, um miteinander in Konflikt stehende und redundante Einstellungen zu eliminieren. Administratoren können Gruppenrichtlinienobjekte mit der Gruppenrichtlinien-Verwaltungskonsole festlegen, um Einstellungen zu konfigurieren und diese Einstellungen auf eine Zielgruppe von Benutzern auf unterschiedlichen Ebenen des Netzwerks anzuwenden.

Diese Gruppenrichtlinienobjekte werden in Active Directory gespeichert und die meisten IT-

Mitarbeiter haben aus Sicherheitsgründen nur eingeschränkten Zugriff auf die Verwaltung dieser Einstellungen.

Einstellungen werden entsprechend ihrer Priorität und Bedingung zusammengefasst. Deaktivierte Einstellungen haben Vorrang vor aktivieren Einstellungen mit niedriger Priorität. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert und setzen keine Einstellungen mit niedrigerer Priorität außer Kraft.

Lokale Richtlinien können auch mit Gruppenrichtlinien in Active Directory in Konflikt stehen. Abhängig von der Situation könnten sie einander überschreiben.

Alle Richtlinien werden in der folgenden Reihenfolge verarbeitet:

1. Der Endbenutzer meldet sich mit Domänenanmeldeinformationen an einer Maschine an.
2. Die Anmeldeinformationen werden an den Domänencontroller gesendet.
3. Active Directory wendet alle Richtlinien an (Endbenutzer, Endpunk, Organisationseinheit und Domäne).
4. Der Endbenutzer meldet sich bei Receiver an und greift auf eine Anwendung oder einen Desktop zu.
5. Richtlinien von Citrix und Microsoft werden für den Endbenutzer und die Maschine, die die Ressource hostet, verarbeitet.
6. Active Directory bestimmt die Priorität für Richtlinieneinstellungen. Es wendet sie dann auf die Registrierung des Endpunktgeräts und die Maschine an, auf der die Ressource gehostet wird.
7. Der Endbenutzer meldet sich von der Ressource ab. Citrix Richtlinien für Endbenutzer und Endpunktgerät sind nicht mehr aktiv.
8. Der Endbenutzer meldet sich vom Benutzergerät ab, das die GPO-Benutzerrichtlinien freigibt.
9. Der Endbenutzer schaltet das Gerät aus und die GPO-Maschinenrichtlinien werden freigegeben.

Beim Erstellen von Richtlinien für Benutzergruppen, Geräte und Maschinen haben einige Mitglieder u. U. unterschiedliche Anforderungen und benötigen Ausnahmen zu einigen Einstellungen. Ausnahmen werden durch Filter in Studio und in der Gruppenrichtlinien-Verwaltungskonsole erstellt und bestimmten, für wen oder was die Richtlinie gilt.

> **Hinweis:**
>
> Das Verwenden von Windows- und Citrix-Richtlinien im gleichen GPO wird nicht unterstützt.

Arbeiten mit Richtlinien

May 14, 2021

Durch das Konfigurieren von Citrix Richtlinien steuern Sie den Benutzerzugriff und die Sitzungsumgebung. Citrix Richtlinien sind die effizienteste Methode zum Steuern der Verbindungs-, Sicherheits- und Bandbreiteneinstellungen. Sie erstellen Richtlinien für bestimmte Benutzergruppen, Geräte oder Verbindungstypen. Jede Richtlinie kann mehrere Einstellungen enthalten.

Tools zum Arbeiten mit Citrix Richtlinien

Sie können die folgenden Tools zum Arbeiten mit Citrix Richtlinien verwenden.

- **Studio**: Wenn Sie ein Citrix Administrator ohne Berechtigung zum Verwalten von Gruppenrichtlinien sind, verwenden Sie Studio, um Richtlinien für Ihre Site zu erstellen. Mit Studio erstellte Richtlinien werden in der Sitedatenbank gespeichert und Updates werden per Push auf den virtuellen Desktop übertragen, wenn der virtuelle Desktop beim Broker registriert wird oder ein Benutzer eine Verbindung mit dem virtuellen Desktop herstellt.
- **Editor für lokale Gruppenrichtlinien** (Snap-In der Microsoft Management Console): Wenn Sie in Ihrer Netzwerkumgebung Active Directory verwenden und Sie die Berechtigungen zur Verwaltung von Gruppenrichtlinien haben, können Sie den Editor für lokale Gruppenrichtlinien verwenden, um Richtlinien für Ihre Site zu erstellen. Die Einstellungen, die Sie konfigurieren, beeinträchtigen die Gruppenrichtlinienobjekte, die Sie in der Gruppenrichtlinien-Verwaltungskonsole angeben.
  Wichtig: Sie müssen den Editor für lokale Gruppenrichtlinien zum Konfigurieren einiger Einstellungen verwenden, u. a. die Einstellungen zum Registrieren von VDAs bei einem Controller und die Einstellungen für Microsoft App-V Server.

Reihenfolge und Priorität bei der Richtlinienverarbeitung

Gruppenrichtlinieneinstellungen (GPOs) werden in der folgenden Reihenfolge verarbeitet:

1. Lokale GPO
2. XenApp- bzw. XenDesktop-Site-GPO (in der Sitedatenbank gespeichert)
3. GPOs auf Siteebene
4. GPOs auf Domänenebene
5. Organisationseinheiten

Bei einem Konflikt können Richtlinieneinstellungen, die zuletzt verarbeitet werden, vorher verarbeitete überschreiben. Das heißt, dass Richtlinieneinstellungen die folgende Rangfolge haben:

1. Organisationseinheiten
2. GPOs auf Domänenebene
3. GPOs auf Siteebene
4. XenApp- bzw. XenDesktop-Site-GPO (in der Sitedatenbank gespeichert)

5. Lokale GPO

Beispiel: Ein Citrix Administrator erstellt eine Richtlinie (Richtlinie A) über Studio, mit der die Clientdateiumleitung für die Vertriebsmitarbeiter des Unternehmens aktiviert wird. Gleichzeitig erstellt ein anderer Administrator mit dem Gruppenrichtlinien-Editor eine Richtlinie (Richtlinie B), mit der die Clientdateiumleitung für die Vertriebsmitarbeiter deaktiviert wird. Wenn sich die Vertriebsmitarbeiter an den virtuellen Desktops anmelden, wird Richtlinie B angewendet und Richtlinie A ignoriert, da Richtlinie B auf der Domänenebene und Richtlinie A auf der Ebene der XenApp- bzw. XenDesktop-Site-GPOs verarbeitet wurde.

Beachten Sie jedoch, dass die Citrix Sitzungseinstellungen die gleichen Einstellungen in einer Active Directory-Richtlinie oder einer Remotedesktop-Sitzungshostkonfiguration überschreiben, wenn ein Benutzer eine ICA- oder Remotedesktopprotokoll (RDP)-Sitzung startet. Zu diesen Einstellungen gehören solche, die mit typischen RDP-Clientverbindungseinstellungen zusammenhängen, wie Desktophintergrund, Menüanimationen und das Anzeigeverhalten bei Drag & Drop.

Wenn Sie mehrere Richtlinien verwenden, können Sie Richtlinien, deren Einstellungen Konflikte verursachen, Prioritäten zuweisen. Weitere Informationen hierzu finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.

Arbeitsablauf bei Citrix Richtlinien

Der Prozess für das Konfigurieren von Richtlinien ist:

1. Erstellen Sie die Richtlinie.
2. Konfigurieren Sie Richtlinieneinstellungen.
3. Weisen Sie die Richtlinie Benutzer- und Maschinenobjekten zu.
4. Weisen Sie der Richtlinie eine Priorität zu.
5. Prüfen Sie die effektive Richtlinie durch Ausführen des Citrix Gruppenrichtlinien-Modellierungsassistenten.

Navigieren durch die Citrix Richtlinien und Einstellungen

Im Editor für lokale Gruppenrichtlinien werden Richtlinien und Einstellungen in zwei Hauptkategorien eingeteilt: Computerkonfiguration und Benutzerkonfiguration. Jede Kategorie hat einen Knoten für Citrix Richtlinien. Weitere Informationen zum Verwenden dieses Snap-Ins finden Sie in der Dokumentation von Microsoft.

In Studio sind die Richtlinieneinstellungen je nach Funktionalität bzw. Feature, für die bzw. das sie gelten, in Kategorien eingeteilt. Beispielsweise enthält der Bereich “Profilverwaltung”Richtlinieneinstellungen für die Profilverwaltung.

- Computereinstellungen (Richtlinieneinstellungen für Maschinen) definieren das Verhalten von virtuellen Desktops und werden beim Start eines virtuellen Desktops angewendet. Diese

Einstellungen werden auch angewendet, wenn keine aktiven Benutzersitzungen auf dem virtuellen Desktop durchgeführt werden. Benutzerrichtlinieneinstellungen definieren die Benutzererfahrung bei Verbindungen über ICA. Benutzerrichtlinien werden angewendet, wenn ein Benutzer eine Verbindung über ICA herstellt oder erneut herstellt. Benutzerrichtlinien werden nicht angewendet, wenn ein Benutzer eine Verbindung über RDP herstellt oder sich direkt bei der Konsole anmeldet.

Sie greifen auf Richtlinien, Einstellungen oder Vorlagen zu, indem Sie im Navigationsbereich von Studio Richtlinien auswählen.

- Die Registerkarte **Richtlinien** listet alle Richtlinien auf. Wenn Sie eine Richtlinie auswählen, wird auf den Registerkarten rechts Folgendes angezeigt: Übersicht (Name, Priorität, Status: Aktiviert bzw. Deaktiviert, und Beschreibung), Einstellungen (Liste der konfigurierten Einstellungen) und Zugewiesen zu (Benutzer- und Maschinenobjekte, denen die Richtlinie momentan zugewiesen ist). Weitere Informationen finden Sie unter Erstellen von Richtlinien.
- Auf der Registerkarte **Vorlagen** werden von Citrix bereitgestellte und benutzerdefinierte Vorlagen, die Sie erstellt haben, aufgelistet. Wenn Sie eine Vorlage auswählen, wird auf den Registerkarten rechts Folgendes angezeigt: Beschreibung (Zweck der Vorlage) und Einstellungen (Liste der konfigurierten Einstellungen). Weitere Informationen finden Sie unter Richtlinienvorlagen.
- Mit der Registerkarte **Vergleich** können Sie die Einstellungen einer Richtlinie oder Vorlage mit denen in anderen Richtlinien oder Vorlagen vergleichen. Sie können beispielsweise Einstellungswerte prüfen, um sicherzustellen, dass optimale Verfahren eingehalten werden. Weitere Informationen finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.
- Auf der Registerkarte **Modellierung** können Sie Verbindungsszenarios mit Citrix Richtlinien simulieren. Weitere Informationen finden Sie unter Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien.

Suchen nach einer Einstellung in einer Richtlinie oder Vorlage

1. Wählen Sie die Richtlinie oder Vorlage aus.
2. Wählen Sie im Aktionsbereich Richtlinie bearbeiten oder Vorlage bearbeiten.
3. Geben Sie auf der Seite Einstellungen den Namen der Einstellung ein.

Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie (z. B. Bandbreite) auswählen oder indem Sie das Kontrollkästchen Nur ausgewählte anzeigen aktivieren. Außerdem können Sie nur die Einstellungen suchen, die der ausgewählten Richtlinie hinzugefügt wurden. Für eine ungefilterte Suche wählen Sie Alle Einstellungen.

- Suchen nach einer Einstellung in einer Richtlinie

  1. Markieren Sie die Richtlinie.

2. Geben Sie auf der Registerkarte Einstellungen den Namen der Einstellung ein.

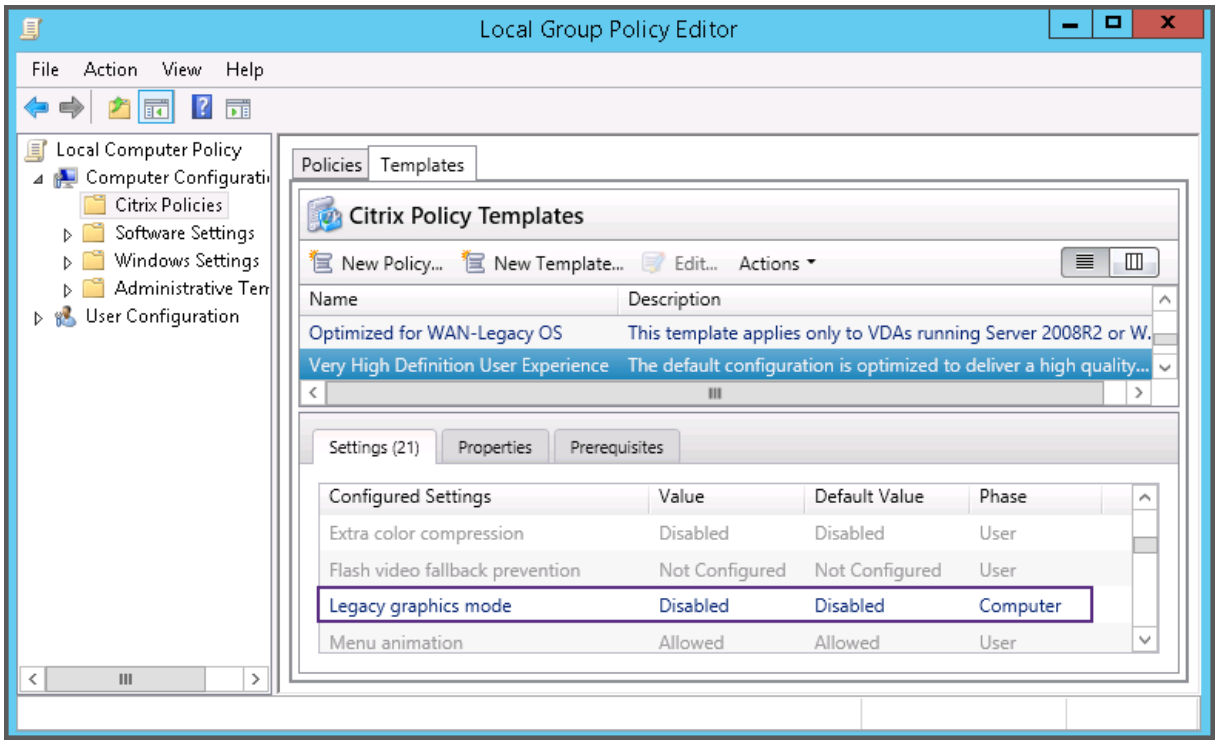
Sie können die Suche verfeinern, indem Sie eine bestimmte Produktversion oder Kategorie auswählen. Für eine ungefilterte Suche wählen Sie Alle Einstellungen.

Eine Richtlinie ist nach ihrer Erstellung völlig unabhängig von der verwendeten Vorlage. Sie können in das Feld “Beschreibung”eingeben, auf welcher Vorlage die neue Richtlinie basiert.

In Studio werden Richtlinien und Vorlagen in einer Liste angezeigt, unabhängig davon, ob sie Benutzer- oder Computereinstellungen oder beide Arten von Einstellungen enthalten, und sie können zudem mit Benutzer- und Computerfiltern angewendet werden.

Im Gruppenrichtlinien-Editor müssen Computer- und Benutzereinstellungen separat angewendet werden, selbst wenn sie auf einer Vorlage basieren, die beide Arten von Einstellungen enthält. In diesem Beispiel wird “Besonders gute High Definition-Benutzererfahrung”in Computerkonfiguration verwendet:

- Der Legacy-Grafikmodus ist eine Computereinstellung, die in einer mit dieser Vorlage erstellten Richtlinie verwendet wird.
- Die Benutzereinstellungen, grau dargestellt, werden nicht in einer mit dieser Vorlage erstellten Richtlinie verwendet.



Richtlinienvorlagen

August 18, 2021

Vorlagen ermöglichen das Erstellen von Richtlinien von einem vordefinierten Ausgangspunkt aus. Integrierte Citrix Vorlagen sind für bestimmte Umgebungen oder Netzwerkbedingungen optimiert und können für Folgendes verwendet werden:

- Als Ausgangspunkt für das Erstellen Ihrer eigenen Richtlinien und Vorlagen, die Sie für verschiedene Sites freigeben können.
- Eine Referenz für einfacheres Vergleichen der Ergebnisse zwischen Bereitstellungen, da Sie sich auf Ergebnisse beziehen können, zum Beispiel "…wenn Sie die Citrix Vorlage x oder y verwenden …".
- Eine Methode für das Übermitteln von Richtlinien an Citrix Support oder vertrauenswürdige Dritte durch Importieren oder Exportieren von Vorlagen.

Richtlinienvorlagen können importiert und exportiert werden. Weitere Vorlagen und/oder Updates für die integrierten Vorlagen finden Sie unter CTX202000.

Informationen zur Verwendung von Vorlagen für die Erstellung von Richtlinien finden Sie unter CTX202330.

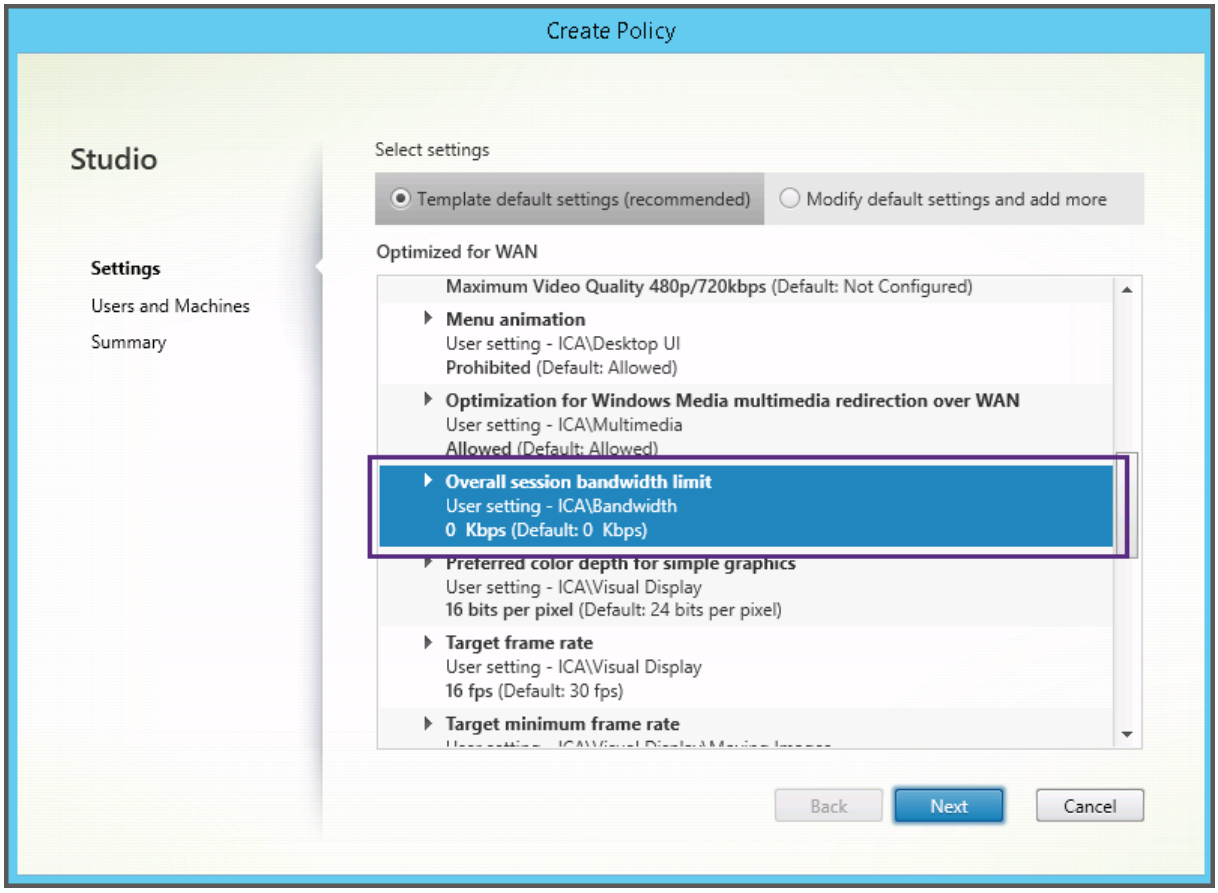
Integrierte Citrix Vorlagen

Die folgenden Richtlinienvorlagen sind verfügbar:

- **Besonders gute High Definition-Benutzererfahrung**: Diese Vorlage erzwingt Standardeinstellungen, die die Benutzererfahrung optimieren. Verwenden Sie diese Vorlage in Szenarios, in denen mehrere Richtlinien in der Reihenfolge der Priorität verarbeitet werden.
- **Hohe Serverskalierbarkeit**: Mit dieser Vorlage können Sie Serverressourcen sparen, da Benutzererfahrung und Serverskalierbarkeit ausbalanciert werden. Die Vorlage ermöglicht eine gute Benutzererfahrung und erhöht gleichzeitig die Anzahl an Benutzern, die auf einem einzelnen Server gehostet werden können. Diese Vorlage verwendet keinen Videocodec für die Komprimierung von Grafiken und verhindert das serverseitige Multimediarendering.
- **Hohe Serverskalierbarkeit –Legacy-OS**: Diese Vorlage für hohe Serverskalierbarkeit gilt nur für VDAs, die unter Windows Server 2008 R2, Windows 7 und älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Für NetScaler SD-WAN optimiert**: Verwenden Sie diese Vorlage für Benutzer, die in Geschäftsstellen arbeiten, in denen die Bereitstellung von XenDesktop durch NetScaler SD-WAN optimiert wird. (NetScaler SD-WAN ist der neue Name für CloudBridge.)

- **Für WAN optimiert**: Verwenden Sie diese Vorlage bei aufgabenorientierten Mitarbeitern, die in Geschäftsstellen über eine gemeinsam genutzte WAN-Verbindung arbeiten oder bei Remotestandorten, wo über Verbindungen mit geringer Bandbreite auf Anwendungen mit grafisch einfachen Benutzeroberflächen und wenig Multimediainhalt zugegriffen wird. Mit dieser Vorlage werden für optimierte Bandbreiteneffizienz Kompromisse bei der Qualität der Videowiedergabe und der Serverskalierbarkeit gemacht.
- **Für WAN optimiert –Legacy-OS**: Die Vorlage Für WAN optimiert gilt nur für VDAs, die auf Server 2008 R2, Windows 7 oder älteren Betriebssystemen ausgeführt werden. Die Vorlage stützt sich auf den Legacy-Grafikmodus, der für diese Betriebssysteme effizienter ist.
- **Sicherheit und Steuerung**: Verwenden Sie diese Vorlage in Umgebungen mit niedriger Fehlertoleranz, um die in XenApp und XenDesktop standardmäßig aktivierten Features zu minimieren. Die in dieser Vorlage enthaltenen Einstellungen deaktivieren den Zugriff auf Drucker, Zwischenablage, Peripheriegeräte, Laufwerkzuordnung, Portumleitung und Flash-Beschleunigung auf Benutzergeräten. Bei Anwendung dieser Vorlage wird möglicherweise mehr Bandbreite genutzt und die Benutzerdichte pro Server verringert.

Wir empfehlen zwar, die integrierten Citrix Vorlagen mit den Standardeinstellungen zu verwenden, jedoch haben einige Einstellungen keine empfohlenen Werte (z. B. die Einstellung "Bandbreitenlimit für Sitzung insgesamt"in der Vorlage "Für WAN optimiert"). In diesem Fall wird die Einstellung durch die Vorlage verfügbar gemacht, damit der Administrator die Wirkung dieser Einstellung in diesem Szenario versteht.



Wenn Sie eine Bereitstellung (Richtlinienverwaltung und VDAs) vor XenApp und XenDesktop 7.6 FP3 betreiben und die Vorlagen "Hohe Serverskalierbarkeit"und "Für WAN optimiert"benötigen, verwenden Sie die Vorlagenversionen für ältere Betriebssysteme ("Legacy-OS").

> **Hinweis:**
>
> Integrierte Vorlagen werden von Citrix erstellt und aktualisiert. Diese Vorlagen dürfen nicht geändert oder gelöscht werden.

Erstellen und Verwalten von Vorlagen mit Studio

Erstellen einer neuen Vorlage basierend auf einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann die Vorlage, mit der Sie eine neue Vorlage erstellen möchten.
3. Wählen Sie im Aktionsbereich **Vorlage erstellen**.
4. Wählen und konfigurieren Sie die Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten. Entfernen Sie vorhandene Einstellungen, die nicht eingeschlossen werden sollen. Geben Sie einen Namen für die Vorlage ein.

Nachdem Sie auf **Fertig stellen** geklickt haben, wird die neue Vorlage auf der Registerkarte **Vorlagen** angezeigt.

Erstellen einer neuen Vorlage basierend auf einer Richtlinie

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Richtlinien** und dann die Richtlinie, mit der Sie die neue Vorlage erstellen möchten.
3. Wählen Sie im Aktionsbereich **Als Vorlage speichern**.
4. Wählen und konfigurieren Sie die neuen Richtlinieneinstellungen, die Sie in die Vorlage einschließen möchten. Entfernen Sie vorhandene Einstellungen, die nicht eingeschlossen werden sollen. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein und klicken Sie auf **Fertig stellen**.

Importieren einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann **Vorlage importieren**.
3. Wählen Sie die Vorlagendatei, die Sie importieren möchten, und klicken Sie auf **Öffnen**. Wenn Sie eine Vorlage importieren, die denselben Namen wie eine vorhandene hat, können Sie die vorhandene Vorlage überschreiben oder die Vorlage unter einem anderen Namen speichern, der automatisch generiert wird.

Exportieren einer Vorlage

1. Wählen Sie im Studio-Navigationsbereich **Richtlinien** aus.
2. Wählen Sie die Registerkarte **Vorlagen** und dann **Vorlage exportieren**.
3. Legen Sie den Speicherort für die Vorlage fest, und klicken Sie auf **Speichern**.

Im angegebenen Speicherort wird eine GPT-Datei erstellt.

Erstellen und Verwalten von Vorlagen mit dem Gruppenrichtlinien-Editor

Navigieren Sie im Gruppenrichtlinien-Editor zu
“Computerkonfiguration”oder
“Benutzerkonfiguration”. Erweitern Sie den Knoten
“Richtlinien”und wählen Sie dann
“Citrix Richtlinien”. Wählen Sie die entsprechende Aktion aus.

Aufgabe	Anweisung
Erstellen einer Vorlage basierend auf einer vorhandenen Richtlinie	Wählen Sie auf der Registerkarte Richtlinien die Richtlinie aus und wählen Sie dann Aktionen > Als Vorlage speichern.
Erstellen einer Richtlinie basierend auf einer vorhandenen Vorlage	Wählen Sie auf der Registerkarte Vorlagen die entsprechende Vorlage aus und klicken Sie dann auf Neue Richtlinie.
Erstellen einer Vorlage basierend auf einer vorhandenen Vorlage	Wählen Sie auf der Registerkarte Vorlagen die entsprechende Vorlage aus und klicken Sie dann auf Neue Vorlage.
Importieren einer Vorlage	Wählen Sie auf der Registerkarte Vorlagen die Option Aktionen > Importieren.
Exportieren einer Vorlage	Wählen Sie auf der Registerkarte Vorlagen die Option Aktionen > Exportieren.
Anzeigen der Vorlageneinstellungen	Wählen Sie auf der Registerkarte Vorlagen die Vorlage aus und klicken Sie auf die Registerkarte Einstellungen.
Anzeigen einer Zusammenfassung von Vorlageneigenschaften	Wählen Sie auf der Registerkarte Vorlagen die Vorlage aus und klicken Sie auf die Registerkarte Eigenschaften.
Anzeigen von Vorlagenvoraussetzungen	Wählen Sie auf der Registerkarte Vorlagen die Vorlage aus und klicken Sie auf die Registerkarte Voraussetzungen.

Vorlagen und delegierte Administration

Richtlinienvorlagen werden auf der Maschine gespeichert, auf der das Richtlinienverwaltungspaket installiert wurde. Das ist entweder die Maschine mit dem Delivery Controller oder die Maschine für die Verwaltung der Gruppenrichtlinienobjekte, jedoch nicht die Maschine mit der XenApp- und XenDesktop-Sitedatenbank. Daher werden die Richtlinienvorlagen nicht über die Rollen und Geltungsbereiche der delegierten Site-Verwaltung, sondern über Windows-Administratorrechte gesteuert.

Dies bedeutet, dass ein Administrator, der über Leseberechtigungen für die Site verfügt, beispielsweise neue Vorlagen erstellen kann. Da Vorlagen jedoch lokale Dateien sind, werden an der Umgebung keine Änderungen vorgenommen.

Benutzerdefinierte Vorlagen sind für das Benutzerkonto sichtbar, das sie erstellt hat, und werden im Windows-Profil des Benutzers gespeichert. Wenn Sie eine benutzerdefinierte Vorlage umfassender

verfügbar machen möchten, erstellen Sie daraus eine Richtlinie oder exportieren Sie die Vorlage in einen freigegebenen Speicherort.

Erstellen von Richtlinien

August 18, 2021

Legen Sie vor dem Erstellen einer Richtlinie fest, für welche Benutzergruppen oder Geräte sie gelten soll. Sie können Richtlinien basierend auf Aufgabenbereich, Verbindungstyp, Benutzergerät oder geografischer Position erstellen. Alternativ können Sie die gleichen Kriterien verwenden wie für Windows Active Directory-Gruppenrichtlinien.

Wenn Sie bereits eine Richtlinie für eine Gruppe erstellt haben, sollten Sie möglichst die Richtlinie bearbeiten und die entsprechenden Einstellungen konfigurieren, statt eine andere Richtlinie zu erstellen. Vermeiden Sie es, eine neue Richtlinie zu erstellen, deren einziger Zweck ist, eine bestimmte Einstellung zu aktivieren oder bestimmte Benutzer von der Richtlinie auszunehmen.

Wenn Sie eine Richtlinie erstellen, verwenden Sie als Basis eine Richtlinienvorlage und passen Sie die Einstellungen nach Bedarf an. Sie können die Richtlinie natürlich auch ohne Vorlage erstellen und alle benötigten Einstellungen hinzufügen.

In Citrix Studio werden neu erstellte Richtlinien auf "Deaktiviert"festgelegt, sofern das Kontrollkästchen "Aktiviert"nicht explizit aktiviert wird.

Richtlinieneinstellungen

Richtlinieneinstellungen können deaktiviert, aktiviert oder nicht konfiguriert sein. Standardmäßig sind Richtlinieneinstellungen nicht konfiguriert, d. h. sie wurden keiner Richtlinie hinzugefügt. Einstellungen werden nur angewendet, wenn sie einer Richtlinie hinzugefügt wurden.

Manche Richtlinieneinstellungen können einen der folgenden Zustände haben:

- Mit Zugelassen oder Nicht zugelassen wird die durch die Einstellung gesteuerte Aktion ermöglicht oder verhindert. In manchen Fällen dürfen Benutzer die Aktion der Einstellung in der Sitzung verwalten, in anderen dürfen sie das nicht. Wenn beispielsweise für Menüanimation die Einstellung auf "Zugelassen"festgelegt ist, können Benutzer Menüanimationen in ihrer Clientumgebung steuern.
- Mit Aktiviert oder Deaktiviert schalten Sie die Einstellung ein oder aus. Wenn Sie eine Einstellung deaktivieren, wird sie nicht durch Richtlinien mit geringerer Priorität aktiviert.

Manche Einstellungen steuern außerdem die Wirksamkeit von abhängigen Einstellungen. Die Einstellung Clientlaufwerkumleitung steuert beispielsweise, ob Benutzer auf die Laufwerke ihres Geräts zugreifen können. Damit Benutzer auf Netzlaufwerke zugreifen können, muss sowohl diese Einstellung als auch die Einstellung Clientnetzlaufwerke der Richtlinie hinzugefügt werden. Wenn die Einstellung Clientlaufwerkumleitung deaktiviert ist, können Benutzer nicht auf ihre Netzlaufwerke zugreifen, selbst wenn die Einstellung Clientnetzlaufwerke aktiviert ist.

In der Regel treten Änderungen an Richtlinieneinstellungen, die sich auf Maschinen auswirken, in Kraft, wenn der virtuelle Desktop neu gestartet wird oder wenn sich ein Benutzer anmeldet. Änderungen an Richtlinieneinstellungen, die Auswirkungen auf Benutzer haben, treten in Kraft, wenn sich die Benutzer das nächste Mal anmelden. Wenn Sie Active Directory verwenden, werden die Richtlinieneinstellungen aktualisiert, wenn Active Directory die Richtlinien in 90-Minuten-Intervallen erneut evaluiert. Die Richtlinieneinstellungen werden angewendet, wenn der virtuelle Desktop neu gestartet wird oder wenn sich ein Benutzer anmeldet.

Für manche Richtlinieneinstellungen können Sie einen Wert eingeben oder auswählen, wenn Sie die Einstellung der Richtlinie hinzufügen. Sie können die Konfiguration der Einstellung einschränken, indem Sie Standardwert verwenden wählen. Dadurch deaktivieren Sie die Konfiguration der Einstellung und nur der Standardwert der Einstellung darf verwendet werden, wenn die Richtlinie angewendet wird, unabhängig von dem Wert, der vor dem Aktivieren von Standardwert verwenden eingegeben wurde.

Bewährte Methoden:

- Weisen Sie Richtlinien Gruppen statt einzelnen Benutzern zu. Wenn Sie Richtlinien Gruppen zuweisen, werden Zuweisungen automatisch aktualisiert, wenn Sie Benutzer Gruppen hinzufügen oder sie daraus entfernen.
- Aktivieren Sie nicht widersprechende oder überlappende Einstellungen in der Konfiguration des Remotedesktop-Sitzungshosts. In manchen Fällen bietet die Remotedesktop-Sitzungshostkonfiguration ähnliche Funktionalität wie Citrix Richtlinieneinstellungen. Wählen Sie nach Möglichkeit für alle Einstellungen den gleichen Status (aktiviert oder deaktiviert), um die Problembehandlung zu erleichtern.
- Deaktivieren Sie Richtlinien, die nicht verwendet werden. Richtlinien, denen keine Einstellungen hinzugefügt wurden, verursachen unnötigen Verarbeitungsaufwand.

Richtlinienzuweisungen

Wenn Sie eine Richtlinie erstellen und bestimmten Benutzer- und Maschinenobjekten zuweisen, wird sie gemäß bestimmter Kriterien oder Regeln auf Verbindungen angewendet. Basierend auf einer Kombination von Kriterien können Sie in der Regel beliebig viele Zuweisungen für eine Richtlinie hinzufügen. Wenn keine Zuweisung angegeben wurde, gilt die Richtlinie für alle Verbindungen.

In der folgenden Tabelle werden verfügbare Zuweisungen aufgelistet:

Name	Anwendung der Richtlinie basierend auf
Zugriffssteuerung	Zugriffssteuerungsbedingungen, unter denen Clients eine Verbindung herstellen Verbindungstyp: ob die Richtlinie auf Verbindungen anzuwenden ist, die mit oder ohne NetScaler Gateway hergestellt wurden. NetScaler Gateway-Farmname: Name des virtuellen NetScaler Gateway-Servers. Zugriffsbedingung: Name der zu verwendenden Endpunktanalyserichtlinie oder Sitzungsrichtlinie.
Citrix CloudBridge	Ob eine Benutzersitzung über Citrix CloudBridge gestartet wird. **Hinweis:** Sie können einer Richtlinie nur eine Citrix CloudBridge-Zuweisung hinzufügen.
Client-IP-Adresse	IP-Adresse des Benutzergeräts, das zum Verbinden der Sitzung verwendet wird IPv4-Beispiele: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6-Beispiele: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Clientname	Name des Benutzergeräts Genaue Übereinstimmung: ClientABCName. Verwenden von Platzhalter: Client*Name
Bereitstellungsgruppe	Bereitstellungsgruppen-Mitgliedschaft
Bereitstellungsgruppentyp	Desktop- oder Anwendungstyp: privater Desktop, freigegebener Desktop, private Anwendung oder freigegebene Anwendung
Organisationseinheit	Organisationseinheit
Tag	Tags **Hinweis:** Installieren Sie den unter CTX142439 verfügbaren Hotfix, um sicherzustellen, dass die Richtlinien bei der Verwendung von Tags richtig angewendet werden.
Benutzer oder Gruppe	Benutzer- oder Gruppenname

Alle Richtlinien, die mit den Zuweisungen für die Verbindung übereinstimmen, werden bei der

Anmeldung eines Benutzers identifiziert. Die Richtlinien werden nach Priorität sortiert und mehrere Instanzen jeder Einstellung werden verglichen. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet. Jede deaktivierte Richtlinieneinstellung hat Vorrang vor einer aktivierten Richtlinieneinstellung, deren Priorität niedriger ist. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert.

Wichtig: Bei der Konfiguration von Active Directory- und Citrix Richtlinien mit der Gruppenrichtlinien-Verwaltungskonsole werden Zuweisungen und Einstellungen möglicherweise nicht wie erwartet angewendet. Weitere Informationen finden Sie unter CTX127461.

Eine Richtlinie mit dem Namen "Ungefiltert"ist standardmäßig verfügbar.

- Wenn Sie Studio zur Verwaltung von Citrix Richtlinien verwenden, werden die Einstellungen, die Sie der Richtlinie "Ungefiltert"hinzufügen, auf alle Server, Desktops und Verbindungen einer Site angewendet.
- Wenn Sie mit dem Editor für lokale Gruppenrichtlinien Citrix Richtlinien verwalten, gelten Einstellungen, die Sie der Richtlinie "Ungefiltert"hinzufügen, für alle Sites und Verbindungen, die zu dem Geltungsbereich des Gruppenrichtlinienobjekts gehören, das die Richtlinie enthält. Beispiel: Die Organisationseinheit (OU) "Verkauf"enthält ein Gruppenrichtlinienobjekt "Verkauf-USA", das alle Mitarbeiter des US-Verkaufsteams einschließt. Das Gruppenrichtlinienobjekt "Verkauf-USA"ist mit einer Richtlinie "Ungefiltert"konfiguriert, die mehrere Benutzerrichtlinieneinstellungen enthält. Wenn der US-Verkaufsleiter sich an der Site anmeldet, werden die Einstellungen der Richtlinie "Ungefiltert"automatisch auf die Sitzung angewendet, weil der Benutzer Mitglied des Gruppenrichtlinienobjekts "Verkauf-USA"ist.

Der Modus einer Zuweisung entscheidet, ob die Richtlinie nur auf Verbindungen angewendet wird, die alle Zuweisungskriterien erfüllen. Wenn der Modus
"Zulassen"(Standardwert) ist, wird die Richtlinie nur auf Verbindungen angewendet, die die Zuweisungskriterien erfüllen. Wenn der Modus
"Verweigern"ist, wird die Richtlinie angewendet, wenn eine Verbindung die Zuweisungskriterien nicht erfüllt. Das folgende Beispiel zeigt, wie Zuweisungsmodi sich auf Citrix Richtlinien auswirken, wenn mehrere Zuweisungen vorhanden sind.

- **Beispiel: Zuweisungen des gleichen Typs mit unterschiedlichen Modi:** In Richtlinien mit zwei Zuweisungen des gleichen Typs, eine mit der Einstellung "Zulassen"und die andere mit der Einstellung "Verweigern", hat die Zuweisung mit der Einstellung "Verweigern"Vorrang, wenn die Verbindung die Kriterien beider Zuweisungen erfüllt. Beispiel:

  Richtlinie 1 enthält die folgenden Zuweisungen:

  - Zuweisung A bestimmt die Verkaufsgruppe und der Modus ist Zulassen
  - Zuweisung B bestimmt das Konto des Verkaufsleiters und der Modus ist Verweigern

Da der Modus für Zuweisung B Verweigern ist, wird die Richtlinie nicht angewendet, wenn der Verkaufsleiter sich bei der Site anmeldet, obwohl er Mitglied der Verkaufsgruppe ist.

- **Beispiel: Zuweisungen unterschiedlichen Typs mit gleichen Modi:** In Richtlinien mit zwei oder mehr Zuweisungen unterschiedlichen Typs, für die "Zulassen"eingestellt ist, muss die Verbindung die Kriterien von mindestens einer Zuweisung jedes Typs erfüllen, damit die Richtlinie angewendet wird. Beispiel:

  Richtlinie 2 enthält die folgenden Zuweisungen:

  - Zuweisung C ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt, und der Modus ist Zulassen
  - Zuweisung D ist eine Client-IP-Adressenzuweisung, die 10.8.169.* festlegt (das Unternehmensnetzwerk), und der Modus ist Zulassen.

  Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie angewendet, weil die Verbindung die Kriterien beider Zuweisungen erfüllt.

  Richtlinie 3 enthält die folgenden Zuweisungen:

  - Zuweisung E ist eine Benutzerzuweisung, die die Verkaufsgruppe angibt, und der Modus ist Zulassen
  - Zuweisung F ist eine Zugriffssteuerungszuweisung, die NetScaler Gateway-Verbindungsbedingungen angibt, und der Modus ist Zulassen.

  Wenn der Verkaufsleiter sich im Büro bei der Site anmeldet, wird die Richtlinie nicht angewendet, weil die Verbindung nicht die Kriterien von Zuweisung F erfüllt.

Erstellen einer Richtlinie basierend auf einer Vorlage mit Studio

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Wählen Sie die Registerkarte "Vorlagen"und wählen Sie dann eine Vorlage.
3. Wählen Sie im Aktionsbereich Richtlinie aus Vorlage erstellen.
4. Standardmäßig verwendet die neue Richtlinie alle Standardeinstellungen der Vorlage (das Optionsfeld Standardeinstellungen der Vorlage ist ausgewählt). Um die Einstellungen zu ändern, wählen Sie das Optionsfeld Standardeinstellungen ändern und Einstellungen hinzufügen, und fügen Sie Einstellungen hinzu oder entfernen Sie sie.
5. Legen Sie fest, wie die Richtlinie angewendet werden soll, indem Sie eine der folgenden Optionen auswählen:

   - Ausgewählten Benutzer- und Maschinenobjekten zuweisen und wählen Sie dann die Benutzer- und Maschinenobjekte, auf die Sie die Richtlinie anwenden möchten.

- Allen Objekten in der Site zuweisen, damit die Richtlinie auf alle Benutzer- und Maschinenobjekte in der Site angewendet wird.

6. Geben Sie einen Namen für die Richtlinie ein (oder akzeptieren Sie den Standardwert). Empfehlenswert sind Richtliniennamen, die beschreiben, wer von der Richtlinie betroffen ist, z. B. Buchhaltung oder Remotebenutzer. Geben Sie optional eine Beschreibung ein.

   Die Richtlinie ist standardmäßig aktiviert. Sie können sie deaktivieren. Wenn die Richtlinie aktiviert ist, kann sie sofort auf Benutzer, die sich anmelden, angewendet werden. Deaktivieren der Richtlinie verhindert, dass sie angewendet wird. Wenn Sie die Priorität der Richtlinie ändern müssen oder später weitere Einstellungen hinzufügen möchten, können Sie die Richtlinie deaktivieren, bis Sie damit fertig sind, und die Richtlinie dann anwenden.

Erstellen einer Richtlinie mit Studio

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Wählen Sie die Registerkarte Richtlinien.
3. Wählen Sie im Aktionsbereich Richtlinie erstellen.
4. Fügen Sie Richtlinieneinstellungen nach Bedarf hinzu und konfigurieren Sie diese.
5. Legen Sie fest, wie die Richtlinie angewendet werden soll, indem Sie eine der folgenden Optionen auswählen:

   - Ausgewählten Benutzer- und Maschinenobjekten zuweisen und wählen Sie dann die Benutzer- und Maschinenobjekte, auf die Sie die Richtlinie anwenden möchten.
   - Allen Objekten in der Site zuweisen, damit die Richtlinie auf alle Benutzer- und Maschinenobjekte in der Site angewendet wird.

6. Geben Sie einen Namen für die Richtlinie ein (oder akzeptieren Sie den Standardwert). Empfehlenswert sind Richtliniennamen, die beschreiben, wer von der Richtlinie betroffen ist, z. B. Buchhaltung oder Remotebenutzer. Geben Sie optional eine Beschreibung ein.

   Die Richtlinie ist standardmäßig aktiviert. Sie können sie deaktivieren. Wenn die Richtlinie aktiviert ist, kann sie sofort auf Benutzer, die sich anmelden, angewendet werden. Deaktivieren der Richtlinie verhindert, dass sie angewendet wird. Wenn Sie die Priorität der Richtlinie ändern müssen oder später weitere Einstellungen hinzufügen möchten, können Sie die Richtlinie deaktivieren, bis Sie damit fertig sind, und die Richtlinie dann anwenden.

Erstellen und Verwalten von Richtlinien mit dem Gruppenrichtlinien-Editor

Navigieren Sie im Gruppenrichtlinien-Editor zu
“Computerkonfiguration”oder

“Benutzerkonfiguration”. Erweitern Sie den Knoten
“Richtlinien”und wählen Sie dann
“Citrix Richtlinien”. Wählen Sie die entsprechende Aktion aus.

Aufgabe	Anweisung
Erstellen einer Richtlinie	Klicken Sie auf der Registerkarte Richtlinien auf Neu.
Bearbeiten einer bestehenden Richtlinie	Wählen Sie auf der Registerkarte Richtlinien die entsprechende Richtlinie aus und klicken Sie dann auf Bearbeiten.
Ändern der Priorität einer bestehenden Richtlinie	Wählen Sie auf der Registerkarte Richtlinien die entsprechende Richtlinie aus und klicken Sie dann auf Höhere Priorität oder Geringere Priorität.
Anzeigen einer Zusammenfassung über eine Richtlinie	Wählen Sie auf der Registerkarte Richtlinien die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Zusammenfassung.
Anzeigen und Ändern der Richtlinieneinstellungen	Wählen Sie auf der Registerkarte Richtlinien die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Einstellungen.
Anzeigen und Ändern der Richtlinienfilter	Wählen Sie auf der Registerkarte Richtlinien die entsprechende Richtlinie aus und klicken Sie dann auf die Registerkarte Filter.
Aktivieren oder Deaktivieren einer Richtlinie	Wählen Sie auf der Registerkarte Richtlinien die entsprechende Richtlinie aus und klicken Sie dann auf Aktionen > Aktivieren oder Aktionen > Deaktivieren.
Erstellen einer Richtlinie basierend auf einer vorhandenen Vorlage	Wählen Sie auf der Registerkarte Vorlagen die entsprechende Vorlage aus und klicken Sie dann auf Neue Richtlinie.

Vergleichen, Priorisieren, Modellieren und Problembehandlung für Richtlinien

August 18, 2021

Sie können mit mehreren Richtlinien Ihre Umgebung an die Anforderungen der Benutzer, basierend auf deren Aufgabengebiet, geografischem Standort oder Verbindungstyp anpassen. Beispielsweise sind Sie vielleicht aus Sicherheitsgründen gezwungen, Benutzergruppen, die regelmäßig mit sensiblen Daten arbeiten, Beschränkungen aufzuerlegen. Sie können eine Richtlinie erstellen, die Benutzer daran hindert, vertrauliche Daten auf ihren lokalen Clientlaufwerken zu speichern. Wenn jedoch manche Mitglieder dieser Benutzergruppe Zugang zu ihren lokalen Laufwerken benötigen, können Sie eine andere Richtlinie für diese Benutzer erstellen. Anschließend können Sie den beiden Richtlinien jeweils eine Priorität zuweisen und damit festlegen, welche Richtlinie Vorrang haben soll.

Wenn Sie mehrere Richtlinien verwenden, müssen Sie festlegen, wie Prioritäten zugewiesen und Ausnahmen erstellt werden und wie die wirksame Richtlinie bei Richtlinienkonflikten angezeigt wird.

In der Regel setzen Richtlinien ähnliche Einstellungen, die für die gesamte Site, für bestimmte Delivery Controller oder auf dem Benutzergerät konfiguriert wurden, außer Kraft. Die Ausnahme von diesem Prinzip sind Sicherheitseinstellungen. Die höchste Verschlüsselungseinstellung in der Umgebung, einschließlich Betriebssystem, und die Spiegelungseinstellung mit der größten Einschränkung haben immer Vorrang vor allen anderen Einstellungen und Richtlinien.

Citrix Richtlinien interagieren mit den Richtlinien, die Sie im Betriebssystem eingestellt haben. In einer Citrix Umgebung überschreiben Citrix Einstellungen die gleichen Einstellungen in einer Active Directory-Richtlinie oder in der Konfiguration des Remotedesktop-Sitzungshosts. Dazu gehören auch Einstellungen, die mit typischen Remotedesktopprotokoll-Clientverbindungseinstellungen zusammenhängen, wie Desktophintergrund, Menüanimation und das Anzeigeverhalten beim Drag & Drop. Manche Richtlinieneinstellungen, wie Secure ICA, müssen mit den Einstellungen im Betriebssystem übereinstimmen. Wenn anderswo ein höherer Verschlüsselungsgrad festgelegt wurde, kann die Secure ICA-Richtlinieneinstellung oder die Einstellung beim Veröffentlichen einer Anwendung außer Kraft gesetzt werden.

Die beim Erstellen von Bereitstellungsgruppen angegebenen Verschlüsselungseinstellungen sollten beispielsweise den gleichen Verschlüsselungsgrad verwenden, den Sie an anderer Stelle in der Umgebung verwenden.

Hinweis: Wenn im zweiten Hop eines Double-Hop-Szenarios ein Desktopbetriebssystem-VDA eine Verbindung mit einem Serverbetriebssystem-VDA herstellt, ist die Wirkung der Citrix Richtlinien auf den Desktopbetriebssystem-VDA die gleiche wie beim Benutzergerät. Wenn Richtlinien beispielsweise das Zwischenspeichern von Bildern auf dem Benutzergerät festlegen, werden die Bilder, die während des zweiten Hop in einem Double-Hop-Szenario zwischengespeichert werden, auf der Desktopbetriebssystem-VDA-Maschine zwischengespeichert.

Vergleichen von Richtlinien und Vorlagen

Sie können die Einstellungen einer Richtlinie oder Vorlage mit denen in anderen Richtlinien oder Vorlagen vergleichen. Beispielsweise ist die Prüfung von Einstellungswerten erforderlich, um sicherzustellen, dass optimale Verfahren eingehalten werden. Außerdem ist ggf. ein Vergleich von Einstellungen in einer Richtlinie oder Vorlage mit den Standardeinstellungen von Citrix erforderlich.

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus.
2. Klicken Sie auf die Registerkarte "Vergleich"und dann auf Auswählen.
3. Wählen Sie die Richtlinien oder Vorlagen aus, die Sie vergleichen möchten. Aktivieren Sie das Kontrollkästchen Mit Standardeinstellungen vergleichen, um Standardwerte im Vergleich einzuschließen.
4. Wenn Sie auf Vergleichen klicken, werden die konfigurierten Einstellungen in Spalten angezeigt.
5. Zum Anzeigen aller Einstellungen wählen Sie Alle Einstellungen anzeigen. Sie kehren zur Standardansicht zurück, indem Sie Gemeinsame Einstellungen anzeigen auswählen.

Festlegen der Richtlinienpriorität

Durch Festlegen der Richtlinienpriorität definieren Sie, welche Richtlinie Vorrang hat, wenn es Konflikte gibt. Alle Richtlinien, die mit den Zuweisungen für die Verbindung übereinstimmen, werden bei der Anmeldung eines Benutzers identifiziert. Die Richtlinien werden nach Priorität sortiert und mehrere Instanzen jeder Einstellung werden verglichen. Die einzelnen Einstellungen werden gemäß der Richtlinien-Prioritätsreihenfolge angewendet.

Sie weisen Richtlinien Prioritäten zu, indem Sie ihnen unterschiedliche Prioritätswerte in Studio geben. Neue Richtlinien erhalten standardmäßig die niedrigste Priorität. Falls widersprüchliche Richtlinieneinstellungen auftreten, setzt eine Richtlinie mit einem höheren Prioritätswert (eine Priorität von "1"hat die höchste Priorität) eine Richtlinie mit einem niedrigeren Prioritätswert außer Kraft. Einstellungen werden nach der Priorität und dem Zustand der Einstellung, z. B. ob die Einstellung deaktiviert oder aktiviert ist, zusammengeführt. Jede deaktivierte Einstellung hat Vorrang vor einer aktivierten Einstellung, deren Priorität niedriger ist. Richtlinieneinstellungen, die nicht konfiguriert sind, werden ignoriert und setzen keine Einstellungen mit niedrigerer Priorität außer Kraft.

1. Wählen Sie im Studio-Navigationsbereich Richtlinien aus. Wählen Sie die Registerkarte "Richtlinien"aus.
2. Wählen Sie eine Richtlinie.
3. Wählen Sie im Aktionsbereich "Geringere Priorität"oder "Höhere Priorität".

Ausnahmen

Wenn Sie Richtlinien für Benutzergruppen, Benutzergeräte oder Maschinen erstellen, werden Sie möglicherweise feststellen, dass für einige Mitglieder einer Gruppe Ausnahmen zu einigen Einstellungen erstellt werden müssen. Sie können Ausnahmen wie folgt erstellen:

- Erstellen Sie eine Richtlinie für die Gruppenmitglieder, für die Ausnahmen erforderlich sind, und stufen Sie die Richtlinie mit höherer Priorität ein als die Richtlinie für die gesamte Gruppe.
- Verwenden Sie den Modus Verweigern in einer Zuweisung, die Sie der Richtlinie hinzufügen.

Die Zuweisung im Modus
"Verweigern"wendet eine Richtlinie nur auf Verbindungen an, die nicht den Zuweisungskriterien entsprechen. Beispielsweise könnte eine Richtlinie folgende Zuweisungen enthalten:

- Zuweisung A ist eine Client-IP-Adressenzuweisung, die den Bereich 208.77.88.* festlegt, und der Modus ist Zulassen
- Zuweisung B ist eine Benutzerzuweisung, die ein spezifisches Benutzerkonto angibt, und der Modus ist Verweigern

Die Richtlinie wird auf alle Benutzer angewendet, die sich bei der Site mit einer IP-Adresse aus dem in Zuweisung A festgelegten Bereich anmelden. Die Richtlinie wird aber nicht auf den Benutzer angewendet, der sich mit dem in Zuweisung B festgelegten Konto anmeldet, obwohl dem Computer dieses Benutzers eine IP-Adresse aus dem in Zuweisung A festgelegten Bereich zugewiesen wurde.

Ermitteln der auf eine Verbindung angewendeten Richtlinien

Manchmal reagiert eine Verbindung nicht wie erwartet, weil mehrere Richtlinien gelten. Wenn eine Richtlinie mit einer höheren Priorität auf eine Verbindung angewendet wird, kann sie Einstellungen, die Sie in der ursprünglichen Richtlinie konfigurieren, außer Kraft setzen. Sie können ermitteln, wie die Richtlinieneinstellungen am Ende für eine Verbindung zusammengeführt werden, indem sie den Richtlinienergebnissatz berechnen.

Sie berechnen den Richtlinienergebnissatz mit folgenden Methoden:

- Verwenden Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung, um ein Verbindungsszenario zu simulieren und festzustellen, wie Citrix Richtlinien angewendet werden können. Sie können Bedingungen für ein Verbindungsszenario angeben, z. B. Domänencontroller, Benutzer, Citrix Richtlinienzuweisungsbeweiswerte und simulierte Umgebungseinstellungen wie langsame Netzwerkverbindungen. Der von dem Assistenten erstellte Bericht listet die Citrix Richtlinien auf, die in dem Szenario wahrscheinlich wirksam werden. Wenn Sie beim Controller als Domänenbenutzer angemeldet sind, berechnet der Assistent den Richtlinienergebnissatz anhand von Richtlinieneinstellungen für die Site und Active Directory-Gruppenrichtlinienobjekten.

- Verwenden Sie das Tool "Gruppenrichtlinienergebnisse", um einen Bericht zu erstellen, der beschreibt, welche Citrix Richtlinien für einen bestimmten Benutzer oder einen bestimmten Controller angewendet werden. Das Tool "Gruppenrichtlinienergebnisse"unterstützt Sie dabei, den aktuellen Zustand von Gruppenrichtlinienobjekten in der Umgebung zu evaluieren, und generiert einen Bericht, in dem beschrieben wird, wie diese Objekte, einschließlich Citrix Richtlinien, derzeit auf einen bestimmten Benutzer und Controller angewendet werden.

Sie können den Assistenten für die Citrix Gruppenrichtlinienmodellierung im Bereich Aktionen in Studio starten. Sie können beide Tools in der Gruppenrichtlinien-Verwaltungskonsole von Windows starten.

Wenn Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung oder das Tool "Gruppenrichtlinienergebnisse"über die Gruppenrichtlinien-Verwaltungskonsole ausführen, werden die mit Studio erstellten Site-Richtlinieneinstellungen nicht in den Richtlinienergebnissatz einbezogen.

Um sicherzustellen, dass Sie den umfassendsten Richtlinienergebnissatz erhalten, empfiehlt Citrix das Starten des Assistenten für die Citrix Gruppenrichtlinienmodellierung über Studio, es sei denn, Sie erstellen Richtlinien nur über die Gruppenrichtlinien-Verwaltungskonsole.

Verwenden des Assistenten für die Citrix Gruppenrichtlinienmodellierung

Öffnen Sie den Assistenten für die Citrix Gruppenrichtlinienmodellierung mit einer der folgenden Optionen:

- Wählen Sie Richtlinien im Navigationsbereich von Studio, wählen Sie dann die Registerkarte "Modellierung"und dann im Aktionsbereich die Option Modellierungsassistenten starten.
- Starten Sie die Gruppenrichtlinien-Verwaltungskonsole (gpmc.msc), klicken Sie mit der rechten Maustaste in der Konsolenstruktur auf Citrix Gruppenrichtlinienmodellierung und wählen Sie dann Citrix Gruppenrichtlinienmodellierungsassistent aus.

Folgen Sie den Anweisungen des Assistenten, um den Domänencontroller, Benutzer, Computer, Umgebungseinstellungen und Citrix Zuweisungskriterien für die Simulation auszuwählen. Wenn Sie auf Fertig stellen klicken, erstellt der Assistent einen Bericht mit den Modellierungsergebnissen. In Studio wird der Bericht im mittleren Bereich unter der Registerkarte Modellierung angezeigt.

Zum Anzeigen des Berichts wählen Sie Modellierungsbericht anzeigen.

Problembehandlung bei Richtlinien

Für Benutzer, IP-Adressen und andere zugewiesene Objekte können mehrere Richtlinien gleichzeitig gelten. Dies kann zu Konflikten führen, wenn eine Richtlinie sich nicht wie erwartet verhält. Wenn Sie den Citrix Gruppenrichtlinienmodellierungsassistenten oder das Gruppenrichtlinienergebnisse-Tool ausführen, entdecken Sie möglicherweise, dass keine Richtlinien auf die Benutzerverbindungen

angewendet werden. In diesen Fall sind Benutzer nicht von Richtlinieneinstellungen betroffen, wenn sie sich unter Bedingungen mit Anwendungen verbinden, die den Richtlinienkriterien entsprechen. Dies passiert in folgenden Fällen:

- Keine Richtlinie hat eine Zuweisung, die den Richtlinienkriterien entspricht.
- Richtlinien, die der Zuweisung entsprechen, haben keine konfigurierten Einstellungen.
- Richtlinien, die der Zuweisung entsprechen, sind deaktiviert.

Wenn Sie Richtlinieneinstellungen auf Verbindungen anwenden möchten, die bestimmten Kriterien entsprechen, stellen Sie Folgendes sicher:

- Die Richtlinien, die auf diese Verbindungen angewendet werden sollen, sind aktiviert.
- In den Richtlinien, die Sie anwenden möchten, sind die geeigneten Einstellungen konfiguriert.

Standardrichtlinieneinstellungen

August 18, 2021

Die folgenden Tabellen enthalten Richtlinieneinstellungen, die Standardeinstellungen und die VDA-Versionen, für die sie gelten.

ICA

Name	Standardeinstellung	VDA
Clientzwischenablagenumleitung	Zugelassen	Alle VDA-Versionen
Desktop starten	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version
EDT	Aus	VDA 7.13. Siehe Adaptiver Transport.
ICA-Listener - Verbindungstimeout	120.000 Millisekunden	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
ICA-Listenerportnummer	1494	Alle VDA-Versionen
Starten nicht-veröffentlichter Programme bei Clientverbindung	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Zum Schreiben in Clientzwischenablage zugelassene Formate	Keine Formate angegeben	VDA 7.6 bis aktuelle Version
Schreiben in Clientzwischenablage einschränken	Nicht zugelassen	VDA 7.6 bis aktuelle Version
Schreiben in Sitzungszwischenablage einschränken	Nicht zugelassen	VDA 7.6 bis aktuelle Version
Zum Schreiben in Sitzungszwischenablage zugelassene Formate	Keine Formate angegeben	VDA 7.6 bis aktuelle Version

ICA/Adobe Flash-Bereitstellung/Flash-Umleitung

Name	Standardeinstellung	VDA
Verhindern von Flash-Videofallback	Nicht konfiguriert	VDA 7.6 FP3 bis aktuelle Version
Fehler beim Verhindern von Flash-Videofallback *.swf		VDA 7.6 FP3 bis aktuelle Version

ICA/Audio

Name	Standardeinstellung	VDA
Audio Plug & Play	Zugelassen	VDA für Server-OS 7 bis aktuelle Version
Audioqualität	Hoch - High Definition Audio	Alle VDA-Versionen
Clientaudioumleitung	Zugelassen	Alle VDA-Versionen
Clientmikrofonumleitung	Zugelassen	Alle VDA-Versionen

ICA/Automatische Wiederverbindung von Clients

Name	Standardeinstellung	VDA
Automatische Wiederverbindung von Clients	Zugelassen	Alle VDA-Versionen
Authentifizierung bei automatischer Wiederverbindung von Clients	Keine Authentifizierung erforderlich	Alle VDA-Versionen
Protokollierung der automatischen Wiederverbindung von Clients	Kein Protokollieren von Wiederverbindungsereignissen	Alle VDA-Versionen

ICA/Bandbreite

Name	Standardeinstellung	VDA
Bandbreitenlimit für die Audioumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für die Audioumleitung (Prozent)	0	Alle VDA-Versionen
Bandbreitenlimit für Client-USB-Geräteumleitung	0 KBit/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bandbreitenlimit für Zwischenablagenumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Zwischenablagenumleitung (Prozent)	0	Alle VDA-Versionen
Bandbreitenlimit für COM-Portumleitung	0 KBit/s	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.

Name	Standardeinstellung	VDA
Bandbreitenlimit für COM-Portumleitung (Prozent)	0	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.
Bandbreitenlimit für Dateiumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Dateiumleitung (Prozent)	0	Alle VDA-Versionen
Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung	0 KBit/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 und VDA für Desktop-OS 7 bis zum aktuellen VDA für Server-OS und VDA für Desktop-OS
Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bandbreitenlimit für LPT-Portumleitung	0 KBit/s	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.
Bandbreitenlimit für LPT-Portumleitung (Prozent)	0	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.
Bandbreitenlimit für Sitzung insgesamt	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Druckerumleitung	0 KBit/s	Alle VDA-Versionen
Bandbreitenlimit für Druckerumleitung (Prozent)	0	Alle VDA-Versionen
Bandbreitenlimit für TWAIN-Geräteumleitung	0 KBit/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)	0	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Clientsensoren

Name	Standardeinstellung	VDA
Anwendungen können den physischen Standort des Clientgeräts verwenden	Nicht zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Desktopbenutzeroberfläche

Name	Standardeinstellung	VDA
Desktopgestaltungsumleitung	Deaktiviert (7.6 FP3 bis aktuelle Version), Aktiviert (5.6 bis 7.6 FP2)	VDA 5.6, VDA für Desktopbetriebssysteme 7 bis aktuelle Version
Grafikqualität Desktopgestaltung	Mittel	VDA 5.6, VDA für Desktopbetriebssysteme 7 bis aktuelle Version
Desktophintergrund	Zugelassen	Alle VDA-Versionen
Menüanimation	Zugelassen	Alle VDA-Versionen
Fensterinhalt beim Verschieben anzeigen	Zugelassen	Alle VDA-Versionen

ICA/Endbenutzerüberwachung

Name	Standardeinstellung	VDA
ICA-Roundtripberechnung	Aktiviert	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Intervall für ICA-Roundtripberechnung	15 Sekunden	Alle VDA-Versionen
ICA-Roundtrip für Verbindungen im Leerlauf berechnen	Deaktiviert	Alle VDA-Versionen

ICA/Enhanced Desktop Experience

Name	Standardeinstellung	VDA
Enhanced Desktop Experience	Zugelassen	VDA für Server-OS 7 bis aktuelle Version

ICA/Dateiumleitung

Name	Standardeinstellung	VDA
Clientlaufwerke automatisch verbinden	Zugelassen	Alle VDA-Versionen
Clientlaufwerkumleitung	Zugelassen	Alle VDA-Versionen
Lokale Clientfestplattenlaufwerke	Zugelassen	Alle VDA-Versionen
Clientdiskettenlaufwerke	Zugelassen	Alle VDA-Versionen
Clientnetzlaufwerke	Zugelassen	Alle VDA-Versionen
Optische Clientlaufwerke	Zugelassen	Alle VDA-Versionen
Clientwechsellaufwerke	Zugelassen	Alle VDA-Versionen
Host-zu-Client-Umleitung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
Clientlaufwerksbuchstaben erhalten	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Schreibgeschützter Zugriff auf Clientlaufwerke	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Umleitung spezieller Ordner	Zugelassen	Nur Webinterface-Bereitstellungen; VDA für Server-OS 7 bis aktuelle Version
Asynchrones Schreiben verwenden	Deaktiviert	Alle VDA-Versionen

ICA/Grafik

Name	Standardeinstellung	VDA
Visuell verlustfreie Komprimierung zulassen	Deaktiviert	VDA 7.6 bis aktuelle Version
Anzeigespeicherlimit	65536 KBit	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Herabsetzungspräferenz für Anzeigemodus	Zuerst Farbtiefe herabsetzen	Alle VDA-Versionen
Dynamische Fenstervorschau	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bildzwischenspeicherung	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Legacygrafikmodus	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Maximal zugelassene Farbtiefe	32 Bit pro Pixel	Alle VDA-Versionen
Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Warteschlange und Verwerfen	Aktiviert	Alle VDA-Versionen
Verwenden von Videocodec für die Komprimierung	Videocodec verwenden, wenn bevorzugt	VDA 7.6 FP3 bis aktuelle Version
Verwenden der Hardwarecodierung für Videocodec	Aktiviert	VDA 7.11 bis aktuelle Version

ICA/Grafik/Zwischenspeicherung

Name	Standardeinstellung	VDA
Schwellenwert für permanenten Cache	3000000 Bit/s	VDA für Server-OS 7 bis aktuelle Version

ICA/Grafik/Framehawk

Name	Standardeinstellung	VDA
Framehawk-Anzeigekanal	Deaktiviert	VDA 7.6 FP2 bis aktuelle Version
Portbereich für Framehawk-Anzeigekanal	3224, 3324	VDA 7.6 FP2 bis aktuelle Version

ICA/Keep-Alive

Name	Standardeinstellung	VDA
ICA-Keep-Alive - Timeout	60 Sekunden	Alle VDA-Versionen
ICA-Keep-Alives	Keine ICA-Keep-Alive-Meldungen senden	Alle VDA-Versionen

ICA/Zugriff auf lokale Anwendungen

Name	Standardeinstellung	VDA
Lokalen App-Zugriff zulassen	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
URL-Umleitungssperrliste	Keine Sites angegeben	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
URL-Umleitungspositivliste	Keine Sites angegeben	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Mobilerfahrung

Name	Standardeinstellung	VDA
Automatische Anzeige der Tastatur	Nicht zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Für Fingereingabe optimierten Desktop starten	Zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version Diese Einstellung ist deaktiviert und für Maschinen mit Windows 10 und Windows Server 2016 nicht verfügbar.
Kombinationsfelder remoten	Nicht zugelassen	VDA 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Multimedia

Name	Standardeinstellung	VDA
HTML5-Videoumleitung	Nicht zugelassen	VDA 7.12 bis aktuelle Version

Name	Standardeinstellung	VDA
Videoqualität beschränken	Nicht konfiguriert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Multimediakonferenzen	Zugelassen	Alle VDA-Versionen
Optimierung von Windows Media-Multimediaumleitung über WAN	Zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
GPU für die Optimierung von Windows Media-Multimediaumleitung über WAN verwenden	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Verhinderung von Fallback auf Windows Media	Nicht konfiguriert	VDA 7.6 FP3 bis aktuelle Version
Clientseitiger Abruf von Windows Media-Inhalten	Zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Windows Media-Umleitung	Zugelassen	Alle VDA-Versionen
Windows Media-Umleitungspuffergröße	5 Sekunden	VDA 5, 5.5, 5.6 FP1
Verwendung von Windows Media-Umleitungspuffergröße	Deaktiviert	VDA 5, 5.5, 5.6 FP1

ICA/Multistreamverbindungen

Name	Standardeinstellung	VDA
Audio über UDP	Zugelassen	VDA für Server-OS 7 bis aktuelle Version
Audio-UDP-Portbereich	16500, 16509	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Multiportrichtlinie	Primärer Port (2598) hat hohe Priorität	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Multistreamcomputereinstellung	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Multistreambenutzereinstellung	Deaktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA\Portumleitung

Name	Standardeinstellung	VDA
Client-COM-Ports automatisch verbinden	Deaktiviert	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.
Client-LPT-Ports automatisch verbinden	Deaktiviert	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.
Client-COM-Portumleitung	Nicht zugelassen	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.
Client-LPT-Portumleitung	Nicht zugelassen	Alle VDA-Versionen; bei VDA 7.0 bis 7.8 müssen Sie diese Einstellung in der Registrierung konfigurieren.

ICA/Drucken

Name	Standardeinstellung	VDA
Clientdruckerumleitung	Zugelassen	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Standarddrucker	Hauptdrucker des Clients als Standarddrucker verwenden	Alle VDA-Versionen
Druckerzuordnungen	Der aktuelle Drucker des Benutzers wird als Standarddrucker in der Sitzung verwendet.	Alle VDA-Versionen
Präferenz für Ereignisprotokoll bei automatischer Druckererstellung	Fehler und Warnungen protokollieren	Alle VDA-Versionen
Sitzungsdrucker	Keine Drucker angegeben	Alle VDA-Versionen
Warten bis Drucker erstellt sind (Desktop)	Deaktiviert	Alle VDA-Versionen

ICA/Drucken/Clientdrucker

Name	Standardeinstellung	VDA
Clientdrucker automatisch erstellen	Alle Clientdrucker automatisch erstellen	Alle VDA-Versionen
Generischen universellen Drucker automatisch erstellen	Deaktiviert	Alle VDA-Versionen
Clientdruckernamen	Standarddruckernamen	Alle VDA-Versionen
Direkte Verbindungen zu Druckservern	Aktiviert	Alle VDA-Versionen
Druckertreiberzuordnung und -kompatibilität	Keine Regeln angegeben	Alle VDA-Versionen
Speicherung von Druckereigenschaften	Im Profil speichern, wenn sie nicht auf dem Client gespeichert sind	Alle VDA-Versionen
Gespeicherte und wiederhergestellte Clientdrucker	Zugelassen	VDA 5, 5.5, 5.6 FP1

ICA/Drucken/Treiber

Name	Standardeinstellung	VDA
Automatische Installation von mitgelieferten Druckertreibern	Aktiviert	Alle VDA-Versionen
Priorität universeller Treiber	EMF, XPS, PCL5c, PCL4, PS	Alle VDA-Versionen
Verwendung universeller Druckertreiber	Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist	Alle VDA-Versionen

ICA/Drucken/Universeller Druckserver

Name	Standardeinstellung	VDA
Universellen Druckserver aktivieren	Deaktiviert	Alle VDA-Versionen
Port für Druckdatenstrom des universellen Druckservers (CGP)	7229	Alle VDA-Versionen
Universeller Druckserver - Eingabebandbreitenlimit für Druckdatenstrom (KBit/s)	0	Alle VDA-Versionen
Port für universellen Druckserverwebdienst (HTTP/SOAP)	8080	Alle VDA-Versionen
Universelle Druckserver für den Lastausgleich		VDA 7.9 bis aktuelle Version
Außer-Betrieb-Schwellenwert für universelle Druckserver	180 (Sekunden)	VDA 7.9 bis aktuelle Version

ICA/Drucken/Universelles Drucken

Name	Standardeinstellung	VDA
Universelles Drucken - EMF-Verarbeitungsmodus	Direkt zum Drucker spoolen	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Universelles Drucken - Bildkomprimierungslimit	Optimale Qualität (verlustfreie Komprimierung)	Alle VDA-Versionen
Universelles Drucken - Optimierungsstandards	Bildkomprimierung: Gewünschte Bildqualität = Standardqualität, Heavyweight-Komprimierung aktivieren = False. Zwischenspeicherung von Bildern und Schriftarten: Zwischenspeicherung eingebetteter Bilder zulassen = True, Zwischenspeicherung eingebetteter Schriftarten zulassen = True. Nicht-Administratoren können diese Einstellungen anpassen = False	Alle VDA-Versionen
Universelles Drucken - Vorschaueinstellung	Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwenden	Alle VDA-Versionen
Universelles Drucken - Druckqualitätslimit	Kein Limit	Alle VDA-Versionen

ICA/Sicherheit

Name	Standardeinstellung	VDA
SecureICA-Mindestverschlüsselungsgrad	Standard	VDA für Server-OS 7 bis aktuelle Version

ICA/Serverlimits

Name	Standardeinstellung	VDA
Serverleerlauf-Zeitintervall	0 Millisekunden	VDA für Server-OS 7 bis aktuelle Version

ICA/Sitzungslimits

Name	Standardeinstellung	VDA
Timer für getrennte Sitzung	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Getrennte Sitzungen - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsverbindungstimer	Deaktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsverbindung - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsleerlauftimer	Aktiviert	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version
Sitzungsleerlauf - Timerintervall	1440 Minuten	VDA 5, 5.5, 5.6 FP1, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Sitzungszuverlässigkeit

Name	Standardeinstellung	VDA
Sitzungszuverlässigkeit - Verbindungen	Zugelassen	Alle VDA-Versionen
Sitzungszuverlässigkeit – Portnummer	2598	Alle VDA-Versionen
Sitzungszuverlässigkeit - Timeout	180 Sekunden	Alle VDA-Versionen

ICA/Zeitzonensteuerung

Name	Standardeinstellung	VDA
Lokale Zeitzone für Legacyclients schätzen	Aktiviert	VDA für Server-OS 7 bis aktuelle Version
Lokale Zeit des Clients verwenden	Serverzeitzone verwenden	Alle VDA-Versionen

ICA/TWAIN-Geräte

Name	Standardeinstellung	VDA
TWAIN-Geräteumleitung für Client	Zugelassen	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
TWAIN-Komprimierungsgrad	Mittel	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/USB-Geräte

Name	Standardeinstellung	VDA
Regeln für die Client-USB-Geräteoptimierung	Aktiviert (VDA 7.6 FP3 bis aktuelle Version); Deaktiviert (VDA 7.11 bis aktuelle Version). In der Standardeinstellung sind keine Regeln angegeben.	VDA 7.6 FP3 bis aktuelle Version
Client-USB-Geräteumleitung	Nicht zugelassen	Alle VDA-Versionen
Regeln für die Client-USB-Geräteumleitung	Keine Regeln angegeben	Alle VDA-Versionen
Client-USB-Geräteumleitung für Plug & Play-Geräte	Zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Visuelle Anzeige

Name	Standardeinstellung	VDA
Bevorzugte Farbtiefe für einfache Grafiken	24 Bit pro Pixel	VDA 7.6 FP3 bis aktuelle Version
Frameratesollwert	30 f/s	Alle VDA-Versionen
Bildqualität	Mittel	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Visuelle Anzeige/Bewegtbilder

Name	Standardeinstellung	VDA
Mindestbildqualität	Normal	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Bewegtbildkomprimierung	Aktiviert	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Grad der progressiven Komprimierung	Ohne	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Schwellenwert für progressive Komprimierung	2147483647 Kbit/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Mindestframeratesollwert	10 f/s	VDA 5.5, 5.6 FP1, VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

ICA/Visuelle Anzeige/Festbilder

Name	Standardeinstellung	VDA
Zusätzliche Farbkomprimierung	Deaktiviert	Alle VDA-Versionen
Schwellenwert für zusätzliche Farbkomprimierung	8192 Kbit/s	Alle VDA-Versionen
Heavyweight-Komprimierung	Deaktiviert	Alle VDA-Versionen
Grad der verlustreichen Komprimierung	Mittel	Alle VDA-Versionen
Schwellenwert für verlustreiche Komprimierung	2147483647 Kbit/s	Alle VDA-Versionen

ICA/WebSockets

Name	Standardeinstellung	VDA
WebSockets-Verbindungen	Nicht zugelassen	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
WebSockets-Portnummer	8008	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Vertrauenswürdige WebSockets-Ursprungsserverliste	Bei Verwendung des Platzhalters * wird allen Receiver für Web-URLs vertraut.	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Lastverwaltung

Name	Standardeinstellung	VDA
Toleranzwert für gleichzeitige Anmeldungen	2	VDA für Server-OS 7 bis aktuelle Version
CPU-Nutzung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
CPU-Nutzung ausschließlich Prozesspriorität	Unter normal oder niedrig	VDA für Server-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Datenträgernutzung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
Sitzungshöchstanzahl	250	VDA für Server-OS 7 bis aktuelle Version
Speichernutzung	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version
Speichernutzung - Ausgangslast	Nulllast: 768 MB	VDA für Server-OS 7 bis aktuelle Version

Profilverwaltung/Erweiterte Einstellungen

Name	Standardeinstellung	VDA
Automatische Konfiguration deaktivieren	Deaktiviert	Alle VDA-Versionen
Benutzer bei Problem abmelden	Deaktiviert	Alle VDA-Versionen
Anzahl Wiederholungen beim Zugriff auf gesperrte Dateien	5	Alle VDA-Versionen
Internet-Cookiedateien bei Abmeldung verarbeiten	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Grundeinstellungen

Name	Standardeinstellung	VDA
Aktiv zurückschreiben	Deaktiviert	Alle VDA-Versionen
Profilverwaltung aktivieren	Deaktiviert	Alle VDA-Versionen
Ausgeschlossene Gruppen	Deaktiviert. Mitglieder aller Benutzergruppen werden verarbeitet.	Alle VDA-Versionen
Unterstützung von Offlineprofilen	Deaktiviert	Alle VDA-Versionen
Pfad zu Benutzerspeicher	Windows	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Anmeldungen lokaler Administratoren verarbeiten	Deaktiviert	Alle VDA-Versionen
Verarbeitete Gruppen	Deaktiviert. Mitglieder aller Benutzergruppen werden verarbeitet.	Alle VDA-Versionen

Profilverwaltung/Plattformübergreifende Einstellungen

Name	Standardeinstellung	VDA
Benutzergruppen für plattformübergreifende Einstellungen	Deaktiviert. Alle in Verarbeitete Gruppen angegebenen Benutzergruppen werden verarbeitet	Alle VDA-Versionen
Plattformübergreifende Einstellungen aktivieren	Deaktiviert	Alle VDA-Versionen
Pfad zu plattformübergreifenden Definitionen	Deaktiviert. Kein Pfad angegeben.	Alle VDA-Versionen
Pfad zum Speicher für plattformübergreifende Einstellungen	Deaktiviert. Windows\PM_CM wird verwendet.	Alle VDA-Versionen
Quelle für Erstellung plattformübergreifender Einstellungen	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Dateisystem/Ausschlüsse

Name	Standardeinstellung	VDA
Ausschlussliste - Verzeichnisse	Deaktiviert. Alle Ordner im Benutzerprofil werden synchronisiert.	Alle VDA-Versionen
Ausschlussliste - Dateien	Deaktiviert. Alle Dateien im Benutzerprofil werden synchronisiert.	Alle VDA-Versionen

Profilverwaltung/Dateisystem/Synchronisierung

Name	Standardeinstellung	VDA
Zu synchronisierende Verzeichnisse	Deaktiviert. Nur nicht ausgeschlossene Ordner werden synchronisiert.	Alle VDA-Versionen
Zu synchronisierende Dateien	Deaktiviert. Nur nicht ausgeschlossene Dateien werden synchronisiert.	Alle VDA-Versionen
Zu spiegelnde Ordner	Deaktiviert. Es werden keine Ordner gespiegelt.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung

Name	Standardeinstellung	VDA
Administratorzugriff gewähren	Deaktiviert	Alle VDA-Versionen
Domänennamen einschließen	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/AppData(Roaming)

Name	Standardeinstellung	VDA
AppData(Roaming)-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für AppData(Roaming)	Inhalte werden zu dem in der Richtlinieneinstellung AppData(Roaming)-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Kontakte

Name	Standardeinstellung	VDA
‘Kontakte’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Kontakte’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Kontakte’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Desktop

Name	Standardeinstellung	VDA
‘Desktop’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Desktop’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Desktop’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Dokumente

Name	Standardeinstellung	VDA
‘Dokumente’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Dokumente’	Inhalte werden zu dem in der Richtlinieneinstellung “‘Dokumente’-Pfad” angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Downloads

Name	Standardeinstellung	VDA
‘Downloads’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Downloads’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Downloads’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Favoriten

Name	Standardeinstellung	VDA
‘Favoriten’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Favoriten’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Favoriten’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Links

Name	Standardeinstellung	VDA
‘Links’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Links’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Links’ -Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Musik

Name	Standardeinstellung	VDA
‘Musik’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Musik’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Musik’ -Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Bilder

Name	Standardeinstellung	VDA
‘Bilder’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Bilder’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Bilder’ -Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Gespeicherte Spiele

Name	Standardeinstellung	VDA
‘Gespeicherte Spiele’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Gespeicherte Spiele’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Gespeicherte Spiele’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Suchen

Name	Standardeinstellung	VDA
‘Suchen’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Suchen’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Suchen’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Startmenü

Name	Standardeinstellung	VDA
Startmenü-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Startmenü’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Startmenü’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Ordnerumleitung/Videos

Name	Standardeinstellung	VDA
‘Videos’-Pfad	Deaktiviert. Kein Speicherort angegeben.	Alle VDA-Versionen
Umleitungseinstellungen für ‘Videos’	Inhalte werden zu dem in der Richtlinieneinstellung ‘Videos’-Pfad angegebenen UNC-Pfad umgeleitet.	Alle VDA-Versionen

Profilverwaltung/Protokolleinstellungen

Name	Standardeinstellung	VDA
Active Directory-Aktionen	Deaktiviert	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Allgemeine Informationen	Deaktiviert	Alle VDA-Versionen
Allgemeine Warnungen	Deaktiviert	Alle VDA-Versionen
Protokollierung aktivieren	Deaktiviert	Alle VDA-Versionen
Dateisystemaktionen	Deaktiviert	Alle VDA-Versionen
Dateisystembenachrichtigungen	Deaktiviert	Alle VDA-Versionen
Abmeldung	Deaktiviert	Alle VDA-Versionen
Anmeldebildschirm	Deaktiviert	Alle VDA-Versionen
Maximale Größe der Protokolldatei	1048576	Alle VDA-Versionen
Pfad zur Protokolldatei	Deaktiviert. Protokolldateien werden im Standardspeicherort gespeichert: %System-Root%\System32\Logfiles\UserProfileManager.	Alle VDA-Versionen
Persönliche Benutzerinformationen	Deaktiviert	Alle VDA-Versionen
Richtlinienwerte bei Anmeldung und Abmeldung	Deaktiviert	Alle VDA-Versionen
Registrierungsaktionen	Deaktiviert	Alle VDA-Versionen
Registrierungsunterschiede bei der Abmeldung	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Profilverarbeitung

Name	Standardeinstellung	VDA
Verzögerung vor dem Löschen von zwischengespeicherten Profilen	0	Alle VDA-Versionen
Lokal zwischengespeicherte Profile nach Abmeldung löschen	Deaktiviert	Alle VDA-Versionen
Behandlung von Konflikten lokaler Profile	Lokales Profil verwenden	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Migration vorhandener Profile	Lokal und Roaming	Alle VDA-Versionen
Pfad zum Vorlagenprofil	Deaktiviert. Neue Benutzerprofile werden von dem Standardbenutzerprofil auf dem Gerät erstellt, auf dem sich ein Benutzer als Erstes anmeldet.	Alle VDA-Versionen
Vorlagenprofil überschreibt lokales Profil	Deaktiviert	Alle VDA-Versionen
Vorlagenprofil überschreibt Roamingprofil	Deaktiviert	Alle VDA-Versionen
Als verbindliche Citrix Profil für alle Anmeldungen verwendete Vorlagenprofil	Deaktiviert	Alle VDA-Versionen

Profilverwaltung/Registrierung

Name	Standardeinstellung	VDA
Ausschlussliste	Deaktiviert. Alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet, wenn ein Benutzer sich abmeldet.	Alle VDA-Versionen
Aufnahmeliste	Deaktiviert. Alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet, wenn ein Benutzer sich abmeldet.	Alle VDA-Versionen

Profilverwaltung/Gestreamte Benutzerprofile

Name	Standardeinstellung	VDA
Immer zwischenspeichern	Deaktiviert	Alle VDA-Versionen

Name	Standardeinstellung	VDA
Immer Cachegröße	0 MBit	Alle VDA-Versionen
Profilstreaming	Deaktiviert	Alle VDA-Versionen
Gestreamte Benutzerprofilgruppen	Deaktiviert. Alle Benutzerprofile in einer Organisationseinheit werden normal verarbeitet.	Alle VDA-Versionen
Timeout für gesperrte Dateien im ausstehenden Bereich (Tage)	1 Tag	Alle VDA-Versionen

Receiver

Name	Standardeinstellung	VDA
StoreFront-Kontenliste	Keine Stores angegeben	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Virtual Delivery Agent

Name	Standardeinstellung	VDA
IPv6-Netzwerkmaske für Controllerregistrierung	Keine Netzwerkmaske angegeben.	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Controllerregistrierungsport	80	Alle VDA-Versionen
Controller-SIDs	Keine SIDs angegeben	Alle VDA-Versionen
Controller	Keine Controller angegeben	Alle VDA-Versionen
Automatische Controllerupdates aktivieren	Aktiviert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version
Nur IPv6-Controllerregistrierung verwenden	Deaktiviert	VDA für Server-OS 7 bis aktuelle Version, VDA für Desktop-OS 7 bis aktuelle Version

Name	Standardeinstellung	VDA
Site-GUID	Kein GUID angegeben.	Alle VDA-Versionen

Virtual Delivery Agent für HDX 3D Pro

Name	Standardeinstellung	VDA
Verlustfrei aktivieren	Aktiviert	VDA 5.5, 5.6 FP1
HDX 3D Pro-Qualitätseinstellungen		VDA 5.5, 5.6 FP1

Virtual Delivery Agent

Name	**Standardeinstellung**	**VDA**
Prozessüberwachung aktivieren	Deaktiviert	VDA 7.11 bis aktuelle Version
Ressourcenüberwachung aktivieren	Aktiviert	VDA 7.11 bis aktuelle Version

Virtuelle IP

Name	Standardeinstellung	VDA
Virtuelle IP - Loopbackunterstützung	Deaktiviert	VDA 7.6 bis aktuelle Version
Virtuelle IP - Programme für virtuelles Loopback	-	VDA 7.6 bis aktuelle Version

Referenz für Richtlinieneinstellungen

November 29, 2018

Richtlinien enthalten Einstellungen, die gelten, wenn die Richtlinie angewendet wird. Die Beschreibungen in diesem Abschnitt geben auch an, ob zusätzliche Einstellungen zum Aktivieren eines Features erforderlich sind oder ob Einstellungen sich ähnlich sind.

Kurzanleitung

Die folgenden Tabellen listen die Einstellungen auf, die Sie in einer Richtlinie konfigurieren können. In der linken Spalte finden Sie die Aufgaben, in der rechten die dazugehörigen Einstellungen.

Audio

Aufgabe	Richtlinieneinstellung
Steuern der Verwendung mehrerer Audiogeräte	Audio Plug & Play
Steuern, ob Audioeingaben vom Mikrofon auf dem Benutzergerät zulässig sind	Clientmikrofonumleitung
Steuern der Audioqualität auf dem Benutzergerät	Audioqualität
Steuern der Audiozuordnung für Lautsprecher am Benutzergerät	Clientaudioumleitung

Bandbreite für Benutzergeräte

Beschränken der Bandbreite	Richtlinieneinstellung
Clientaudiozuordnung	Bandbreitenlimit für die Audioumleitung oder Bandbreitenlimit für die Audioumleitung (Prozent)
Kopieren und Einfügen mit der lokalen Zwischenablage	Bandbreitenlimit für Zwischenablageumleitung oder Bandbreitenlimit für Zwischenablagenumleitung (Prozent)
Zugriff auf lokale Clientlaufwerke in einer Sitzung	Bandbreitenlimit für Dateiumleitung oder Bandbreitenlimit für Dateiumleitung (Prozent)

Beschränken der Bandbreite	Richtlinieneinstellung
HDX MediaStream-Multimediabeschleunigung	Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung oder Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)
Clientsitzung	Bandbreitenlimit für Sitzung insgesamt
Drucken	Bandbreitenlimit für Druckerumleitung oder Bandbreitenlimit für Druckerumleitung (Prozent)
TWAIN-Geräte (wie Kameras oder Scanner)	Bandbreitenlimit für TWAIN-Geräteumleitung oder Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)
USB-Geräte	Bandbreitenlimit für Client-USB-Geräteumleitung oder Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)

Umleitung von Clientlaufwerken und Benutzergeräten

Aufgabe	Richtlinieneinstellung
Steuern, ob Laufwerke des Benutzergeräts verbunden werden, wenn Benutzer sich am Server anmelden	Clientlaufwerke automatisch verbinden
Steuern der Datenübertragung mit Kopier- und Einfügeoperationen zwischen dem Server und der lokalen Zwischenablage	Clientzwischenablagenumleitung
Steuern der Laufwerkzuordnung des Benutzergeräts	Clientlaufwerkumleitung
Steuern, ob die lokalen Festplatten des Benutzers in einer Sitzung verfügbar sind	Lokale Clientfestplattenlaufwerke und Clientlaufwerkumleitung
Steuern, ob die lokalen Diskettenlaufwerke des Benutzers in einer Sitzung verfügbar sind	Clientdiskettenlaufwerke und Clientlaufwerkumleitung
Steuern, ob die Netzlaufwerke des Benutzers in einer Sitzung verfügbar sind	Clientnetzlaufwerke und Clientlaufwerkumleitung

Aufgabe	Richtlinieneinstellung
Steuern, ob die lokalen CD-, DVD- oder Blu-ray-Laufwerke des Benutzers in einer Sitzung verfügbar sind	Optische Clientlaufwerke und Clientlaufwerkumleitung
Steuern, ob die lokalen Clientwechseldatenträger des Benutzers in einer Sitzung verfügbar sind	Clientwechseldatenträger und Clientlaufwerkumleitung
Steuern, ob TWAIN-Geräte, wie Scanner und Kameras, in einer Sitzung verfügbar sind und Steuern der Komprimierung bei der Übertragung von Bilddaten	Client-TWAIN-Geräteumleitung und TWAIN-Umleitung
Steuern, ob die USB-Geräte in einer Sitzung verfügbar sind	Client-USB-Geräteumleitung und Regeln für die Client-USB-Geräteumleitung
Geschwindigkeit beim Schreiben und Kopieren von Dateien auf einen Clientdatenträger über ein WAN erhöhen	Asynchrones Schreiben verwenden

Inhaltsumleitung

Aufgabe	Richtlinieneinstellung
Steuern der Verwendung der Inhaltsumleitung vom Server zum Benutzergerät	Host-zu-Client-Umleitung

Desktopbenutzeroberfläche

Aufgabe	Richtlinieneinstellung
Steuern, ob der Desktophintergrund in Benutzersitzungen angezeigt wird	Desktophintergrund
Anzeigen des Fensterinhalts beim Verschieben des Fensters	Fensterinhalt beim Verschieben anzeigen

Grafiken & Multimedia

Aufgabe	Richtlinieneinstellung
Steuern der maximalen Anzahl von Frames pro Sekunde, die an Benutzergeräte von virtuellen Desktops gesendet werden	Frameratesollwert
Steuern der visuellen Qualität der auf dem Benutzergerät angezeigten Bilder	Bildqualität
Steuern, ob Flash-Inhalte in Sitzungen wiedergegeben werden	Flash-Standardverhalten
Steuern, ob Flash-Inhalte auf Websites in Sitzungen angezeigt werden	URL-Liste für serverseitigen Flash-Inhaltsabruf; Flash-URL-Kompatibilitätsliste; Einstellung der Richtlinie zum Verhindern von Videofallback; Fehler beim Verhindern von Flash-Videofallback *.swf
Steuern der Komprimierung von auf dem Server wiedergegebenem Video	Videocodec zur Komprimierung verwenden; Hardwarecodierung für Videocodec verwenden
Steuern der Bereitstellung von HTML5-Multimediawebinhalt für Benutzer	HTML5-Videoumleitung

Priorisieren des Multistream-Netzwerkdatenverkehrs

Aufgabe	Richtlinieneinstellung
Angeben der Ports für ICA-Datenübertragungen über mehrere Verbindungen und Festlegen der Netzwerkprioritäten	Multiportrichtlinie
Aktivieren der Unterstützung von Multistreamverbindungen zwischen Servern und Benutzergeräten	Multistream (Computer- und Benutzereinstellungen)

Drucken

Aufgabe	Richtlinieneinstellung
Steuern der Clientdruckererstellung auf dem Benutzergerät	Automatisches Erstellen von Clientdruckern und Clientdruckerumleitung
Steuern des Speicherorts für die Druckereigenschaften	Speicherung von Druckereigenschaften

Aufgabe	Richtlinieneinstellung
Steuern, ob Druckanfragen vom Client oder vom Server verarbeitet werden	Direkte Verbindungen zu Druckservern
Steuern, ob Benutzer auf Drucker zugreifen können, die an die Benutzergeräte angeschlossen sind	Clientdruckerumleitung
Steuern, ob bei der automatischen Erstellung von Client- und Netzwerkdruckern native Windows-Treiber installiert werden	Automatische Installation von mitgelieferten Druckertreibern
Steuern, wann der universelle Druckertreiber verwendet wird	Verwendung universeller Druckertreiber
Wählen des Druckers anhand von Sitzungsinformationen eines mobilen Benutzers	Standarddrucker
Lastausgleich und Failover-Schwellenwert für universellen Druckserver festlegen	Universelle Druckserver für den Lastausgleich, Außer-Betrieb-Schwellenwert für universelle Druckserver

> Hinweis:
>
> Richtlinien können nicht zum Aktivieren eines Bildschirmschoners in einer Desktop- oder Anwendungssitzung verwendet werden. Wenn Benutzer einen Bildschirmschoner benötigen, muss dieser auf dem Benutzergerät eingerichtet werden.

Einstellungen der Richtlinie “ICA”

August 18, 2021

Der Abschnitt “ICA”enthält Richtlinieneinstellungen für ICA-Listenerverbindungen und die Zwischenablagenzuordnung.

Adaptiver Transport

Diese Einstellung steuert den Datentransport über EDT als primäre Methode mit Fallback auf TCP.

Standardmäßig ist adaptiver Transport deaktiviert (**Aus**) und TCP wird immer verwendet.

1. Aktivieren Sie in Studio die Richtlinieneinstellung “Adaptiver HDX-Transport”(standardmäßig deaktiviert). Citrix empfiehlt außerdem, dieses Feature nicht als universelle Richtlinie für alle Objekte der Site zu aktivieren.

2. Zum Aktivieren der Richtlinieneinstellung legen Sie den Wert auf **Bevorzugt** fest und klicken Sie dann auf **OK**.

Bevorzugt: Nach Möglichkeit wird adaptiver Transport über EDT verwendet, andernfalls erfolgt ein Fallback auf TCP.

Diagnosemodus: EDT wird erzwungen und das Fallback auf TCP wird deaktiviert. Citrix empfiehlt diese Einstellung nur für die Problembehandlung.

Aus. TCP wird erzwungen und EDT wird deaktiviert.

Weitere Informationen finden Sie unter Adaptiver Transport.

Timeout beim Warten auf Anwendungsstart

Über diese Einstellung wird das Timeout in Millisekunden festgelegt, das Sitzungen auf den Start der ersten Anwendung abwarten sollen. Erfolgt der Start der Anwendung nach diesem Zeitraum, wird die Sitzung beendet.

Wählen Sie die Standardzeit (10.000 Millisekunden) oder geben Sie eine Zahl in Millisekunden ein.

Clientzwischenablagenumleitung

Mit dieser Einstellung legen Sie fest, ob die Zwischenablage auf dem Clientgerät der Zwischenablage auf dem Server zugeordnet wird.

Standardmäßig ist die Umleitung der Zwischenablage zugelassen.

Wenn Sie verhindern möchten, dass Daten durch Kopieren und Einfügen über die Zwischenablage zwischen einer Sitzung und der lokalen Zwischenablage übertragen werden, wählen Sie Nicht zugelassen. Benutzer können weiterhin die Zwischenablage für das Kopieren von Daten zwischen Anwendungen einsetzen, die in Sitzungen ausgeführt werden.

Nachdem diese Einstellung zugelassen wurde, konfigurieren Sie die maximal zulässige Bandbreite, die die Zwischenablage in einer Clientverbindung verbrauchen darf. Verwenden Sie dazu die Einstellung Bandbreitenlimit für Zwischenablagenumleitung oder Bandbreitenlimit für Zwischenablagenumleitung (Prozent).

Zum Schreiben in Clientzwischenablage zugelassene Formate

Wenn die Einstellung Schreiben in Clientzwischenablage einschränken aktiviert ist, können Hostzwischenablagedaten nicht für den Clientendpunkt freigegeben werden. Mit dieser Einstellung können bestimmte Datenformate für die Zwischenablage des Clientendpunkts freigegeben werden. Um diese Einstellung zu verwenden, aktivieren Sie sie und fügen Sie die zulässigen Formate hinzu.

Die folgenden Zwischenablageformate sind vom System definiert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Die folgenden benutzerdefinierten Formate sind in XenApp und XenDesktop vordefiniert:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Das HTML-Format ist standardmäßig deaktiviert. Aktivieren des Features

- Stellen Sie sicher, dass **Clientzwischenablagenumleitung** zugelassen ist.
- Stellen Sie sicher, dass **Schreiben in Clientzwischenablage einschränken** aktiviert ist.
- Fügen Sie **Zum Schreiben in Clientzwischenablage zugelassene Formate** einen Eintrag für **CF_HTML** (sowie alle anderen Formate, die unterstützt werden sollen) hinzu.

Hinweis: Durch das Aktivieren der Unterstützung für das HTML-Zwischenablagenkopieren (HTML-Format) werden sämtliche Skripts (sofern vorhanden) von der Quelle des kopierten Inhalts an das Ziel kopiert. Vergewissern Sie sich vor dem Kopieren, dass eine Vertrauensstellung zur Quelle besteht.

Wenn Sie Inhalte mit Skripts kopieren, werden diese nur aktiviert, wenn Sie die Zieldatei als HTML-Datei speichern und ausführen.

Zusätzliche benutzerdefinierte Formate können hinzugefügt werden. Der Name des benutzerdefinierten Formats muss mit den Formaten übereinstimmen, die mit dem System registriert werden. Bei Formatnamen muss die Groß- und Kleinschreibung beachtet werden.

Diese Einstellung hat keine Gültigkeit, wenn Clientzwischenablageumleitung oder Schreiben in Clientzwischenablage einschränken auf Nicht zugelassen festgelegt ist.

Desktop starten

Mit dieser Einstellung legen Sie fest, ob Benutzer ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind, über eine ICA-Verbindung eine Verbindung zu einer Sitzung auf dem VDA herstellen können.

Standardmäßig können Benutzer ohne Administratorrechte keine Verbindung zu diesen Sitzungen herstellen.

Diese Einstellung hat keine Auswirkungen auf Benutzer ohne Administratorrechte, die in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind und eine RDP-Verbindung verwenden. Diese Benutzer können eine Verbindung zum VDA herstellen, unabhängig davon, ob diese Einstellung aktiviert ist. Diese Einstellung hat keine Auswirkungen auf Benutzer ohne Administratorrechte, die nicht in der Gruppe der Benutzer mit direktem Zugriff eines VDAs sind. Diese Benutzer können keine Verbindung zum VDA herstellen, unabhängig davon, ob diese Einstellung aktiviert ist.

ICA-Listener - Verbindungstimeout

Hinweis: Diese Einstellung gilt nur für Virtual Delivery Agents 5.0, 5.5 und 5.6 Feature Pack 1.

Mit dieser Einstellung geben Sie die maximale Wartezeit an, bis eine Verbindung mit dem ICA-Protokoll abgeschlossen wird.

Standardmäßig ist die maximale Wartezeit 120000 Millisekunden oder zwei Minuten.

ICA-Listenerportnummer

Mit dieser Einstellung konfigurieren Sie die TCP/IP-Portnummer, die vom ICA-Protokoll auf dem Server verwendet wird.

Die Standardeinstellung der Portnummer ist 1494.

Gültige Portnummern müssen zwischen 0 und 65535 liegen. Sie dürfen keinen Konflikt mit anderen gängigen Portnummern verursachen. Wenn Sie die Portnummer ändern, muss der Server neu gestartet werden, damit der neue Wert wirksam werden kann. Wenn Sie die Portnummer auf dem Server ändern, müssen Sie sie auch in jedem Citrix Receiver oder Plug-In ändern, das eine Verbindung zu diesem Server herstellt.

Starten nicht-veröffentlichter Programme bei Clientverbindung

Mit dieser Einstellung geben Sie an, ob Startanwendungen über RDP auf dem Server gestartet werden.

Standardmäßig ist das Starten von Startanwendungen über RDP auf dem Server nicht zulässig.

Startverzögerung der Abmeldeprüfung

Über diese Einstellung wird die Dauer der Verzögerung bis zum Starten der Abmeldeprüfung festgelegt. Verwenden Sie diese Richtlinie zum Vorgeben der Zeitdauer (in Sekunden), die bis zum Trennen von Clientsitzungen abgewartet wird.

Durch diese Einstellung wird auch die Zeitdauer der Benutzerabmeldung vom Server erhöht.

Schreiben in Clientzwischenablage einschränken

Wenn diese Einstellung zugelassen ist, können Hostzwischenablagedaten nicht für den Clientendpunkt freigegeben werden. Durch Aktivieren der Einstellung Zum Schreiben in Clientzwischenablage zugelassene Formate können Sie bestimmte Formate zulassen.

Die Standardeinstellung ist "Nicht zugelassen".

Schreiben in Sitzungszwischenablage einschränken

Wenn diese Einstellung zugelassen ist, können Clientzwischenablagedaten nicht für die Benutzersitzung freigegeben werden. Durch Aktivieren der Einstellung Zum Schreiben in Sitzungszwischenablage zugelassene Formate können Sie bestimmte Formate zulassen.

Die Standardeinstellung ist "Nicht zugelassen".

Zum Schreiben in Sitzungszwischenablage zugelassene Formate

Wenn die Einstellung Schreiben in Sitzungszwischenablage einschränken auf Aktiviert festgelegt ist, können Clientzwischenablagedaten nicht für Sitzungsanwendungen freigegeben werden. Mit dieser

Einstellung können jedoch bestimmte Datenformate für die Sitzungszwischenablage freigegeben werden.

Die folgenden Zwischenablageformate sind vom System definiert:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Die folgenden benutzerdefinierten Formate sind in XenApp und XenDesktop vordefiniert:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Das HTML-Format ist standardmäßig deaktiviert. Aktivieren des Features

- Stellen Sie sicher, dass **Clientzwischenablagenumleitung** zugelassen ist.
- Stellen Sie sicher, dass **Schreiben in Sitzungszwischenablage einschränken** aktiviert ist.
- Fügen Sie **Zum Schreiben in Sitzungszwischenablage zugelassene Formate** einen Eintrag für **CF_HTML** (sowie alle anderen Formate, die unterstützt werden sollen) hinzu.

Hinweis: Durch das Aktivieren der Unterstützung für das HTML-Zwischenablagenkopieren (HTML-Format) werden sämtliche Skripts (sofern vorhanden) von der Quelle des kopierten Inhalts an das

Ziel kopiert. Vergewissern Sie sich vor dem Kopieren, dass eine Vertrauensstellung zur Quelle besteht. Wenn Sie Inhalte mit Skripts kopieren, werden diese nur aktiviert, wenn Sie die Zieldatei als HTML-Datei speichern und ausführen.

Weitere benutzerdefinierte Formate können hinzugefügt werden. Der Name des benutzerdefinierten Formats muss mit den Formaten übereinstimmen, die mit dem System registriert werden. Bei Formatnamen muss die Groß- und Kleinschreibung beachtet werden.

Diese Einstellung hat keine Gültigkeit, wenn die Clientzwischenablageumleitung oder "Schreiben in Sitzungszwischenablage einschränken"auf "Nicht zugelassen"festgelegt ist.

Einstellungen der Richtlinie "Automatische Wiederverbindung von Clients"

November 29, 2018

Der Abschnitt "Automatische Wiederverbindung von Clients"enthält Richtlinieneinstellungen, mit denen Sie die automatische Wiederverbindung von Sitzungen steuern.

Automatische Wiederverbindung von Clients

Diese Einstellung legt fest, ob die automatische Wiederverbindung des gleichen Clients zulässig ist, nachdem eine Verbindung unterbrochen wurde.

Ab Citrix Receiver für Windows 4.7 verwendet die automatische Clientwiederverbindung nur die Richtlinieneinstellungen aus Citrix Studio. Bei Änderungen an diesen Richtlinien in Studio wird die automatische Wiederverbindung vom Server an den Client synchronisiert. Bei älteren Versionen von Citrix Receiver für Windows konfigurieren Sie die automatische Clientwiederverbindung über eine Studio-Richtlinie und modifizieren die Registrierung oder die Datei default.ica.

Ist die automatische Wiederverbindung zulässig, können Benutzer ihre Arbeit an der Stelle wiederaufnehmen, an der die Verbindung unterbrochen wurde. Die automatische Wiederverbindung erkennt unterbrochene Verbindungen und verbindet die Benutzer wieder mit ihren Sitzungen.

Wenn das Citrix Receiver-Cookie mit dem Schlüssel für die Sitzungs-ID und den Anmeldeinformationen nicht verwendet wird, kann bei der automatischen Wiederverbindung eine neue Sitzung gestartet werden. Diese wird anstelle der vorhandenen Sitzung gestartet. Das Cookie wird nicht verwendet, wenn es abgelaufen ist, z. B. weil die Wiederverbindung verzögert wird, oder wenn die Anmeldeinformationen neu eingegeben werden müssen. Wenn Benutzer die Sitzung absichtlich trennen, wird die automatische Wiederverbindung wird nicht ausgelöst.

Wenn eine Wiederverbindung erfolgt, ist das Sitzungsfenster ausgegraut. Ein Countdowntimer zeigt die verbleibende Zeit bis zur Wiederverbindung der Sitzung an. Wenn der Countdowntimer für die Sitzung abläuft, wird die Sitzung getrennt.

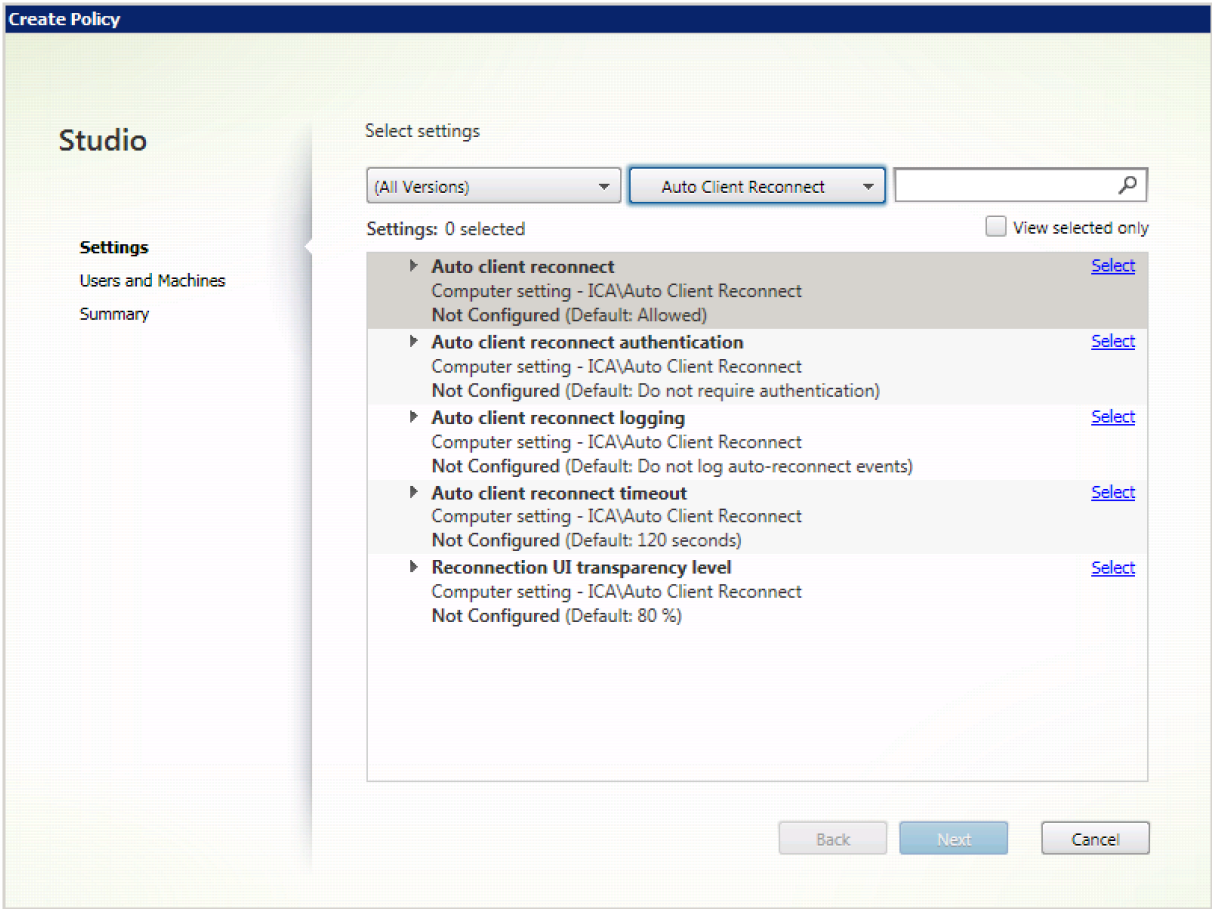
Bei Anwendungssitzungen erscheint bei zugelassener automatischer Wiederverbindung ein Countdowntimer im Infobereich, der angibt, wie viel Zeit verbleibt, bevor die Sitzung wiederverbunden wird. Citrix Receiver versucht, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Wenn die automatische Wiederverbindung zugelassen ist, versucht Citrix Receiver bei Benutzersitzungen eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Der Standardwert für diese Zeit ist zwei Minuten. Wenn Sie den Zeitraum ändern möchten, bearbeiten Sie die Richtlinie.

Standardmäßig ist die automatische Wiederverbindung zugelassen.

Deaktivieren der automatischen Wiederverbindung von Clients

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Client automatisch wieder verbinden**.
3. Legen Sie für die Richtlinie **Nicht zugelassen** fest.



Authentifizierung bei automatischer Wiederverbindung von Clients

Mit dieser Einstellung ist die Authentifizierung erforderlich, wenn die Verbindung zum Client automatisch wiederhergestellt wird.

Wenn sich ein Benutzer erstmals anmeldet, werden seine Anmeldeinformationen verschlüsselt und gespeichert und es wird ein Cookie mit dem Schlüssel erstellt. Das Cookie wird an Citrix Receiver gesendet. Wenn diese Einstellung konfiguriert ist, werden keine Cookies verwendet. Stattdessen wird ein Dialogfeld mit der Aufforderung zur Eingabe der Anmeldeinformationen angezeigt, wenn Citrix Receiver versucht, die Verbindung automatisch wiederherzustellen.

Standardmäßig ist die Authentifizierung nicht erforderlich.

Ändern der Authentifizierung bei automatischer Wiederverbindung von Clients

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Authentifizierung bei automatischer Wiederverbindung von Clients**.
3. Aktiviert oder deaktiviert die Authentifizierung.
4. Klicken Sie auf **OK**.

Protokollierung der automatischen Wiederverbindung von Clients

Mit dieser Einstellung legen Sie fest, ob die automatischen Wiederverbindungen im Ereignisprotokoll aufgezeichnet werden.

Wenn die Protokollierung aktiviert ist, werden Informationen über erfolgreiche und fehlgeschlagene Wiederverbindungsereignisse im Serversystemprotokoll aufgezeichnet. Eine Site stellt kein kombiniertes Protokoll zu Wiederverbindungsereignissen auf allen Servern zur Verfügung.

Standardmäßig ist die Protokollierung deaktiviert.

Ändern der Protokollierung der automatischen Wiederverbindung von Clients

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Protokollierung der automatischen Wiederverbindung von Clients**.
3. Aktivieren oder deaktivieren Sie die Protokollierung.
4. Klicken Sie auf **OK**.

Timeout beim automatischen Wiederverbinden von Clients

Standardmäßig ist das Timeout der automatischen Wiederverbindung auf 120 Sekunden festgelegt. Der zulässige Höchstwert beträgt 300 Sekunden.

Ändern des Timeouts beim automatischen Wiederverbinden von Clients

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Timeout für autom. Wiederverbindung von Clients**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

UI-Transparenzstufe während Wiederverbindung

Über eine Studio-Richtlinie können Sie die Transparenzstufe konfigurieren, die während der Sitzungswiederverbindung auf das XenApp- oder XenDesktop-Sitzungsfenster angewendet wird.

Standardmäßig ist die Transparenz der Benutzeroberfläche beim Wiederverbinden auf 80 % festgelegt.

Ändern der Transparenzstufe für die Benutzeroberfläche beim Wiederverbinden

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Transparenzstufe für Benutzeroberfläche bei Wiederverbindung**.
3. Bearbeiten Sie den Wert.
4. Klicken Sie auf **OK**.

Einstellungen der Richtlinie "Audio"

January 22, 2019

Der Abschnitt "Audio" enthält Richtlinieneinstellungen, mit denen Sie das Senden und Empfangen von Audiodaten auf dem Benutzergerät konfigurieren können, ohne dass es dabei zu einer unerwünschten Verschlechterung der Leistung kommt.

Audio über UDP - Real-time Transport

Diese Einstellung aktiviert bzw. deaktiviert die Audioübertragung und den Audioempfang zwischen VDA und Benutzergeräten über RTP mit UDP (User Datagram Protocol). Wenn diese Einstellung deaktiviert ist, wird Audio über TCP gesendet und empfangen.

Standardmäßig ist Audio über UDP zugelassen.

Audio Plug & Play

Mit dieser Einstellung lassen Sie die Verwendung mehrerer Audiogeräte zum Aufzeichnen und zum Wiedergeben von Ton zu oder verhindern sie.

Standardmäßig ist die Verwendung mehrerer Audiogeräte zulässig.

Diese Einstellung gilt nur für Windows-Serverbetriebssystemmaschinen.

Audioqualität

Mit dieser Einstellung legen Sie die Tonqualität fest, die in Benutzersitzungen empfangen wird.

In der Standardeinstellung ist die Tonqualität auf Hoch - High Definition-Audio eingestellt.

Um die Tonqualität zu steuern, wählen Sie eine der folgenden Optionen:

- Wählen Sie Gering - für langsame Verbindungen für Verbindungen mit geringer Bandbreite. An das Benutzergerät gesendete Audiodaten werden bis auf 16 KBit/s komprimiert. Diese Komprimierung führt zu einer erheblichen Verringerung der Tonqualität, ermöglicht aber eine akzeptable Leistung bei einer Verbindung mit geringer Bandbreite.
- Wählen Sie Mittel - für Sprache optimiert, um VoIP-Anwendungen oder Medienanwendungen bei schwierigen Netzwerkverbindungen mit Leitungen unter 512 KBit/s oder bei erheblicher Überlastung und Paketverlust bereitzustellen. Dieses Codec bietet eine schnelle Codierung und ist daher ideal für Softphones und Unified Communications-Anwendungen geeignet, wenn Sie eine serverseitige Medienverarbeitung benötigen.

Die an das Benutzergerät gesendeten Audiodaten werden bis auf 64 KBit/s komprimiert; diese Komprimierung führt zu einer moderaten Verringerung der Tonqualität auf dem Benutzergerät mit niedriger Latenz und geringem Bandbreitenverbrauch. Wenn die Einstellung eine unbefriedigende VoIP-Qualität liefert, stellen Sie sicher, dass die Richtlinie Audio über UDP - Real-time Transport auf Zugelassen eingestellt ist.

Real-time Transport (RTP) über UDP wird zurzeit nur unterstützt, wenn diese Audioqualität ausgewählt ist. Verwenden Sie diese Audioqualität, wenn Sie Medienanwendungen in schwierigen Netzwerkbedingungen bereitstellen, z. B. bei Verbindungen mit weniger als 512 KBit/s, bei denen es außerdem zu Verzögerungen und Paketverlusten im Netzwerk kommt.

- Wählen Sie Hoch - High Definition Audio für Verbindungen, bei denen die Bandbreite keine Rolle spielt und bei denen die Tonqualität wichtig ist. Clients können Audiodaten mit der nativen Abspielrate wiedergeben. Audiodaten werden mit einer hohen Qualitätsstufe bei Erhaltung der CD-Qualität komprimiert, die bis zu 112 KBit/s Bandbreite benötigt. Die Übertragung dieser Datenmenge kann zu einer höheren CPU-Belastung und Engpässen im Netzwerk führen.

Die Bandbreite wird nur verbraucht, während Audio aufgenommen oder abgespielt wird. Wenn beides gleichzeitig stattfindet, verdoppelt sich der Bandbreitenverbrauch.

Konfigurieren Sie die Einstellungen Bandbreitenlimit für die Audioumleitung oder Bandbreitenlimit für die Audioumleitung (Prozent), um die maximale Bandbreite anzugeben.

Clientaudioumleitung

Mit dieser Einstellung legen Sie fest, ob auf dem Server gehostete Anwendungen Audiodateien über ein auf dem Benutzergerät installiertes Audiogerät wiedergeben können. Diese Einstellung gibt auch an, ob Benutzer Audio aufzeichnen können.

Standardmäßig ist die Audioumleitung zugelassen.

Nachdem Sie diese Einstellung zugelassen haben, können Sie die Bandbreite beschränken, die durch die Wiedergabe oder das Aufzeichnen von Audio verbraucht wird. Durch Beschränken der Bandbreite, die durch Audio verbraucht wird, kann sich die Anwendungsleistung steigern, die Audioqualität wird aber herabgesetzt. Die Bandbreite wird nur verbraucht, während Audio aufgenommen oder abgespielt wird. Wenn beides gleichzeitig stattfindet, verdoppelt sich der Bandbreitenverbrauch. Konfigurieren Sie die Einstellungen Bandbreitenlimit für die Audioumleitung oder Bandbreitenlimit für die Audioumleitung (Prozent), um die maximale Bandbreite anzugeben.

Auf Windows-Serverbetriebssystemmaschinen müssen Sie sicherstellen, dass für Audio Plug & Play die Unterstützung mehrerer Audiogeräte aktiviert ist.

Wichtig: Wenn die Clientaudioumleitung nicht zugelassen ist, sind alle HDX-Audiofunktionen deaktiviert.

Clientmikrofonumleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Umleitung von Clientmikrofonen. Wenn aktiviert, können Benutzer Mikrofone für die Aufnahme von Audioeingaben in einer Sitzung verwenden.

Standardmäßig ist die Clientmikrofonumleitung zugelassen.

Aus Sicherheitsgründen werden Benutzer darauf hingewiesen, wenn Server, die keine vertrauenswürdige Beziehung zu den Geräten haben, auf Mikrofone zugreifen. Benutzer können den Zugriff ermöglichen oder ablehnen. Benutzer können die Warnung in Citrix Receiver deaktivieren.

Auf Windows-Serverbetriebssystemmaschinen müssen Sie sicherstellen, dass für Audio Plug & Play die Unterstützung mehrerer Audiogeräte aktiviert ist.

Wenn die Einstellung Clientaudioumleitung auf dem Benutzergerät deaktiviert ist, hat diese Regel keine Auswirkung.

Einstellungen der Richtlinie "Bandbreite"

April 4, 2019

Der Abschnitt "Bandbreite"enthält Richtlinieneinstellungen, mit denen Sie Leistungsprobleme vermeiden können, die sich aus der Bandbreitenverwendung in der Clientsitzung ergeben.

> Wichtig:
>
> Die Verwendung dieser Richtlinieneinstellungen mit den "Multistream"-Richtlinieneinstellungen kann zu unerwarteten Ergebnissen führen. Wenn Sie Multistreameinstellungen in einer Richtlinie verwenden, stellen Sie sicher, dass diese Richtlinieneinstellungen für das Bandbreitenlimit nicht eingeschlossen sind.

Bandbreitenlimit für die Audioumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Wiedergabe oder die Aufnahme von Audio in einer Benutzersitzung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für die Audioumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für die Audioumleitung (Prozent)

Mit dieser Einstellung geben Sie das maximal zulässige Bandbreitenlimit für die Wiedergabe oder die Aufnahme von Audio in als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für die Audioumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Client-USB-Geräteumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Umleitung von USB-Geräten zum und vom Client in Kilobit pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für Client-USB-Geräteumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Umleitung von USB-Geräten zum und vom Client als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Client-USB-Geräteumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Zwischenablagenumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde für Datenübertragungen zwischen einer Sitzung und der lokalen Zwischenablage an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Zwischenablagenumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für Zwischenablagenumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für Datenübertragungen zwischen einer Sitzung und der lokalen Zwischenablage als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Zwischenablagenumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für COM-Portumleitung

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf einen COM-Port in einer Clientverbindung in Kilobits pro Sekunde an. Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für COM-Portumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für COM-Portumleitung (Prozent)

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf COM-Ports in einer Clientverbindung als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für COM-Portumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Dateiumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientlaufwerke in einer Clientverbindung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung einen Wert angeben und auch für die Einstellung Bandbreitenlimit für Dateiumleitung (Prozent), wird die restriktivere Einstellung (mit dem niedrigeren Wert) angewendet.

Bandbreitenlimit für Dateiumleitung (Prozent)

Mit dieser Einstellung geben Sie das maximal zulässige Bandbreitenlimit für den Zugriff auf Clientlaufwerke als Prozentsatz der Gesamtsitzungsbandbreite an

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Dateiumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Bereitstellung von Streamingaudio und -video mit HDX MediaStream-Multimediabeschleunigung in Kilobit pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung einen Wert angeben und auch für die Einstellung Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent), wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Bereitstellung von Streamingaudio und -video mit HDX MediaStream-Multimediabeschleunigung als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung "Bandbreitenlimit für HDX MediaStream-Multimediabeschleunigung"einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für LPT-Portumleitung

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde an, die für Druckaufträge über den LPT-Port in einer Benutzersitzung verwendet werden kann.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für LPT-Portumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für LPT-Portumleitung (Prozent)

Hinweis: Konfigurieren Sie bei Virtual Delivery Agent 7.0 bis 7.8 diese Einstellung über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung).

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite, die für Druckaufträge über den LPT-Port in einer Sitzung verwendet werden darf, als Prozent der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und auch für die Einstellung Bandbreitenlimit für LPT-Portumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für Sitzung insgesamt

Mit dieser Einstellung geben Sie Gesamtbandbreite in Kilobits pro Sekunde an, die für Benutzersitzungen verwendet werden kann.

Die maximal erzwingbare Bandbreitenbeschränkung ist 10 MBit/s (10.000 KBit/s). Standardmäßig ist kein Maximalwert (Null) angegeben.

Durch Beschränken der Bandbreite, die von einer Clientverbindung verbraucht wird, kann zu einer Leistungsverbesserung führen, wenn andere Anwendungen außerhalb der Clientverbindung auch auf die Bandbreite zugreifen.

Bandbreitenlimit für Druckerumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientdrucker in einer Benutzersitzung in Kilobits pro Sekunde an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Druckerumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für Druckerumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für den Zugriff auf Clientdrucker als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für Druckerumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Bandbreitenlimit für TWAIN-Geräteumleitung

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite in Kilobits pro Sekunde für die Steuerung von TWAIN-Bildverarbeitungsgeräten in veröffentlichten Anwendungen an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent) einen Wert angeben, wird die restriktivere Einstellung angewendet.

Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)

Mit dieser Einstellung geben Sie die maximal zulässige Bandbreite für die Steuerung von TWAIN-Bildverarbeitungsgeräten in veröffentlichten Anwendungen als Prozentsatz der Gesamtsitzungsbandbreite an.

Standardmäßig ist kein Maximalwert (Null) angegeben.

Wenn Sie für diese Einstellung und für die Einstellung Bandbreitenlimit für TWAIN-Geräteumleitung einen Wert angeben, wird die restriktivere Einstellung angewendet.

Wenn Sie die Einstellung konfigurieren, müssen Sie auch die Einstellung Bandbreitenlimit für Sitzung insgesamt konfigurieren, mit der die Gesamtbandbreite definiert wird, die für Clientsitzungen verfügbar ist.

Richtlinieneinstellungen für die bidirektionale Inhaltsumleitung

Bidirektionale Inhaltsumleitung zulassen

Legen Sie diese Richtlinie auf **Zugelassen** fest, um die Umleitung zwischen Server (VDA) und Client zu ermöglichen. Die Standardeinstellung ist **Nicht zugelassen**.

Verwenden Sie die Richtlinie **Für Umleitung an Client zulässige URLs**, um die Liste der URLs für die VDA-zu-Client-Umleitung zu konfigurieren.

> **Hinweis:**
>
> Diese Richtlinie muss mit der Richtlinie **Bidirektionale Inhaltsumleitung** auf dem Client festgelegt werden, damit die Umleitung zulässig ist.

Für Umleitung an Client zulässige URLs

Gibt die Liste der URLs an, die auf dem Client geöffnet werden, wenn eine bidirektionale Inhaltsumleitung zulässig ist.

Ein Semikolon (;) ist das Trennzeichen. Ein Sternchen (*) kann als Platzhalter verwendet werden. Beispiel:

```
*.xyz.com;https://www.example.com
```


Einstellungen der Richtlinie "Clientsensoren"

February 22, 2019

Der Abschnitt "Clientsensoren" enthält Richtlinieneinstellungen, mit denen gesteuert wird, wie Informationen über den Mobilgerätsensor in einer Benutzersitzung gehandhabt werden.

Anwendungen können den physischen Standort des Clientgeräts verwenden

Diese Einstellung legt fest, ob Anwendungen, die in einer Sitzung auf einem Mobilgerät ausgeführt werden, den physischen Standort des Benutzergeräts verwenden können.

In der Standardeinstellung ist die Verwendung von Standortinformationen nicht zugelassen.

Wenn diese Einstellung nicht zugelassen ist und eine Anwendung versucht, die Standortinformationen abzurufen, wird ein Wert von "Zugriff verweigert" zurückgegeben.

Wenn diese Einstellung nicht zugelassen ist, kann ein Benutzer die Verwendung von Standortinformationen verhindern und eine Citrix Receiver-Anforderung für den Zugriff auf den Standort ablehnen. Android- und iOS-Geräte senden am Anfang jeder Sitzung eine Anforderung für die Standortinformationen.

Berücksichtigen Sie beim Entwickeln von gehosteten Anwendungen, die die Einstellung "Anwendungen können den physischen Standort des Clientgeräts verwenden" enthalten, Folgendes:

- Eine standortaktivierte Anwendung sollte sich aus den folgenden Gründen nicht darauf verlassen, dass Standortinformationen verfügbar sind:
  - Ein Benutzer gewährt möglicherweise keinen Zugriff auf die Standortinformationen.
  - Der Standort ist ggf. nicht verfügbar oder ändert sich, währen die Anwendung ausgeführt wird.
  - Ein Benutzer stellt möglicherweise eine Verbindung mit der Anwendungssitzung von einem anderen Gerät her, das keine Standortinformationen unterstützt.
- Anforderungen für eine standortaktivierte Anwendung:
  - Das Standortfeature muss in der Standardeinstellung deaktiviert sein.
  - Eine Benutzeroption für das Zulassen oder Ablehnen des Features muss bei Ausführung der Anwendung verfügbar sein.
  - Eine Benutzeroption muss verfügbar sein, mit der von der Anwendung zwischengespeicherte Standortdaten gelöscht werden. (Citrix Receiver speichert keine Standortdaten im Cache.)

- Eine standortaktivierte Anwendung muss die Granularität der Standortinformationen verwalten, damit die abgefragten Daten dem Zweck der Anwendung entsprechen und die entsprechenden Gesetze einhalten.
- Bei der Verwendung der Standortdienste sollte eine sichere Verbindung (zum Beispiel mit TLS oder einem VPN) erzwungen werden. Citrix Receiver sollte eine Verbindung mit vertrauenswürdigen Servern herstellen.
- Sie sollten eine Rechtsberatung hinsichtlich der Verwendung von Standortdiensten erwägen.

Einstellungen der Richtlinie "Desktopbenutzeroberfläche"

November 29, 2018

Der Abschnitt "Desktopbenutzeroberfläche"enthält Richtlinieneinstellungen für visuelle Effekte, wie Desktophintergrund, Menüanimationen und das Verhalten von Fensterinhalten beim Drag & Drop, um die für Clientverbindungen verbrauchte Bandbreite zu steuern. Die Anwendungsleistung über ein WAN lässt sich durch Beschränken des Bandbreitenverbrauchs verbessern.

Desktopgestaltungsumleitung

Mit dieser Einstellung geben Sie an, ob die Verarbeitung des Grafikprozessors (GPU) oder des integrierten Grafikprozessors (IGP) auf dem Benutzergerät für die lokale DirectX-Grafikwiedergabe verwendet werden soll, um eine nahtlosere Windows-Desktopdarstellung zu erzielen. Wenn die Desktopgestaltungsumleitung aktiviert ist, wird eine hoch reaktionsfähige Windows-Benutzererfahrung bei Beibehaltung einer hohen Skalierbarkeit auf dem Server gewährleistet.

Standardmäßig ist die Desktopgestaltungsumleitung deaktiviert.

Um die Desktopgestaltungsumleitung auszuschalten und die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, wählen Sie Deaktiviert aus, wenn Sie diese Einstellung einer Richtlinie hinzufügen.

Grafikqualität Desktopgestaltung

Mit dieser Einstellung wird die Qualität der für die Desktopgestaltungsumleitung verwendeten Grafiken angegeben.

Die Standardeinstellung ist "Hoch".

Wählen Sie die Qualität Hoch, Mittel, Niedrig oder Verlustfrei aus.

Desktophintergrund

Mit dieser Einstellung legen Sie fest, ob Hintergründe in Benutzersitzungen angezeigt werden.

Standardmäßig kann der Desktophintergrund in Benutzersitzungen angezeigt werden.

Um den Desktophintergrund auszuschalten und die für Benutzersitzungen erforderliche Bandbreite zu reduzieren, wählen Sie die Einstellung Nicht zugelassen, wenn Sie diese Einstellung einer Richtlinie hinzufügen.

Menüanimation

Mit dieser Einstellung legen Sie fest, ob Menüanimation in Benutzersitzungen zugelassen oder verhindert wird.

Standardmäßig ist Menüanimation zugelassen.

Menüanimation ist eine Microsoft-Einstellung für erleichterte Bedienung. Ist die Einstellung aktiviert, werden Menüs nach einer kurzen Verzögerung durch Bildlauf- oder Einblendeffekt angezeigt. Unten im Menü wird ein Pfeil angezeigt. Das Menü wird eingeblendet, wenn Sie mit der Maus auf diesen Pfeil zeigen.

Menüanimation ist auf einem Desktop aktiviert, wenn diese Richtlinieneinstellung auf Zugelassen festgelegt ist und die Microsoft-Einstellung für Menüanimation aktiviert ist.

Hinweis: Änderungen an der Microsoft-Einstellung für Menüanimation sind Desktopänderungen. Dies bedeutet, dass einem Benutzer, der Menüanimation in einer Sitzung aktiviert hat, in späteren Sitzungen auf dem Desktop keine Menüanimation zur Verfügung steht, wenn die Desktopeinstellungen so festgelegt sind, dass am Desktop vorgenommene Änderungen nach dem Beenden der Sitzung verworfen werden. Aktivieren Sie daher für Benutzer, die Menüanimation benötigen, die Microsoft-Einstellung im Masterimage für den Desktop oder stellen Sie sicher, dass der Desktop vom Benutzer vorgenommene Änderungen beibehält.

Fensterinhalt beim Verschieben anzeigen

Mit dieser Einstellung legen Sie fest, ob Fensterinhalte beim Verschieben des Fensters auf dem Bildschirm angezeigt werden.

Standardmäßig ist die Anzeige des Fensterinhalts beim Verschieben zugelassen.

Wenn Zugelassen ausgewählt ist, wird beim Verschieben das ganze Fenster angezeigt. Wenn Nicht zugelassen ausgewählt ist, wird bis zum Ablegen nur der Fensterrahmen beim Verschieben angezeigt.

Einstellungen der Richtlinie “Endbenutzerüberwachung”

November 29, 2018

Der Abschnitt “Endbenutzerüberwachung”enthält Richtlinien zum Messen von Sitzungsnetzwerkverkehr.

ICA-Roundtripberechnung

Mit dieser Einstellung legen Sie fest, ob ICA-Roundtripberechnungen für aktive Verbindungen durchgeführt werden.

Standardmäßig sind die Berechnungen für aktive Verbindungen aktiviert.

Standardmäßig wird die Initiierung des ICA-Roundtripmessung verzögert, bis Netzwerkverkehr auf eine Benutzeraktion hinweist. Diese Verzögerung kann eine unbestimmte Länge haben und verhindert, dass die ICA-Roundtripmessung der einzige Grund für den ICA-Verkehr ist

Intervall für ICA-Roundtripberechnung

Mit dieser Einstellung geben Sie die Häufigkeit an, in Sekunden, mit der ICA-Roundtripberechnungen durchgeführt werden

Standardmäßig wird der ICA-Roundtrip alle 15 Sekunden berechnet.

ICA-Roundtrip für Verbindungen im Leerlauf berechnen

Mit dieser Einstellung legen Sie fest, ob ICA-Roundtripberechnungen für Verbindungen im Leerlauf durchgeführt werden.

Standardmäßig werden Berechnungen nicht für Verbindungen im Leerlauf durchgeführt.

Standardmäßig wird die Initiierung des ICA-Roundtripmessung verzögert, bis Netzwerkverkehr auf eine Benutzeraktion hinweist. Diese Verzögerung kann eine unbestimmte Länge haben und verhindert, dass die ICA-Roundtripmessung der einzige Grund für den ICA-Verkehr ist

Richtlinieneinstellung für Enhanced Desktop Experience

November 29, 2018

Durch die Richtlinieneinstellung "Enhanced Desktop Experience"werden Sitzungen auf Serverbetriebssystemen so konfiguriert, dass sie wie lokale Windows 7-Desktops aussehen, damit Benutzer in den Genuss einer verbesserten Desktopdarstellung kommen.

Standardmäßig ist diese Einstellung auf Zugelassen festgelegt.

Wenn ein Benutzerprofil mit dem Design "Windows –klassisch"bereits auf dem virtuellen Desktop vorhanden ist, wird durch Aktivieren dieser Richtlinie nicht die verbesserte Desktopdarstellung für diesen Benutzer bereitgestellt. Wenn sich ein Benutzer, dessen Benutzerprofil mit einem Windows 7-Design konfiguriert ist, bei einem virtuellen Desktop unter Windows Server 2012 anmeldet, für den diese Richtlinie deaktiviert oder nicht konfiguriert ist, wird eine Fehlermeldung angezeigt, die angibt, dass das Design nicht angewendet werden kann.

In beiden Fällen kann das Problem durch Zurücksetzen des Benutzerprofils gelöst werden.

Wenn die Richtlinie auf einem virtuellen Desktop mit aktiven Benutzersitzungen deaktiviert wird, sind Aussehen und Verhalten von Sitzungen nicht mit der Desktopdarstellung von Windows 7 und Windows - klassisch konsistent. Wenn Sie dies vermeiden möchten, starten Sie den virtuellen Desktop neu, nachdem Sie die Richtlinieneinstellung geändert haben. Sie müssen auch sämtliche Roamingprofile auf dem virtuellen Desktop löschen. Citrix empfiehlt außerdem, alle anderen Benutzerprofile auf dem virtuellen Desktop zu löschen, um Inkonsistenzen zwischen Profilen zu vermeiden.

Wenn Sie Roamingbenutzerprofile in der Umgebung verwenden, stellen Sie sicher, dass das Feature "Enhanced Desktop Experience"für alle virtuellen Desktops, die sich ein Profil teilen, entweder aktiviert oder deaktiviert ist.

Citrix rät davon ab, Roamingprofile zwischen virtuellen Desktops, auf denen Serverbetriebssysteme und Clientbetriebssysteme ausgeführt werden, freizugeben. Die Profile für Client- und Serverbetriebssysteme sind unterschiedlich und das Freigeben von Roamingprofilen zwischen beiden Systemtypen kann zu Inkonsistenzen in den Profileigenschaften führen, wenn ein Benutzer zwischen den Systemen wechselt.

Einstellungen der Richtlinie "Dateiumleitung"

November 29, 2018

Der Abschnitt "Dateiumleitung"enthält Richtlinieneinstellungen für die Clientlaufwerkzuordnung und die Clientlaufwerkoptimierung.

Clientlaufwerke automatisch verbinden

Mit dieser Einstellung legen Sie fest, ob die automatische Verbindung von Clientlaufwerken bei der Benutzeranmeldung zugelassen ist.

In der Standardeinstellung ist die automatische Verbindung zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie die Einstellungen für die Laufwerktypen aktivieren, die automatisch verbunden werden. Konfigurieren Sie beispielsweise Optische Clientlaufwerke, damit CD-Laufwerke auf dem Clientgerät automatisch verbunden werden.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Clientlaufwerkumleitung
- Clientdiskettenlaufwerke
- Optische Clientlaufwerke
- Lokale Clientfestplattenlaufwerke
- Clientnetzlaufwerke
- Clientwechsellaufwerke

Clientlaufwerkumleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Dateiumleitung von und zu Laufwerken auf dem Benutzergerät.

In der Standardeinstellung ist die Dateiumleitung aktiviert.

Wenn aktiviert, können Benutzer ihre Dateien auf allen Clientlaufwerken speichern. Wenn deaktiviert, wird jegliche Dateiumleitung verhindert, unabhängig von den Dateiumleitungseinstellungen für einzelne Laufwerkstypen, z. B. Clientdiskettenlaufwerke und Clientnetzlaufwerke.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Clientdiskettenlaufwerke
- Optische Clientlaufwerke
- Lokale Clientfestplattenlaufwerke
- Clientnetzlaufwerke
- Clientwechsellaufwerke

Lokale Clientfestplattenlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die lokalen Festplattenlaufwerke des Benutzergeräts zugreifen oder Dateien darauf speichern können.

In der Standardeinstellung ist der Zugriff auf lokale Festplattenlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können lokale Festplattenlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen –unabhängig von der Einstellung für Lokale Festplattenlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit lokale Festplattenlaufwerke automatisch verbunden werden.

Clientdiskettenlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die Diskettenlaufwerke des Benutzergeräts zugreifen oder Dateien darauf speichern können.

In der Standardeinstellung ist der Zugriff auf Diskettenlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Diskettenlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen –unabhängig von der Einstellung für Clientdiskettenlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Diskettenlaufwerke automatisch verbunden werden.

Clientnetzlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die (remoten) Netzlaufwerke des Benutzergeräts zugreifen oder Dateien speichern können.

In der Standardeinstellung ist der Zugriff auf Netzlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Netzlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen –unabhängig von der Einstellung für Clientnetzlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Netzlaufwerke automatisch verbunden werden.

Optische Clientlaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf CD-, DVD- und BD-Laufwerke des Clientgeräts zugreifen oder Dateien dort speichern können.

In der Standardeinstellung ist der Zugriff auf optische Clientlaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können optische Clientlaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen –unabhängig von der Einstellung für Optische Clientlaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit optische Clientlaufwerke automatisch verbunden werden.

Clientwechsellaufwerke

Mit dieser Einstellung legen Sie fest, ob Benutzer auf die USB-Laufwerke des Benutzergeräts zugreifen oder Dateien speichern können.

In der Standardeinstellung ist der Zugriff auf Clientwechsellaufwerke zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellungen deaktiviert sind, können Clientwechsellaufwerke nicht zugeordnet werden und Benutzer können auch nicht manuell auf diese Laufwerke zugreifen –unabhängig von der Einstellung für Clientwechsellaufwerke.

Konfigurieren Sie außerdem die Einstellung Clientlaufwerke automatisch verbinden, damit Clientwechsellaufwerke automatisch verbunden werden.

Host-zu-Client-Umleitung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Dateitypzuordnungen für URLs und manche Medieninhalte, damit sie auf dem Clientgerät geöffnet werden. Wenn deaktiviert, werden Inhalte auf dem Server geöffnet.

In der Standardeinstellung ist die Dateitypzuordnung deaktiviert.

Diese Art von URLs werden lokal geöffnet, wenn Sie die Einstellung aktivieren:

- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Real Player und QuickTime (RTSP)
- Real Player und QuickTime (RTSPU)
- Ältere Real Player-URLs (PNM)
- Microsoft Media Server (MMS)

Clientlaufwerksbuchstaben erhalten

Mit dieser Einstellung aktivieren oder deaktivieren Sie, ob die Clientlaufwerksbuchstaben erhalten bleiben.

In der Standardeinstellung bleiben die Clientlaufwerksbuchstaben nicht erhalten.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen.

Schreibgeschützter Zugriff auf Clientlaufwerke

Diese Einstellung erlaubt oder verhindert, dass Benutzer und Anwendungen Dateien oder Ordner auf zugeordneten Clientlaufwerken erstellen oder ändern.

Standardmäßig können Dateien und Ordner auf zugeordneten Clientlaufwerken geändert werden.

Wenn die Einstellung auf Aktiviert gesetzt wird, ist Lesezugriff auf die Dateien und Verzeichnisse möglich.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen.

Umleitung spezieller Ordner

Mit dieser Einstellung legen Sie fest, ob Benutzer von Citrix Receiver und dem Webinterface ihre lokalen speziellen Ordner in einer Sitzung sehen, z. B. "Dokumente"und "Desktop".

In der Standardeinstellung ist die Umleitung spezieller Ordner zugelassen.

Diese Einstellung verhindert, dass jegliche Objekte, die durch eine Richtlinie gefiltert werden, die Umleitung spezieller Ordner verwenden. Einstellungen an anderer Stelle werden nicht beachtet. Wenn diese Einstellung nicht zugelassen ist, werden verwandte Einstellungen im Webinterface, in StoreFront oder Citrix Receiver ignoriert.

Sie legen fest, welche Benutzer die Umleitung spezieller Ordner erhalten, indem Sie Zugelassen wählen und diese Einstellung in eine Richtlinie aufnehmen, die nach den Benutzern gefiltert wird, denen diese Funktion zur Verfügung stehen soll. Diese Einstellung überschreibt alle anderen Einstellungen für die Umleitung spezieller Ordner.

Die Umleitung spezieller Ordner interagiert mit dem Clientgerät. Daher verhindern Einstellungen, die den Benutzerzugriff auf lokale Festplatten untersagen, auch die Umleitung spezieller Ordner.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Lokale Clientfestplattenlaufwerke die Option Zugelassen wählen.

Asynchrones Schreiben verwenden

Mit dieser Einstellung aktivieren oder deaktivieren Sie asynchrones Schreiben auf Laufwerke.

Standardmäßig ist das asynchrone Schreiben deaktiviert.

Für Verbindungen über WANs, die normalerweise durch relativ hohe Bandbreite und hohe Latenz charakterisiert sind, können Sie durch asynchrone Schreibvorgänge die Dateiübertragungen und Schreibvorgänge auf Clientlaufwerke beschleunigen. Sollte jedoch ein Verbindungsfehler oder Datenträgerfehler auftreten, können die Clientdateien, die geschrieben werden, in einem nicht definierten Zustand enden. Dem Benutzer werden dann in einem Popupfenster die betroffenen Dateien angezeigt. Der Benutzer kann das Problem beheben, z. B. durch Neustart einer unterbrochenen Dateiübertragung bei der Wiederverbindung oder nach Beheben eines Datenträgerfehlers.

Citrix empfiehlt, dass asynchrone Schreibvorgänge auf Datenträgern nur für Benutzer implementiert werden, die eine Remoteverbindung mit guter Geschwindigkeit für die Dateiübertragungen benötigen, und die verlorene Dateien oder Daten problemlos wiederherstellen können, sollten Fehler bei der Verbindung oder dem Datenträger auftreten.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, müssen Sie auch für die Einstellung Clientlaufwerkumleitung die Option Zugelassen wählen. Wenn diese Einstellung deaktiviert ist, finden keine asynchronen Schreibvorgänge statt.

Einstellungen der Richtlinie “Flash-Umleitung”

August 18, 2021

Der Abschnitt “Flash-Umleitung”enthält Richtlinieneinstellungen für die Behandlung von Flash-Inhalten in Benutzersitzungen.

Flash-Beschleunigung

Aktiviert oder deaktiviert die Wiedergabe von Flash-Inhalten auf Benutzergeräten statt auf dem Server. Standardmäßig ist die clientseitige Wiedergabe von Flash-Inhalten aktiviert.

Hinweis: Diese Einstellung wird für die Legacy-Flash-Umleitung mit dem Citrix Online Plug-In 12.1 verwendet.

Wenn aktiviert, reduziert diese Einstellung die Netzwerk- und Serverlast, indem Flash-Inhalte auf dem Clientgerät wiedergegeben werden. Zusätzlich erreichen Sie mit der Einstellung Flash-URL-Kompatibilitätsliste, dass Flash-Inhalte von bestimmten Websites auf dem Server wiedergegeben werden.

Auf dem Benutzergerät muss die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren auch aktiviert sein.

Ist diese Einstellung deaktiviert, werden Flash-Inhalte von allen Websites, unabhängig von deren URLs, auf dem Server wiedergegeben. Damit nur die Flash-Inhalte bestimmter Websites auf dem Benutzergerät wiedergeben werden, konfigurieren Sie die Einstellung Flash-URL-Kompatibilitätsliste.

Flash-Hintergrundfarbenliste

Mit dieser Einstellung können Sie Schlüsselfarben für bestimmte URLs festlegen.

In der Standardeinstellung sind keine Schlüsselfarben angegeben.

Schlüsselfarben werden hinter clientseitig wiedergegebenem Flash angezeigt und unterstützen die visuelle Erkennung von Bereichen. Die angegebene Schlüsselfarbe sollte selten sein, sonst funktioniert die visuelle Bereichserkennung ggf. nicht richtig.

Gültige Eingaben bestehen aus einer URL (mit optionalen Platzhaltern am Anfang und Ende), der ein 24-Bit-RGB-Farbhexcode folgt. Beispiel: `https://citrix.com 000003`.

Stellen Sie sicher, dass die angegebene URL die URL für den Flash-Inhalt ist. Sie weicht möglicherweise von der URL der Website ab.

> **Warnung**
>
> Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Auf VDA-Maschinen, auf denen Windows 8 oder Windows 2012 ausgeführt wird, werden mit dieser Einstellung möglicherweise nicht die Schlüsselfarben für die URL festgelegt. Wenn dieses Problem auftritt, bearbeiten Sie die Registrierung auf der VDA-Maschine.

Verwenden Sie bei 32-Bit-Maschinen die folgende Registrierungseinstellung:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] “ForceHDXFlashEnabled”=dword:00000001

Verwenden Sie bei 64-Bit-Maschinen die folgende Registrierungseinstellung:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] “ForceHDXFlashEnabled”=dword:00000001

Flash-Abwärtskompatibilität

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung von Originalfeatures für die Legacy-Flash-Umleitung mit älteren Versionen von Citrix Receiver (früher Citrix Online Plug-In).

Standardmäßig ist diese Einstellung aktiviert.

Auf dem Benutzergerät muss die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren auch aktiviert sein.

Flash-Umleitungsfeatures der zweiten Generation können mit Citrix Receiver 3.0 verwendet werden. Legacyumleitungsfeatures werden mit dem Citrix Online Plug-In 12.1 unterstützt. Um sicherzustellen, dass die Flash-Umleitungsfeatures der zweiten Generation verwendet werden, muss die Flash-Umleitung der zweiten Generation auf dem Server und dem Benutzergerät aktiviert sein. Wenn die Legacyumleitung entweder auf dem Server oder dem Benutzergerät aktiviert ist, werden die Legacyumleitungsfeatures verwendet.

Flash-Standardverhalten

Mit dieser Einstellung wird das Standardverhalten für die Flash-Beschleunigung der zweiten Generation festgelegt.

Standardmäßig ist die Flash-Beschleunigung aktiviert.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- Flash-Beschleunigung aktivieren: Flash-Umleitung wird verwendet.
- Flash Player blockieren: Flash-Umleitung sowie serverseitiges Rendering werden nicht verwendet. Der Benutzer kann keine Flash-Inhalte anzeigen.
- Flash-Beschleunigung deaktivieren: Flash-Umleitung wird nicht verwendet. Der Benutzer kann auf dem Server wiedergegebene Flash-Inhalte anzeigen, wenn ein mit den Inhalten kompatibler Adobe Flash Player für Windows Internet Explorer auf dem Server installiert ist.

Diese Einstellung kann für einzelne Webseiten und Flash-Instanzen basierend auf der Einstellung Flash-URL-Kompatibilitätsliste außer Kraft gesetzt werden. Außerdem muss auf dem Benutzergerät die Einstellung HDX MediaStream Flash-Umleitung auf dem Benutzergerät aktivieren aktiviert sein.

Flash-Ereignisprotokollierung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Aufzeichnung von Flash-Ereignissen im Windows-Anwendungsereignisprotokoll.

Standardmäßig ist die Protokollierung aktiviert.

Auf Computern unter Windows 7 oder Windows Vista wird ein spezielles Protokoll für die Flash-Umleitung im Knoten “Anwendungs- und Dienstprotokolle”angezeigt.

Flash - intelligentes Fallback

Mit dieser Einstellung aktivieren oder deaktivieren Sie automatische Versuche, das serverseitige Rendering für Flash Player-Instanzen zu verwenden, wenn das clientseitige Rendering entweder unnötig ist oder eine schlechte Benutzererfahrung ergibt.

Standardmäßig ist diese Einstellung aktiviert.

Flash-Latenzschwellenwert

Mit dieser Einstellung geben Sie einen Schwellenwert zwischen 0-30 Millisekunden an, um festzulegen, wo Adobe Flash-Inhalte wiedergegeben werden.

In der Standardeinstellung ist der Schwellenwert 30.

Beim Start wird die aktuelle Latenz zwischen Server und Benutzergerät von HDX MediaStream für Flash gemessen. Wenn die Latenz unter dem Schwellenwert liegt, werden Flash-Inhalte mit HDX MediaStream für Flash auf dem Benutzergerät wiedergegeben. Wenn die Latenz den Schwellenwert überschreitet, werden die Inhalte auf dem Netzwerkserver wiedergegeben, wenn Adobe Flash Player dort vorhanden ist.

Wenn Sie diese Einstellung aktivieren, muss die Einstellung Flash-Abwärtskompatibilität vorhanden und auf Zugelassen eingestellt sein.

Hinweis: Dies gilt nur, wenn HDX MediaStream Flash-Umleitung im Legacymodus verwendet wird.

Verhindern von Flash-Videofallback

Mit dieser Einstellung geben Sie an, ob und wie "kleine"Flash-Inhalte gerendert und angezeigt werden.

Standardmäßig ist diese Einstellung nicht konfiguriert.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- **Nur kleiner Inhalt:** Es werden nur Intelligentes-Fallback-Inhalte auf dem Server gerendert, andere Flash-Inhalte werden durch eine Fehler-SWF-Datei ersetzt.
- **Nur kleiner Inhalt mit einem unterstützten Client:** Es werden nur Intelligentes-Fallback-Inhalte auf dem Server gerendert, wenn der Client aktuell die Flash-Umleitung verwendet, andere Flash-Inhalte werden durch eine Fehler-SWF-Datei ersetzt.
- **Kein serverseitiger Inhalt:** Alle Inhalte auf dem Server werden durch eine Fehler-SWF-Dateiersetzt.

Zum Verwenden dieser Richtlinieneinstellung geben Sie eine Fehler-SWF-Datei an. Diese Fehler-SWF-Datei ersetzt alle Flash-Inhalte, die nicht auf dem VDA gerendert werden sollen.

Fehler beim Verhindern von Flash-Videofallback *.swf

Diese Einstellung legt die URL der Fehlermeldung fest, die anstelle von Flash-Instanzen angezeigt wird, wenn Server-Lastverwaltungsrichtlinien verwendet werden. Beispiel:

`http://domainName.tld/sample/path/error.swf`

URL-Liste für serverseitigen Flash-Inhaltsabruf

Mit dieser Einstellung geben Sie die Websites an, deren Flash-Inhalte auf den Server heruntergeladen und dann auf das Benutzergerät zur Wiedergabe übertragen werden.

In der Standardeinstellung sind keine Sites angegeben.

Diese Einstellung wird verwendet, wenn das Benutzergerät keinen direkten Internetzugang hat; der Server stellt die Verbindung bereit. Auf dem Benutzergerät muss die Einstellung Serverseitigen Inhaltsabruf aktivieren auch aktiviert sein.

Die Flash-Umleitung der zweiten Generation enthält ein Fallback für den serverseitigen Flash-Inhaltsabruf für SWF-Dateien. Wenn ein Benutzergerät Flash-Inhalte einer Website nicht abrufen kann und die Website in der URL-Liste für serverseitigen Flash-Inhaltsabruf aufgeführt ist, erfolgt der serverseitige Inhaltsabruf automatisch.

Hinzufügen von URLs zur Liste:

- Fügen Sie die URL der Flash-Anwendung und nicht die HTML-Seite auf oberster Ebene hinzu, die Flash Player initiiert.
- Verwenden Sie ein Sternchen (*) am Anfang oder am Ende der URL als Platzhalterzeichen.
- Verwenden Sie den Platzhalter am Ende, um alle untergeordneten URLs zuzulassen (`http://www.citrix.com/*`).
- Die Präfixe `http://` und `https://` werden verwendet (falls vorhanden), sind jedoch für gültige Listeneinträge nicht vorgeschrieben.

Flash-URL-Kompatibilitätsliste

Mit dieser Einstellung geben Sie die Regeln an, die festlegen, ob die Wiedergabe von Flash-Inhalten auf bestimmten Websites auf dem Benutzergerät oder auf dem Server erfolgt oder ob sie blockiert wird.

In der Standardeinstellung sind keine Regeln angegeben.

Hinzufügen von URLs zur Liste:

- Sortieren Sie die Liste nach Priorität, sodass die wichtigsten URLs, Aktionen und Wiedergabeorte ganz oben stehen.

- Verwenden Sie ein Sternchen (*) am Anfang oder am Ende der URL als Platzhalterzeichen.
- Verwenden Sie den Platzhalter am Ende, um auf alle untergeordneten URLs zu verweisen (`https://www.citrix.com/*`).
- Die Präfixe `http://` und `https://` werden verwendet (falls vorhanden), sind jedoch für gültige Listeneinträge nicht vorgeschrieben.
- Fügen Sie der Liste Websites hinzu, deren Flash-Inhalte nicht richtig auf dem Benutzergerät wiedergegeben werden, und wählen Sie entweder die Optionen Auf Server rendern oder Blockieren.

Einstellungen der Richtlinie "Grafiken"

August 18, 2021

Der Abschnitt "Grafiken"enthält Richtlinieneinstellungen, mit denen Sie steuern, wie Bilder in Benutzersitzungen behandelt werden.

Visuell verlustfreie Komprimierung zulassen

Mit dieser Einstellung wird für Grafiken visuell verlustfreie Komprimierung statt echter verlustfreier Komprimierung verwendet. Visuell verlustfreie Komprimierung steigert im Vergleich zu echter verlustfreier Komprimierung die Leistung, hat jedoch geringe Verluste, die für das Auge nicht erkennbar sind. Durch diese Einstellung ändert sich die Verwendung der Einstellungswerte für die visuelle Qualität.

Diese Einstellung ist standardmäßig deaktiviert.

Anzeigespeicherlimit

Mit dieser Einstellung geben Sie die maximale Größe des Videopuffers (in Kilobytes) für die Sitzung an.

Das Standardlimit für den Anzeigespeicher ist 65536 KB.

Gibt die maximale Größe des Videopuffers (in Kilobytes) für die Sitzung an. Geben Sie einen Wert zwischen 128 und 4.194.303 Kilobyte an. Der maximale Wert von 4.194.303 limitiert den Anzeigespeicher nicht. Das Standardlimit für den Anzeigespeicher ist 65536 KB. Verwenden einer größeren Farbtiefe und einer höheren Auflösung für Verbindungen erfordert mehr Speicher. Wird im Legacygrafikmodus das Speicherlimit erreicht, wird die Anzeige gemäß der Einstellung "Herabsetzungspräferenz für Anzeigemodus"herabgesetzt.

Für Verbindungen, die eine größere Farbtiefe und eine höhere Auflösung erfordern, erhöhen Sie den Grenzwert. Berechnen Sie den maximal erforderlichen Arbeitsspeicher mit dieser Formel:

Speicher in Byte = (Farbtiefe in Bits pro Pixel) / 8) * (vertikale Auflösung in Pixel) * (horizontale Auflösung in Pixel).

Beispiel: Bei einer Farbtiefe von 32, einer vertikalen Auflösung von 600 und einer horizontalen Auflösung von 800 ergibt dies einen maximal erforderlichen Arbeitsspeicher von (32 / 8) * (600) * (800) = 1920000 Byte, was ein Anzeigespeicherlimit von 1920 KB ergibt.

Andere Farbtiefen als 32 Bit sind nur verfügbar, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

HDX weist Benutzern nur den pro Sitzung erforderlichen Anzeigespeicher zu. Wenn also nur einige Benutzer mehr als den Standardspeicher benötigen, hat das Erhöhen des Anzeigespeicherlimits keine negativen Auswirkungen auf die Skalierbarkeit.

Herabsetzungspräferenz für Anzeigemodus

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Diese Einstellung gibt an, ob die Farbtiefe oder die Auflösung zuerst herabgesetzt werden soll, wenn das Speicherlimit für die Sitzung erreicht wird.

Standardmäßig wird die Farbtiefe zuerst herabgesetzt.

Wenn das Speicherlimit der Sitzung erreicht wird, können Sie die Bildqualität verringern, indem Sie erst die Farbtiefe oder erst die Auflösung herabsetzen. Wird erst die Farbtiefe herabgesetzt, werden Bilder mit weniger Farben dargestellt. Wird erst die Auflösung herabgesetzt, werden Bilder mit weniger Pixel pro Zoll angezeigt.

Wenn Benutzer in dem Fall benachrichtigt werden sollen, dass entweder die Farbtiefe oder die Auflösung herabgesetzt werden muss, konfigurieren Sie die Einstellung Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen.

Dynamische Fenstervorschau

Mit dieser Einstellung kann die Anzeige von Seamlessfenster in den Fenstervorschaumodi Flip, Flip 3D, Taskleistenvorschau und Einsehen aktiviert bzw. deaktiviert werden.

Windows Aero-Vorschauoption	Beschreibung
Symbolleistenvorschau	Wenn der Benutzer auf das Symbol eines Fensters zeigt, wird ein Bild dieses Fensters über der Symbolleiste angezeigt.
Fenstervorschau	Wenn der Benutzer auf ein Symbolleistenvorschaubild zeigt, wird das Bild in voller Größe auf dem Bildschirm angezeigt.
Flip	Wenn der Benutzer Alt + Tab drückt, werden kleine Vorschausymbole für jedes geöffnete Fenster angezeigt.
Flip-3D	Wenn der Benutzer die Tabulator- und Windows-Tasten drückt, werden große Bilder der geöffneten Fenster überlappend auf dem Bildschirm angezeigt.

Standardmäßig ist diese Einstellung aktiviert.

Bildzwischenspeicherung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Zwischenspeichern und Abrufen von Bildabschnitten in Sitzungen. Durch das Zwischenspeichern von Bildern in Abschnitten und das Abrufen dieser Abschnitte wird das Ruckeln beim Bildlauf verringert. Darüber hinaus werden weniger Daten über das Netzwerk übertragen und die Verarbeitung auf dem Benutzergerät wird reduziert.

Standardmäßig ist die Einstellung für die Bildzwischenspeicherung aktiviert.

Hinweis: Die Einstellung für die Bildzwischenspeicherung steuert, wie Bilder zwischengespeichert und abgerufen werden, jedoch nicht, ob sie zwischengespeichert werden. Wenn die Einstellung "Legacygrafikmodus"aktiviert ist, werden Bilder zwischengespeichert.

Legacygrafikmodus

Mit dieser Einstellung wird die umfassende Grafikdarstellung deaktiviert. Verwenden Sie diese Option, um den Legacygrafikmodus wiederherzustellen und den Bandbreitenverbrauch über ein WAN oder eine mobile Verbindung zu reduzieren. Mit der in XenApp und XenDesktop 7.13 eingeführten Bandbreitenverringerung ist dieser Modus nicht länger erforderlich.

Die Einstellung ist standardmäßig deaktiviert und die umfassende Grafikdarstellung wird verwendet.

Der Legacygrafikmodus wird für VDAs unter Windows 7 und Windows Server 2008 R2 unterstützt.

Der Legacygrafikmodus wird unter Windows 8.x, 10 oder Windows Server 2012, 2012 R2 und 2016 nicht unterstützt.

Weitere Informationen zum Optimieren von Grafikmodi und Richtlinien in XenApp und XenDesktop 7.6 FP3 oder später finden Sie in dem Knowledge Center-Artikel CTX202687.

Maximal zugelassene Farbtiefe

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung geben Sie die maximale Farbtiefe an, die für eine Sitzung zulässig ist.

Die Standardeinstellung für die maximal zulässige Farbtiefe ist 32 Bits pro Pixel.

Diese Einstellung gilt nur für Thinwire-Treiber und -Verbindungen. Sie gilt nicht für VDAs mit einem anderen Treiber als Thinwire für die primäre Anzeige, z. B. VDAs mit WDDM-Treiber (Windows Display Driver Model). Bei Desktopbetriebssystem-VDAs mit einem WDDM-Treiber als primären Anzeigetreiber, z. B. Windows 8, hat diese Einstellung keine Auswirkung. Bei Windows-Serverbetriebssystem-VDAs mit WDDM-Treiber, z. B. Windows Server 2012 R2, kann diese Einstellung verhindern, dass Benutzer eine Verbindung mit dem VDA herstellen.

Für eine hohe Farbtiefe ist mehr Speicher erforderlich. Damit die Farbtiefe herabgesetzt wird, wenn das Speicherlimit erreicht wurde, konfigurieren Sie die Einstellung Herabsetzungspräferenz für Anzeigemodus. Wird die Farbtiefe herabgesetzt, werden Bilder mit weniger Farben dargestellt.

Benutzer beim Herabsetzen des Anzeigemodus benachrichtigen

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung erzielen Sie, dass Benutzer eine kurze Erklärung erhalten, wenn die Farbtiefe oder die Auflösung herabgesetzt wird.

Standardmäßig werden Benutzer nicht benachrichtigt.

Warteschlange und Verwerfen

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung werden Bilder in der Warteschlange verworfen, die durch ein anderes Bild ersetzt wurden.

Standardmäßig ist diese Einstellung aktiviert.

Dies verbessert die Reaktionszeit, wenn Grafiken an das Benutzergerät gesendet werden. Wenn Sie diese Einstellung konfigurieren, ruckeln Animationen möglicherweise, weil Frames ausgelassen werden.

Verwenden von Videocodec für die Komprimierung

Ermöglicht die Verwendung eines Videocodecs (H.264) zum Komprimieren von Grafiken, wenn am Endpunkt eine Videodecodierung verfügbar ist. Bei Auswahl von **Für den gesamten Bildschirm** wird der Videocodec als Standardcodec für alles angewendet. Bei Auswahl von **Für aktive Änderungsbereiche** wird der Videocodec auf die Bereiche angewendet, in denen kontinuierliche Änderungen stattfinden. Für andere Daten werden weiterhin Bildkomprimierung und Bitmapcaching verwendet. Ist am Endpunkt keine Videodecodierung verfügbar oder wenn Sie festlegen, dass **kein Videocodec** verwendet werden soll, wird eine Kombination aus Standbildkomprimierung und Bitmapcaching verwendet. Wenn **Bevorzugt Videocodec verwenden** ausgewählt wird, trifft das System basierend auf verschiedenen Faktoren eine Auswahl. Die Ergebnisse variieren u. U. zwischen den Versionen, da die Auswahlmethode verbessert wird.

Wählen Sie **Bevorzugt Videocodec verwenden**, damit das System die geeignete Einstellung für das aktuelle Szenario wählt.

Wählen Sie **Für den gesamten Bildschirm**, um die Benutzererfahrung und Bandbreite zu optimieren, besonders bei viel auf dem Server wiedergegebenem Video und vielen 3D-Grafiken.

Wählen Sie **Für aktive Änderungsbereiche** zur Optimierung der Videoleistung –insbesondere bei Verbindungen mit geringer Bandbreite unter Beibehaltung der Skalierbarkeit für statischen und langsam veränderlichen Inhalt. Diese Einstellung wird in Bereitstellungen mit mehreren Monitoren unterstützt.

Wählen Sie **Videocodec nicht verwenden**, um die Server-CPU-Last zu optimieren und wenn nicht viel auf dem Server wiedergegebenes Video oder andere grafisch intensive Anwendungen verwendet werden.

Die Standardeinstellung ist **Bevorzugt Videocodec verwenden**.

Verwenden der Hardwarecodierung für Video

Diese Einstellung ermöglicht die Verwendung von Grafikhardware (falls verfügbar) zum Komprimieren von Bildschirmelemente mit dem Videocodec (H.264). Ist entsprechende Hardware nicht verfügbar, wird die CPU-basierte Codierung mit dem Software-Videocodec verwendet.

Die Standardeinstellung für diese Richtlinie ist **Aktiviert**.

Mehrere Monitore werden unterstützt.

Alle Citrix Receiver-Versionen, die H.264-Decodierung unterstützen, können mit NVENC-Hardwarecodierung verwendet werden.

Verlustreiche Komprimierung (4:2:0) und visuell verlustfreie Komprimierung (4:4:4) werden unterstützt. Die visuell verlustfreie Komprimierung (Grafikrichtlinieneinstellung Visuell verlustfreie Komprimierung zulassen) erfordert Receiver für Windows 4.5 oder später.

NVIDIA

Für NVIDIA GRID-GPUs wird die Hardwarecodierung von VDAs für Desktopbetriebssysteme im HDX 3D Pro-Modus unterstützt.

NVIDIA-GPUs müssen die NVENC-Hardwarecodierung unterstützen. Eine Liste der unterstützen GPUs finden Sie unter NVIDIA video codec SDK.

NVIDIA GRID erfordert einen Treiber ab Version 3.1. NVIDIA Quadro erfordert einen Treiber ab Version 362.56. Citrix empfiehlt Treiber der Kategorie NVIDIA Release R361.

Verlustfreier Text, ein VDA-Feature im Standardmodus (nicht HDX 3D Pro) ist nicht mit der NVENC-Hardwarecodierung kompatibel. Bei Aktivierung im HDX 3D Pro-Modus hat verlustfreier Text Vorrang vor der NVENC-Hardwarecodierung.

Die selektive Verwendung des H.264-Hardwarecodecs für aktiv veränderliche Bereiche wird nicht unterstützt.

Intel

Für Intel Iris Pro-Grafikprozessoren wird die Hardwarecodierung von VDAs für Desktopbetriebssysteme (im Standard- oder HDX 3D Pro-Modus) und von VDAs für Serverbetriebssysteme unterstützt.

Es werden Intel Iris Pro-Grafikprozessoren der Broadwell Intel-Prozessorfamilie und höher unterstützt. Version 1.0 des Intel Remote Displays-SDKs ist erforderlich. Es kann von der Intel-Website Remote Displays SDK heruntergeladen werden.

Verlustfreier Text wird unterstützt.

Die selektive Verwendung des H.264-Hardwarecodecs für aktiv veränderliche Bereiche wird unterstützt.

Unterstützt unter Windows 10 und Windows Server 2012 und höher.

Auf VDAs im 3D Pro-Modus bietet die Intel-Codierung eine gute Benutzererfahrung für bis zu acht Codierungssitzungen (z. B. wenn ein Benutzer acht Monitore verwendet oder acht Benutzer einen

Monitor). Sind über acht Codierungssitzungen erforderlich, prüfen Sie, mit wie vielen Monitoren die virtuelle Maschine eine Verbindung herstellt. Um eine gute Benutzererfahrung zu gewährleisten können Sie diese Richtlinieneinstellung für einzelne Benutzer oder Maschinen konfigurieren.

Einstellungen der Richtlinie "Zwischenspeichern"

April 4, 2019

Der Abschnitt "Zwischenspeichern"enthält Einstellungen, mit denen Bilddaten auf Benutzergeräten zwischengespeichert werden können, wenn Clientverbindungen eine beschränkte Bandbreite haben.

Schwellenwert für permanenten Cache

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung werden Bitmaps auf der Festplatte des Benutzergeräts zwischengespeichert. Dies ermöglicht eine Wiederverwendung von großen, oft verwendeten Bildern aus früheren Sitzungen.

Der Standardschwellenwert ist 3000000 Bits pro Sekunde.

Der Schwellenwert ist der Wert, unter dem das Feature "Permanentcache"angewendet wird. Beispielsweise werden mit dem Standardwert Bitmaps auf der Festplatte des Benutzergeräts zwischengespeichert, wenn die Bandbreite unter 3000000 Bit/s fällt.

Framehawk-Richtlinieneinstellungen

August 18, 2021

Der Abschnitt "Framehawk"enthält Richtlinieneinstellungen zum Aktivieren und Konfigurieren des Framehawk-Anzeigekanals auf dem Server.

Framehawk-Anzeigekanal

Wenn diese Option aktiviert ist, versucht der Server, den Framehawk-Anzeigekanal für die Grafiken und das Eingabe-Remoting der Benutzer zu verwenden. Bei diesem Anzeigekanal bietet durch UDP

eine bessere Benutzererfahrung in Netzwerken mit hohem Verlust und hoher Latenz, er verbraucht jedoch u. U. mehr Serverressourcen und Bandbreite als andere Grafikmodi.

Standardmäßig ist der Framehawk-Anzeigekanal deaktiviert.

Portbereich für Framehawk-Anzeigekanal

Mit dieser Richtlinieneinstellung geben Sie den Bereich der UDP-Portnummern an (im Format *niedrigste Portnummer,höchste Portnummer*), die vom VDA zum Austausch von Framehawk-Anzeigekanaldaten mit dem Benutzergerät verwendet werden. Der VDA versucht die Verwendung eines Ports, beginnend bei dem Port mit der niedrigsten Nummer und geht dann ggf. zu dem Port mit der nächsthöheren Nummer über. Über den Port erfolgen eingehende und ausgehende Datenübertragungen.

Der Standardportbereich ist 3224,3324.

Einstellungen der Richtlinie "Keep-Alive"

November 29, 2018

Der Abschnitt "Keep-Alive"enthält Richtlinieneinstellungen für die Verwaltung der ICA-Keep-Alive-Meldungen.

ICA-Keep-Alive - Timeout

Mit dieser Einstellung geben Sie die Anzahl der Sekunden zwischen aufeinanderfolgenden ICA-Keep-Alive-Meldungen an.

Das Standardintervall zwischen Keep-Alive-Meldungen ist 60 Sekunden.

Geben Sie ein Intervall zwischen 1-3600 Sekunden an, in dem ICA-Keep-Alive-Meldungen gesendet werden. Konfigurieren Sie diese Einstellung nicht, wenn Sie eine Netzwerküberwachungssoftware zum Schließen inaktiver Verbindungen verwenden.

ICA-Keep-Alives

Mit dieser Einstellung legen Sie fest, ob ICA-Keep-Alive-Meldungen in regelmäßigen Abständen gesendet werden sollen.

Standardmäßig werden keine Keep-Alive-Meldungen gesendet.

Wenn Sie diese Einstellung aktivieren, wird verhindert, dass unterbrochene Verbindungen getrennt werden. Wenn der Server keine Aktivität feststellt, verhindert diese Einstellung, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Der Server sendet alle paar Sekunden Keep-Alive-Meldungen, um zu ermitteln, ob die Sitzung aktiv ist. Wenn die Sitzung nicht mehr aktiv ist, wird die Sitzung vom Server als "Getrennt"gekennzeichnet.

ICA-Keep-Alive funktioniert nicht, wenn Sie die Sitzungszuverlässigkeit verwenden. Konfigurieren Sie daher ICA-Keep-Alive nur für Verbindungen, die die Sitzungszuverlässigkeit nicht verwenden.

Verwandte Richtlinieneinstellungen: Sitzungszuverlässigkeit - Verbindungen.

Einstellungen der Richtlinie "Lokaler App-Zugriff"

November 29, 2018

Der Abschnitt "Lokaler App-Zugriff"enthält Richtlinieneinstellungen, mit denen Sie die Integration lokal installierter Anwendungen mit gehosteten Anwendungen in einer gehosteten Desktopumgebung konfigurieren können.

Lokalen App-Zugriff zulassen

Mit dieser Einstellung legen Sie fest, ob die Integration lokal installierter Anwendungen mit gehosteten Anwendungen in einer gehosteten Desktopumgebung zugelassen oder verweigert werden soll.

Wenn ein Benutzer eine lokal installierte Anwendung startet, wirkt es so, als ob diese auf dem virtuellen Desktop des Benutzers ausgeführt würde, obwohl sie tatsächlich lokal ausgeführt wird.

Standardmäßig ist der lokale App-Zugriff nicht zulässig.

URL-Umleitungssperrliste

Mit dieser Einstellung geben Sie Websites an, die Ziel einer Weiterleitung sind und im lokalen Webbrowser gestartet werden sollen. Dies kann auch Websites umfassen, für die Gebietsschema-Informationen erforderlich sind (z. B. msn.com oder newsgoogle.com) oder Websites mit reichhaltigen Medieninhalten, die besser auf dem Benutzergerät wiedergegeben werden.

In der Standardeinstellung sind keine Sites angegeben.

URL-Umleitungspositivliste

Mit dieser Einstellung geben Sie die Websites an, die in der Umgebung, in der sie gestartet werden, wiedergegeben werden sollen.

In der Standardeinstellung sind keine Sites angegeben.

Einstellungen der Richtlinie "Mobilerfahrung"

November 29, 2018

Der Abschnitt "Mobilerfahrung"enthält Richtlinieneinstellungen für die Handhabung des Citrix Mobility Packs.

Automatische Anzeige der Tastatur

Diese Einstellung aktiviert oder deaktiviert die automatische Anzeige der Tastatur auf Bildschirmen von Mobilgeräten.

Standardmäßig ist die automatische Anzeige der Tastatur deaktiviert.

Für Fingereingabe optimierten Desktop starten

Diese Einstellung ist deaktiviert und für Maschinen mit Windows 10 oder Windows Server 2016 nicht verfügbar.

Diese Einstellung bestimmt das allgemeine Verhalten der Citrix Receiver-Benutzeroberfläche, indem sie eine für die Fingereingabe optimierte Benutzeroberfläche zulässt oder verweigert, die für Tablet-Geräte optimiert ist.

Standardmäßig wird eine für die Fingereingabe optimierte Benutzeroberfläche verwendet.

Setzen Sie diese Richtlinie auf "Nicht zugelassen", um nur die Windows-Benutzeroberfläche zu verwenden.

Kombinationsfelder remoten

Diese Einstellung bestimmt die Typen von Kombinationsfeldern, die in Sitzungen auf mobilen Geräten angezeigt werden können. Stellen Sie diese Richtlinie auf Zugelassen ein, um das gerätenative

Kombinationsfeld-Steuerelement anzuzeigen. Wenn diese Einstellung zugelassen ist, kann ein Benutzer eine Sitzungseinstellung in Citrix Receiver für iOS ändern und das Windows-Kombinationsfeld verwenden.

Standardmäßig wird die Funktion zum Remoten von Kombinationsfeldern verweigert.

Einstellungen der Richtlinie "Multimedia"

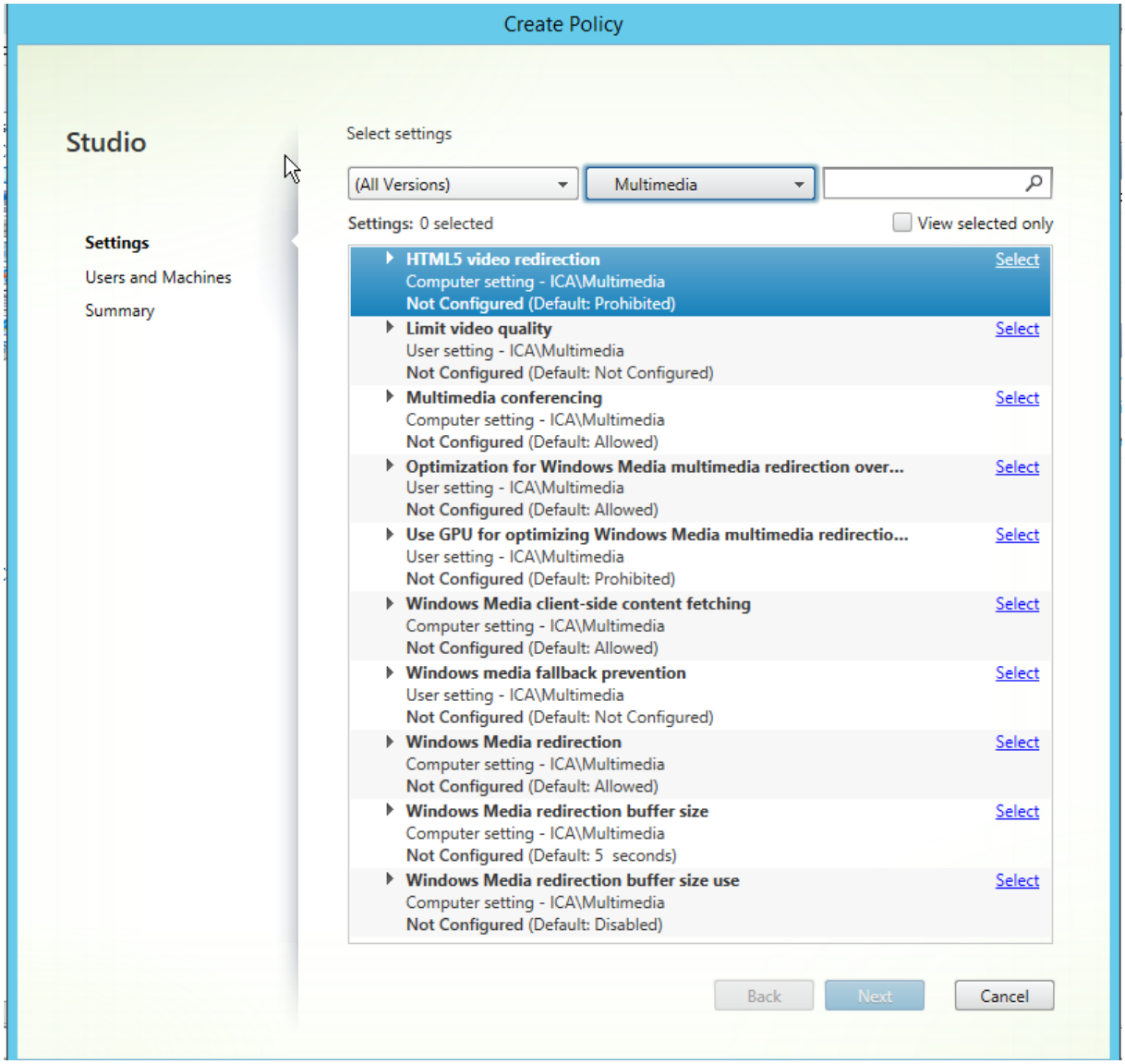
January 21, 2022

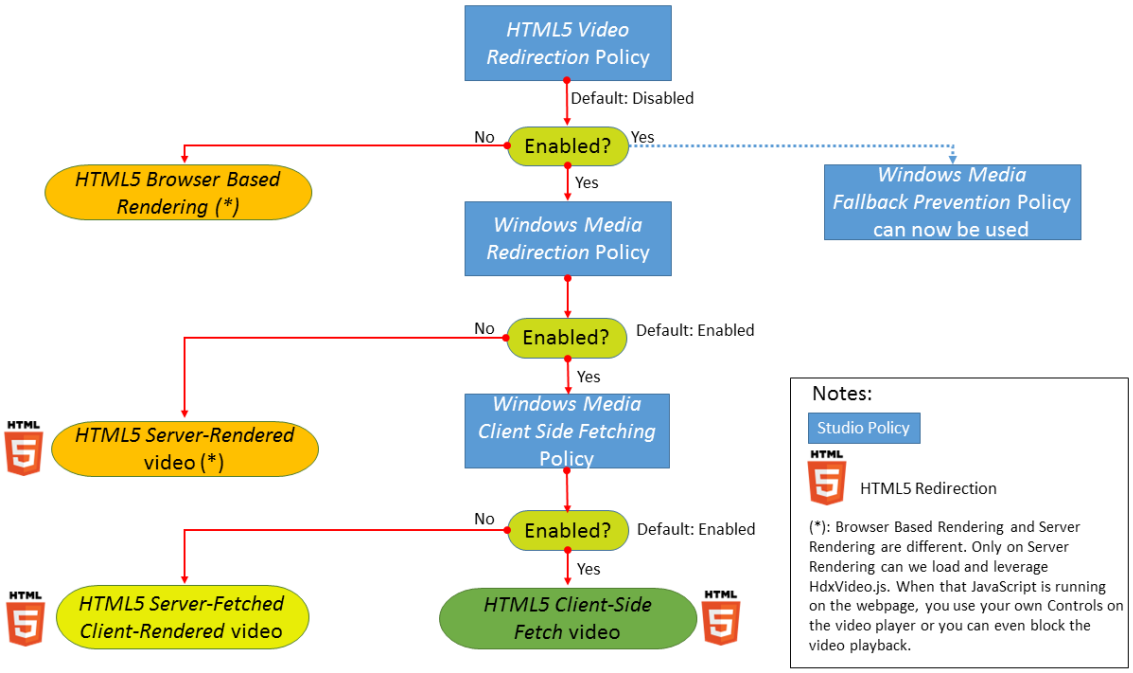
Der Abschnitt "Multimedia" enthält Richtlinieneinstellungen, mit denen Sie das Streaming von HTML5- und Windows-Audio- und Videoinhalten in Benutzersitzungen verwalten.

HTML5-Videoumleitung

Steuert und optimiert die Bereitstellung von HTML5-Multimediawebinhalten durch XenApp- und XenDesktop-Server.

Diese Einstellung ist standardmäßig deaktiviert.





In diesem Release ist dieses Feature nur für Websites verfügbar, die unter Ihrer Kontrolle stehen. Es erfordert das Hinzufügen von JavaScript zu den Webseiten mit HTML5-Multimediainhalten (z. B. Videos auf internen Schulungswebsites).

Konfigurieren der HTML5-Videoumleitung

1. Kopieren Sie die Datei **HdxVideo.js** aus der VDA-Installation unter %Program Files%/Citrix/ICA Service/HTML5 Video Redirection an den Speicherort Ihrer internen Webseite.
2. Fügen Sie folgende Zeile in Ihre Webseite ein (enthält diese weitere Skripts, fügen Sie **HdxVideo.js** davor ein):
   ```
   <script src="HdxVideo.js"type="text/javascript"></script>
   ```

Hinweis: Wenn HdxVideo.js nicht am gleichen Speicherort ist wie die Webseite, geben Sie über das Attribut **src** den vollständigen Pfad an.

Wenn den Webseiten kein JavaScript hinzugefügt wurde und ein Benutzer HTML5-Videos wiedergibt, wird in XenApp und XenDesktop standardmäßig die serverseitige Wiedergabe verwendet.

Lassen Sie Windows Media-Umleitung zu, damit die HTML5-Videoumleitung möglich ist. Diese Richtlinie ist für den serverseitigen Abruf und die clientseitige Wiedergabe obligatorisch und für den clientseitigen Abruf erforderlich (letzterer erfordert seinerseits das Zulassen von *Clientseitiger Inhaltsabruf von Windows Media)*.

Microsoft Edge unterstützt dieses Feature nicht.

HdxVideo.js ersetzt die HTML5-Steuerelemente des Browsers durch seine eigenen. Um zu überprüfen, ob die HTML5-Videoumleitungsrichtlinie auf eine Website angewendet wird, vergleichen Sie die

Player-Steuerelemente mit einem Szenario, in dem die Richtlinie ***HTML5-Videoumleitung*** nicht zugelassen ist:

(Benutzerdefinierte Citrix Steuerelemente bei Richtlinieneinstellung "Zugelassen")

(Native Webseitensteuerelemente bei Richtlinieneinstellung "Nicht zugelassen"bzw. wenn die Richtlinie nicht konfiguriert ist)

Die folgenden Video-Steuerelemente werden unterstützt:

- Wiedergabe
- Pause
- Suchen
- Wiederholen
- Audio
- Vollbild

Unter https://www.citrix.com/virtualization/hdx/html5-redirect.html finden Sie eine HTML5-Videoumleitungstestseite.

TLS- und HTML5-Videoumleitung

Sie können die HTML5-Videoumleitung verwenden, um HTTPS-Websites umzuleiten. Das in diese Websites eingefügte JavaScript muss eine TLS-Verbindung zum Citrix HDX HTML5-Videoumleitungsdienst (WebSocketService.exe) herstellen, der auf dem VDA ausgeführt wird. Zur Gewährleistung der TLS-Integrität der Webseite bei der Umleitung werden zwei benutzerdefinierte Zertifikate vom Citrix HDX HTML5-Videoumleitungsdienst im VDA-Zertifikatspeicher generiert.

HdxVideo.js kommuniziert über Secure Websockets mit dem auf dem VDA ausgeführten Dienst WebSocketService.exe. Diese Prozess wird im lokalen System für SSL-Beendigung und Benutzersitzungszuordnung ausgeführt.

WebSocketService.exe überwacht Port 9001 an 127.0.0.1.

Videoqualität beschränken

Diese Einstellung gilt nur für Windows Media und nicht für HTML5. Sie erfordert die *Optimierung von Windows Media-Multimediaumleitung über WAN*.

Mit dieser Einstellung geben Sie die maximale Videoqualitätsstufe für eine HDX-Verbindung an. Wird die Einstellung konfiguriert, dann wird die Videoqualität auf den angegebenen Wert beschränkt, sodass die Dienstqualität für Multimedia in der Umgebung gewährleistet ist.

Standardmäßig ist diese Einstellung nicht konfiguriert.

Zum Festlegen der maximalen Qualität wählen Sie eine der folgenden Optionen:

- 1080p/8,5 MBit/s
- 720p/4,0 MBit/s
- 480p/720 KBit/s
- 380p/400 KBit/s
- 240p/200 KBit/s

Die gleichzeitige Wiedergabe mehrerer Videos auf einem Server verbraucht viele Ressourcen und kann die Skalierbarkeit des Servers beeinträchtigen.

Multimediakonferenzen

Diese Einstellung ermöglicht oder verhindert das Verwenden einer optimierten Webcam-Umleitungstechnologie durch Videokonferenzanwendungen.

Standardmäßig ist die Unterstützung für Videokonferenzen zugelassen.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung Windows Medienumleitung vorhanden und auf Zugelassen (Standardeinstellung) gesetzt sein.

Für Multimediakonferenzen müssen folgende Bedingungen erfüllt sein:

- Der Gerätetreiber des Herstellers für die in der Multimediakonferenz verwendete Webcam ist installiert.
- Die Webcam wird mit dem Clientgerät verbunden, bevor eine Videokonferenzsitzung initiiert wird. Der Server verwendet zu jedem Zeitpunkt nur eine installierte Webcam. Wenn mehrere Webcams auf dem Benutzergerät installiert sind, versucht der Server nacheinander jede Webcam zu verwenden, bis eine Videokonferenzsitzung steht.

Diese Richtlinie wird nicht benötigt, wenn für die Webcam die generische USB-Umleitung verwendet wird. Installieren Sie in diesem Fall die Webcamtreiber auf dem VDA.

Optimierung von Windows Media-Multimediaumleitung über WAN

Diese Einstellung gilt nur für Windows Media und nicht für HTML5. Mit dieser Einstellung aktivieren Sie die Multimediatranscodierung in Echtzeit. Damit wird Audio- und Videostreaming für mobile Geräte

über problembehaftete Netzwerke ermöglicht und die Benutzererfahrung durch eine verbesserte Übermittlung von Windows Media-Inhalt über WAN optimiert.

Standardmäßig wird die Bereitstellung von Windows Media-Inhalt über das WAN optimiert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung **Windows Media-Umleitung** vorhanden und auf **Zugelassen** gesetzt sein.

Wenn diese Einstellung aktiviert ist, wird die Multimediatranscodierung nach Bedarf automatisch bereitgestellt, sodass Audio- und Videostreaming zur Verbesserung der Benutzererfahrung auch bei schlechten Netzwerkbedingungen ermöglicht wird.

GPU für die Optimierung von Windows Media-Multimediaumleitung über WAN verwenden

Mit dieser Einstellung, die nur für Windows Media gilt, wird die Transcodierung von Multimediainhalten in Echtzeit im Grafikprozessor (GPU) des Virtual Delivery Agent (VDA) ermöglicht. Sie verbessert die Serverskalierbarkeit. Die GPU-Transcodierung ist nur verfügbar, wenn der VDA eine unterstützte GPU für die Hardwarebeschleunigung hat. Andernfalls erfolgt die Transcodierung automatisch in der CPU.

Hinweis: GPU-Transcodierung wird nur von NVIDIA-GPUs unterstützt.

Standardmäßig ist die Verwendung der GPU auf dem VDA zum Optimieren der Bereitstellung von Windows Media-Inhalt über das WAN nicht zulässig.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, stellen Sie sicher, dass die Einstellungen Windows Media-Umleitung und Optimierung von Windows Media-Multimediaumleitung über WAN vorhanden und auf Zugelassen gesetzt sind.

Verhinderung von Fallback auf Windows Media

Diese Einstellung gilt für Windows Media und HTML5. Damit sie für HTML5 funktioniert, legen Sie die Richtlinie ***HTML-Videoumleitung*** auf **Zugelassen** fest.

Administratoren können über die Einstellung der Richtlinie "Verhinderung von Fallback auf Windows Media"die Methoden für die Übertragung gestreamter Inhalte an Benutzer steuern.

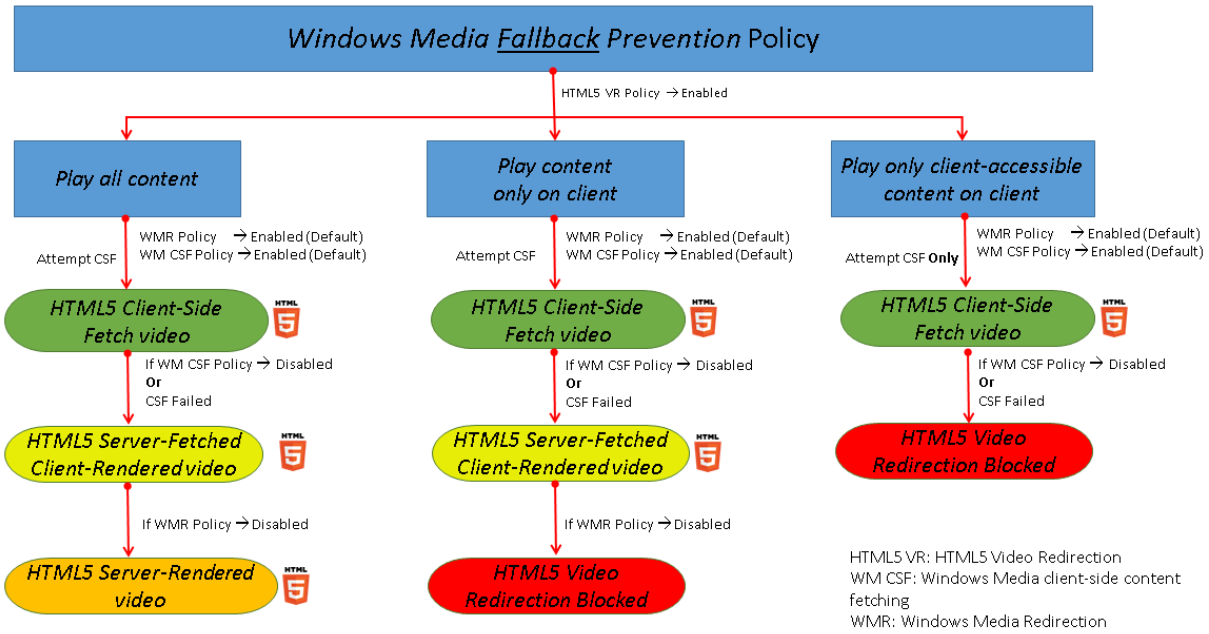
Standardmäßig ist diese Einstellung nicht konfiguriert. Wenn die Einstellung auf "Nicht konfiguriert" festgelegt ist, entspricht dies der Einstellung **Alle Inhalte wiedergeben**.

Wählen Sie für die Konfiguration dieser Einstellung eine der folgenden Optionen:

- **Alle Inhalte wiedergeben:** Versuch des clientseitigen Inhaltsabrufs und anschließende Windows Media-Umleitung. Gelingt dies nicht, wird der Inhalt auf dem Server wiedergegeben.

- **Alle Inhalte nur auf Client wiedergeben:** Versuch des clientseitigen Inhaltsabrufs und anschließende Windows Media-Umleitung. Gelingt dies nicht, wird der Inhalt nicht wiedergegeben.
- **Nur Inhalte auf Client wiedergeben, auf die Client Zugriff hat:** Nur clientseitiger Abruf. Gelingt dies nicht, wird der Inhalt nicht wiedergegeben.

Wird der Inhalt nicht wiedergegeben, wird im Playerfenster gemeldet, dass das Video wegen mangelnder Ressourcen blockiert wurde (Standardanzeigedauer: 5 Sekunden).



Die Anzeigedauer dieser Fehlermeldung kann mit dem folgenden Registrierungsschlüssel auf dem VDA angepasst werden. Wenn der Registrierungseintrag nicht existiert, ist die Anzeigedauer standardmäßig 5 Sekunden.

> **Warnung**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Der Registrierungspfad hängt von der Architektur des VDAs ab:

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

oder

\HKLM\SOFTWARE\Citrix\HdxMediastream

Registrierungsschlüssel:

Name: VideoLoadManagementErrDuration

Typ: DWORD

Bereich: 1 - bis zur DWORD-Grenze (Standardwert = 5)

Einheit: Sekunden

Clientseitiger Abruf von Windows Media-Inhalten

Diese Einstellung gilt für Windows Media und HTML5. Diese Einstellung ermöglicht das Streamen von Multimediadateien direkt vom Quellanbieter im Internet oder Intranet auf Benutzergeräte statt über den XenApp- bzw. XenDesktop-Hostserver.

Standardmäßig ist diese Einstellung auf **Zugelassen** festgelegt. Zulassen dieser Einstellung verbessert die Netzwerknutzung und Serverskalierbarkeit durch Verschieben der gesamten Medienverarbeitung vom Hostserver auf das Benutzergerät. Dadurch wird auch das Erfordernis der Installation eines erweiterten Multimedia-Frameworks, z. B. von Microsoft DirectShow oder Media Foundation, auf Benutzergeräten hinfällig. Diese müssen lediglich eine Datei von einer URL abspielen können.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, muss die Einstellung **Windows Media-Umleitung** vorhanden und auf **Zugelassen** gesetzt sein. Wenn **Windows Media-Umleitung** deaktiviert ist, ist das direkte Streaming von Multimediadateien auf Benutzergeräte ebenfalls deaktiviert.

Windows Media-Umleitung

Diese Einstellung gilt für HTML5 und Windows Media und steuert bzw. optimiert die Art und Weise, mit der Server Audio- und Videostreams Benutzern bereitstellen.

Standardmäßig ist diese Einstellung auf **Zugelassen** festgelegt. Für HTML5 wird diese Einstellung nicht wirksam, wenn die Richtlinie ***HTML5-Videoumleitung*** auf **Nicht zugelassen** festgelegt ist.

Zulassen dieser Einstellung erhöht die Qualität von auf dem Server wiedergegebenem Audio und Video auf ein Niveau, das dem der lokalen Wiedergabe auf dem Benutzergerät entspricht. Der Server streamt Multimediainhalte komprimiert im Originalformat zum Client, Dekomprimierung und Wiedergabe der Medien übernimmt das Benutzergerät.

Die Windows Media-Umleitung optimiert Multimediadateien, die mit Codecs verschlüsselt sind, die den Standards von Microsoft DirectShow, DirectX Media Objects (DMO) und Media Foundation entsprechen. Um eine Multimediadatei wiederzugeben, muss ein mit dem Codierungsformat der Multimediadatei kompatibler Codec auf dem Benutzergerät vorhanden sein.

Standardmäßig ist die Richtlinie **Audio aktivieren** nicht auf dem Client konfiguriert. Wenn Benutzer Multimedia-Anwendungen in ICA-Sitzungen ausführen können, aktivieren Sie Audio oder geben Sie den Benutzern in der Clientbenutzeroberfläche die Berechtigung, Audio zu aktivieren.

Wählen Sie **Verweigert** nur, wenn die Wiedergabe von Medien mit der Windows Media-Umleitung schlechter zu sein scheint, als mit der ICA-Komprimierung und regulärem Audio. Dies ist selten, kann aber mit geringer Bandbreite vorkommen, beispielsweise bei Medien, in denen die Schlüsselbilder (Keyframes) sehr weit auseinander liegen.

Windows Media-Umleitungspuffergröße

Diese Einstellung ist älter und gilt nicht für HTML5.

Mit dieser Einstellung geben Sie für die Multimediabeschleunigung eine Puffergröße zwischen 1 und 10 Sekunden an.

Die Standardpuffergröße ist 5 Sekunden.

Verwendung von Windows Media-Umleitungspuffergröße

Diese Einstellung ist älter und gilt nicht für HTML5.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung der unter **Windows Media-Umleitungspuffergröße** angegebenen Puffergröße.

In der Standardeinstellung wird die angegebene Puffergröße nicht verwendet.

Wenn diese Einstellung deaktiviert oder die Einstellung für die Windows Media-Umleitungspuffergröße nicht konfiguriert ist, verwendet der Server den Standardwert für die Puffergröße (fünf Sekunden).

Einstellungen der Richtlinie "Multistreamverbindungen"

August 18, 2021

Im Abschnitt "Multistreamverbindungen"finden Sie Richtlinieneinstellungen zum Verwalten der Quality-of-Service-Priorität (QoS) für mehrere ICA-Verbindungen in einer Sitzung.

Audio über UDP

Mit dieser Einstellung legen Sie fest, ob Audio über UDP auf dem Server zugelassen wird.

Standardmäßig ist Audio über UDP auf dem Server zugelassen.

Wenn diese Einstellung aktiviert ist, wird ein UDP-Port auf dem Server geöffnet, sodass alle Verbindungen, die zur Verwendung von Audio über UDP - Real-time Transport konfiguriert sind, unterstützt werden.

Audio-UDP-Portbereich

Mit dieser Einstellung geben Sie den Bereich der Portnummern an (im Format niedrigste Portnummer,höchste Portnummer), die von Virtual Desktop Agent (VDA) zum Austausch von Audiopaketdaten mit dem Benutzergerät verwendet werden. Der VDA versucht, jedes UDP-Portpaar für den Austausch von Daten mit dem Benutzergerät zu verwenden. Dabei wird mit dem Port, der die niedrigste Nummer hat, begonnen und die Zahl für jeden folgenden Versuch um zwei erhöht. Alle Ports übernehmen eingehende und ausgehende Datenübertragungen.

Standardmäßig ist dies auf 16500,16509 festgelegt.

Multiportrichtlinie

Mit dieser Einstellung geben Sie die TCP-Ports an, die für den ICA-Verkehr verwendet werden sollen, und legen eine Netzwerkpriorität für jeden Port fest.

Standardmäßig hat der primäre Port (2598) eine hohe Priorität.

Wenn Sie Ports konfigurieren, können Sie die folgenden Prioritäten zuweisen:

- Sehr hoch: für Echtzeitvorgänge, z. B. Webkonferenzen.
- Hoch: für interaktive Elemente, z. B. Bildschirm, Tastatur und Maus.
- Mittel: für Massenvorgänge, z. B. Clientlaufwerkzuordnung.
- Niedrig: für Hintergrundaufgaben, z. B. Drucken.

Jeder Port muss eine eindeutige Priorität haben. Sie können also nicht eine sehr hohe Priorität sowohl für CGP-Port 1 als auch für CGP-Port 3 zuweisen.

Wenn Sie für einen Port keine Priorität einstellen möchten, setzen Sie den Wert für den Port auf 0. Sie können den primären Port nicht entfernen und Sie können seine Prioritätsstufe nicht ändern.

Wenn Sie diese Einstellung konfigurieren, starten Sie den Server neu. Diese Einstellung wird nur angewendet, wenn die Richtlinie Multistreamcomputereinstellung aktiviert ist.

Multistreamcomputereinstellung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Multistream auf dem Server.

Standardmäßig ist Multistream deaktiviert.

Wenn Sie Citrix SD-WAN mit Multistream-Unterstützung in Ihrer Umgebung verwenden, müssen Sie diese Einstellung nicht konfigurieren. Konfigurieren Sie diese Richtlinieneinstellung, wenn Sie Router von Drittanbietern oder Legacy-Branch Repeater verwenden, um die gewünschte Quality of Service (QoS) zu erzielen.

Wenn Sie diese Einstellung konfigurieren, starten Sie den Server neu, um sicherzustellen, dass die Änderungen wirksam werden.

Wichtig: Das Verwenden dieser Richtlinieneinstellung mit den Richtlinieneinstellungen für das Bandbreitenlimit, wie beispielsweise Bandbreitenlimit für Sitzung insgesamt kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Einstellung in eine Richtlinie aufnehmen, stellen Sie sicher, dass Sie keine Bandbreitenlimit-Einstellungen einschließen.

Multistreambenutzereinstellung

Mit dieser Einstellung aktivieren oder deaktivieren Sie Multistream auf dem Benutzergerät.

Standardmäßig ist Multistream für alle Benutzer deaktiviert.

Diese Einstellung wird nur auf Hosts angewendet, für die die Richtlinie Multistreamcomputereinstellung aktiviert ist.

Wichtig: Das Verwenden dieser Richtlinieneinstellung mit den Richtlinieneinstellungen für das Bandbreitenlimit, z. B. "Bandbreitenlimit für Sitzung insgesamt", kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Einstellung in eine Richtlinie aufnehmen, stellen Sie sicher, dass Sie keine Bandbreitenlimit-Einstellungen einschließen.

Einstellungen der Richtlinie "Portumleitung"

August 18, 2021

Der Abschnitt "Portumleitung"enthält Richtlinieneinstellungen für die LPT- und COM-Portzuordnung auf dem Client.

Verwenden Sie bei Virtual Delivery Agent-Versionen **vor 7.0** die folgenden Richtlinieneinstellungen zum Konfigurieren der Portumleitung. Konfigurieren Sie bei VDA **7.0 bis 7.8** diese Einstellungen über die Registrierung (siehe Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung). Verwenden Sie bei VDA-Version **7.9** die folgenden Richtlinieneinstellungen.

Client-COM-Ports automatisch verbinden

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Verbindung von COM-Ports auf dem Benutzergerät, wenn Benutzer sich bei der Site anmelden.

Standardmäßig werden COM-Ports nicht automatisch verbunden.

Client-LPT-Ports automatisch verbinden

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Verbindung von LPT-Ports auf dem Benutzergerät, wenn Benutzer sich bei der Site anmelden.

Standardmäßig werden LPT-Ports nicht automatisch verbunden.

Client-COM-Portumleitung

Mit dieser Einstellung legen Sie fest, ob der Zugriff auf COM-Ports des Benutzergeräts zulässig ist.

Standardmäßig ist die COM-Portumleitung nicht zugelassen.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Bandbreitenlimit für COM-Portumleitung
- Bandbreitenlimit für COM-Portumleitung (Prozent)

Client-LPT-Portumleitung

Mit dieser Einstellung legen Sie fest, ob der Zugriff auf LPT-Ports des Benutzergeräts zulässig ist.

Standardmäßig ist die LPT-Portumleitung nicht zugelassen.

LPT-Ports werden nur von Legacyanwendungen verwendet, die Druckaufträge an LPT-Ports senden und nicht an die Druckerobjekte auf dem Benutzergerät. Die meisten Geräte können heute Druckaufträge and Druckerobjekte senden. Diese Richtlinieneinstellung ist nur für Server erforderlich, auf denen Legacyanwendungen gehostet werden, die für das Drucken LPT-Ports verwenden.

Obwohl die COM-Portumleitung des Clients bidirektional ist, gilt die LPT-Portumleitung nur für die Ausgabe und ist in einer ICA-Sitzung auf \\client\LPT1 und \\client\LPT2 beschränkt.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Bandbreitenlimit für LPT-Portumleitung
- Bandbreitenlimit für LPT-Portumleitung (Prozent)

Einstellungen der Richtlinie “Drucken”

February 22, 2019

Der Abschnitt “Drucken”enthält Richtlinieneinstellungen für die Verwaltung des Clientdrucks.

Clientdruckerumleitung

Mit dieser Einstellung legen Sie fest, ob Clientdrucker einem Server zugeordnet werden können, wenn sich ein Benutzer an einer Sitzung anmeldet.

Standardmäßig ist die Clientdruckerzuordnung zugelassen. Wenn diese Einstellung deaktiviert ist, wird der PDF-Drucker für die Sitzung nicht automatisch erstellt.

Verwandte Richtlinieneinstellungen: Clientdrucker automatisch erstellen

Standarddrucker

Mit dieser Einstellung geben Sie an, wie der Standarddrucker in einer ICA-Sitzung ermittelt wird.

Standardmäßig wird der aktuelle Standarddrucker auf dem Clientgerät als Standarddrucker in der Sitzung verwendet.

Mit “Standarddrucker des Benutzers nicht anpassen”werden die aktuellen Einstellungen für den Standarddrucker in den Remotedesktopdiensten oder im
Windows-Benutzerprofil verwendet. Wenn Sie diese Option auswählen, wird der Standarddrucker nicht im Profil gespeichert und ändert sich nicht entsprechend den anderen Sitzungs- oder Clienteigenschaften. Der Standarddrucker in einer Sitzung ist der erste Drucker, der in der Sitzung automatisch erstellt wird. Das ist:

- Der erste Drucker, der lokal auf dem Windows-Server unter Systemsteuerung > Geräte und Drucker hinzugefügt wurde.
- Der erste automatisch erstellte Drucker, wenn auf dem Server keine Drucker lokal hinzugefügt wurden.

Verwenden Sie diese Option, um Benutzern über Profileinstellungen den nächstgelegenen Drucker anzubieten (Proximitydrucken).

Druckerzuordnungen

Diese Einstellung bietet eine Alternative zu den Einstellungen Standarddrucker und Sitzungsdrucker. Mit den einzelnen Einstellungen für Standarddrucker und Sitzungsdrucker können Sie das Verhalten

einer Site, einer großen Gruppe oder einer Organisationseinheit konfigurieren. Mit der Einstellung Druckerzuweisungen weisen Sie eine große Gruppe Drucker mehreren Benutzern zu.

Mit dieser Einstellung geben Sie an, wie der Standarddrucker auf den aufgeführten Benutzergeräten in einer Sitzung ermittelt wird.

Standardmäßig wird der aktuelle Standarddrucker auf dem Clientgerät als Standarddrucker in der Sitzung verwendet.

Mit dieser Einstellung geben Sie außerdem die Netzwerkdrucker an, die in einer Sitzung für jedes Benutzergerät automatisch erstellt werden sollen. In der Standardeinstellung sind keine Drucker angegeben.

- Beim Einstellen des Standarddruckerwerts:

  Wenn Sie den aktuellen Standarddrucker für das Benutzergerät verwenden möchten, wählen Sie Nicht anpassen.

  Mit Do not adjust werden die aktuellen Einstellungen für den Standarddrucker in den Remotedesktopdiensten oder im Windows-Benutzerprofil verwendet. Wenn Sie diese Option auswählen, wird der Standarddrucker nicht im Profil gespeichert und ändert sich nicht entsprechend den anderen Sitzungs- oder Clienteigenschaften. Der Standarddrucker in einer Sitzung ist der erste Drucker, der in der Sitzung automatisch erstellt wird. Das ist:

  - Der erste Drucker, der lokal auf dem Windows-Server unter Systemsteuerung > Geräte und Drucker hinzugefügt wurde.
  - Der erste automatisch erstellte Drucker, wenn auf dem Server keine Drucker lokal hinzugefügt wurden.

- Beim Einstellen des Sitzungsdruckerwerts: Zum Hinzufügen eines Druckers geben Sie den UNC-Pfad des Druckers ein, der automatisch erstellt werden soll. Nach dem Hinzufügen des Druckers können Sie angepasste Einstellungen für die aktuelle Sitzung bei jeder Anmeldung anwenden.

Präferenz für Ereignisprotokoll bei automatischer Druckererstellung

Mit dieser Einstellung geben Sie an, welche Ereignisse bei der automatischen Druckererstellung protokolliert werden. Sie haben die Option, keine Fehler oder Warnungen, nur Fehler oder Fehler und Warnungen zu protokollieren.

Standardmäßig werden Fehler und Warnungen protokolliert.

Ein Beispiel für eine Warnung ist ein Ereignis, bei dem der native Druckertreiber für einen Drucker nicht installiert werden konnte und stattdessen der universelle Druckertreiber installiert wurde. Damit der universelle Druckertreiber in diesem Szenario verwendet werden kann, stellen Sie für Verwendung universeller Druckertreiber entweder Nur universelles Drucken verwenden oder Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist ein.

Sitzungsdrucker

Mit dieser Einstellung geben Sie die Netzwerkdrucker an, die in einer ICA-Sitzung automatisch erstellt werden sollen.

In der Standardeinstellung sind keine Drucker angegeben.

Um Drucker hinzuzufügen, geben Sie den UNC-Pfad des Druckers ein, der automatisch erstellt werden soll. Nach dem Hinzufügen des Druckers können Sie angepasste Einstellungen für die aktuelle Sitzung bei jeder Anmeldung anwenden.

Warten bis Drucker erstellt sind (Serverdesktop)

Mit dieser Einstellung legen Sie fest, ob es eine Verzögerung bei der Sitzungsverbindung geben soll, sodass Serverdesktopdrucker automatisch erstellt werden können.

Standardmäßig findet keine Verbindungsverzögerung statt.

Einstellungen der Richtlinie "Clientdrucker"

February 22, 2019

Der Abschnitt "Clientdrucker"enthält Richtlinieneinstellungen für Clientdrucker, einschließlich solcher zur automatischen Erstellung von Clientdruckern, zum Speichern von Druckereigenschaften und zum Verbinden mit Druckservern.

Clientdrucker automatisch erstellen

Mit dieser Einstellung geben Sie die Clientdrucker an, die automatisch erstellt werden. Diese Einstellung überschreibt die Standardeinstellungen für die automatische Clientdruckererstellung.

Standardmäßig werden alle Clientdrucker automatisch erstellt.

Diese Einstellung gilt nur, wenn die Einstellung Clientdruckerumleitung vorhanden und Zugelassen ist.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Mit Alle Clientdrucker automatisch erstellen werden alle Drucker auf dem Clientgerät erstellt.
- Mit Nur Standarddrucker des Clients automatisch erstellen wird der Drucker automatisch erstellt, der auf dem Clientgerät als Standarddrucker angegeben wurde.

- Mit Nur lokale Clientdrucker (keine Netzwerkdrucker) automatisch erstellen werden nur die Drucker automatisch erstellt, die über einen LPT-, COM-, USB-, TCP/IP- oder anderen lokalen Port direkt mit dem Clientgerät verbunden sind.
- Mit Clientdrucker nicht automatisch erstellen wird die automatische Erstellung von Clientdruckern beim Anmelden der Benutzer deaktiviert. Die Remotedesktopdienste-Einstellungen für die automatische Erstellung von Clientdruckern überschreiben dann diese Einstellung in Richtlinien mit niedrigerer Priorität.

Generischen universellen Drucker automatisch erstellen

Hinweis: Hotfixes für Probleme aufgrund dieser Richtlinieneinstellung sind in den Knowledge Center-Artikeln CTX141565 und CTX141566 verfügbar.

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Erstellung des generischen universellen Citrix Druckerobjekts für Sitzungen, in denen ein Benutzergerät verwendet wird, das mit der universellen Drucklösung kompatibel ist.

Standardmäßig wird das generische universelle Druckerobjekt nicht automatisch erstellt.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Verwendung universeller Druckertreiber
- Priorität universeller Treiber

Clientdruckernamen

Mit dieser Einstellung legen Sie die Namenskonvention für automatisch erstellte Drucker fest.

Standardmäßig werden die Standardnamen der Drucker verwendet.

Wählen Sie Standarddruckernamen, um Druckernamen im Format "HPLaserJet 4 von Clientname in Sitzung 3"zu verwenden.

Wählen Sie
"Legacydruckernamen", um Clientdruckernamen im alten Stil zuzulassen und die Rückwärtskompatibilität für Benutzer oder Gruppen zu erhalten, die MetaFrame Presentation Server 3.0 oder früher verwenden. Ein Beispiel für einen Legacydruckernamen ist "Client/clientname#/HPLaserJet 4". Diese Option ist weniger sicher.

Hinweis: Diese Option wird nur für Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop bereitgestellt.

Direkte Verbindungen zu Druckservern

Mit dieser Einstellung aktivieren oder deaktivieren Sie direkte Verbindungen vom virtuellen Desktop oder Server, auf dem Anwendungen gehostet werden, zu einem Druckserver für Clientdrucker in einer zugänglichen Netzwerkfreigabe.

Standardmäßig sind direkte Verbindungen aktiviert.

Aktivieren Sie direkte Verbindungen, wenn der Netzwerkdruckserver für virtuelle Desktops bzw. für Server, auf denen Anwendungen gehostet werden, nicht über ein WAN zugänglich ist. Direkte Verbindungen gestatten schnelleres Drucken, wenn der Netzwerkdruckserver und der virtuelle Desktop oder Anwendungsserver sich im gleichen LAN befinden.

Deaktivieren Sie direkte Verbindungen, wenn das Netzwerk über ein WAN verläuft oder hohe Latenz oder beschränkte Bandbreite aufweist. Druckaufträge werden durch das Benutzergerät und den Netzwerkdruckserver geleitet. Daten werden komprimiert an das Benutzergerät gesendet, es wird somit weniger Bandbreite bei der Übertragung der Daten über das WAN gebraucht.

Wenn zwei Netzwerkdrucker den gleichen Namen haben, wird der Drucker benutzt, der im gleichen Netzwerk ist wie der Client.

Druckertreiberzuordnung und -kompatibilität

Mit dieser Einstellung legen Sie Regeln für die Treiberersetzung bei automatisch erstellten Druckern fest.

Diese Einstellung ist so konfiguriert, dass Microsoft OneNote und XPS Document Writer aus der Liste der automatisch erstellten Clientdrucker ausgeschlossen werden.

Wenn Sie Regeln für die Treiberersetzung definieren, können Sie zulassen oder verhindern, dass Drucker mit dem angegebenen Treiber erstellt werden. Außerdem können Sie für erstellte Drucker nur universelle Druckertreiber zulassen. Bei der Treiberersetzung werden die Namen der Druckertreiber, die das Benutzergerät bereitstellt, überschrieben oder zugeordnet und ein äquivalenter Treiber auf dem Server wird ersetzt. So können Serveranwendungen auf Clientdrucker zuzugreifen, die denselben Treiber wie der Server, aber unterschiedliche Treibernamen verwenden.

Sie können eine Treiberzuordnung hinzufügen, eine bestehende Zuordnung bearbeiten, benutzerdefinierte Einstellungen für eine Zuordnung überschreiben oder die Reihenfolge der Treibereinträge in der Liste ändern. Um eine Zuordnung hinzuzufügen, geben Sie den Clientdruckertreibernamen an und wählen dann den Ersatztreiber auf dem Server aus.

Speicherung von Druckereigenschaften

Mit dieser Einstellung geben Sie an, ob die Druckereigenschaften gespeichert werden und wo.

Standardmäßig ermittelt das System, ob Druckereigenschaften auf dem Clientgerät (falls verfügbar) gespeichert werden oder im Benutzerprofil.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Wählen Sie Nur auf dem Clientgerät speichern, wenn Sie ein vorgeschriebenes oder servergespeichertes Profil verwenden, das nicht gespeichert wird. Wählen Sie diese Option nur aus, wenn auf allen Servern in der Farm XenApp 5 oder höher ausgeführt wird und die Benutzer die Citrix Online Plug-In-Versionen 9 bis 12.x oder Citrix Receiver 3.x verwenden.
- Wählen Sie Nur im Benutzerprofil speichern, wenn das System durch die Bandbreite (diese Option reduziert den Datenverkehr im Netzwerk) und die Anmeldegeschwindigkeit begrenzt ist oder die Benutzer Legacy-Plug-Ins verwenden. Bei dieser Option werden die Druckereigenschaften im Benutzerprofil auf dem Server gespeichert. Die Eigenschaften werden nicht mit dem Clientgerät ausgetauscht. Verwenden Sie diese Option für MetaFrame Presentation Server 3.0 oder früher und MetaFrame Presentation Server Client 8.x oder früher. Dies gilt nur, wenn ein servergespeichertes Profil für Remotedesktopdienste (RDS) verwendet wird.
- Mit Nur im Profil speichern, wenn sie nicht auf dem Client gespeichert sind kann das System festlegen, wo die Druckereigenschaften gespeichert werden. Die Druckereigenschaften werden auf dem Clientgerät gespeichert, sofern es verfügbar ist, ansonsten im Benutzerprofil. Diese Option bietet zwar die größte Flexibilität, kann jedoch die Anmeldezeit verlangsamen und zusätzliche Bandbreite für die Systemprüfung verbrauchen.
- Druckereigenschaften nicht speichern verhindert das Speichern von Druckereigenschaften.

Gespeicherte und wiederhergestellte Clientdrucker

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Speichern und Neuerstellen von Clientdruckern. Standardmäßig werden Clientdrucker automatisch gespeichert und automatisch wiederhergestellt.

Gespeicherte Drucker sind vom Benutzer erstellte Drucker, die beim Start der nächsten Sitzung wiederhergestellt werden. Wenn XenApp einen gespeicherten Drucker wiederhergestellt, werden alle Richtlinieneinstellungen außer Clientdrucker automatisch erstellen berücksichtigt.

Gespeicherte Drucker sind Drucker die von einem Administrator vollständig angepasst wurden und deren gespeicherter Zustand permanent mit einem Clientport verbunden ist.

Einstellungen der Richtlinie “Treiber”

November 29, 2018

Der Abschnitt “Treiber”enthält Richtlinieneinstellungen für Druckertreiber.

Automatische Installation von mitgelieferten Druckertreibern

Mit dieser Einstellung aktivieren oder deaktivieren Sie die automatische Installation von Druckertreibern vom standardmäßigen Windows-Treibersatz oder von Treiberpaketen, die auf dem Host mit pnputil.exe /a bereitgestellt wurden.

Standardmäßig werden diese Treiber bei Bedarf installiert.

Priorität universeller Treiber

Mit dieser Einstellung geben Sie an, in welcher Reihenfolge die universellen Druckertreiber verwendet werden, angefangen mit dem ersten Eintrag in der Liste.

Standardmäßig ist die Prioritätsreihenfolge wie folgt:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Sie können Treiber hinzufügen, bearbeiten oder entfernen und die Reihenfolge der Treiber in der Liste ändern.

Verwendung universeller Druckertreiber

Mit dieser Einstellung geben Sie an, wann universelles Drucken verwendet wird.

Standardmäßig wird universelles Drucken nur verwendet, wenn der angeforderte Treiber nicht verfügbar ist.

Universelles Drucken verwendet allgemeine Druckertreiber statt modellspezifischer Standardtreiber; dies verringert potentiell den Aufwand für die Treiberverwaltung auf Hostcomputern. Die Verfügbarkeit universeller Druckertreiber hängt von den Funktionen des Benutzergeräts, des Hosts und der Druckserversoftware ab. In bestimmten Konfigurationen steht universelles Drucken möglicherweise nicht zur Verfügung.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Mit Nur druckermodellspezifische Treiber verwenden verwendet der Clientdrucker nur die modellspezifischen Standardtreiber, die bei der Anmeldung automatisch erstellt wurden. Wenn der erforderliche Treiber nicht verfügbar ist, kann der Clientdrucker nicht automatisch erstellt werden.

- Nur universelles Drucken verwenden gibt an, dass keine modellspezifischen Standardtreiber verwendet werden. Nur universelle Druckertreiber werden zum Erstellen von Druckern verwendet.
- Mit Universelles Drucken nur verwenden, wenn angeforderter Treiber nicht verfügbar ist werden modellspezifische Standardtreiber für die Druckererstellung verwendet, wenn sie verfügbar sind. Wenn der Treiber auf dem Server nicht zur Verfügung steht, wird der Clientdrucker automatisch mit dem entsprechenden universellen Treiber erstellt.
- Mit Druckermodellspezifische Treiber nur verwenden, wenn universelles Drucken nicht verfügbar ist werden universelle Druckertreiber verwendet, wenn sie verfügbar sind. Wenn der Treiber auf dem Server nicht zur Verfügung steht, wird der Clientdrucker automatisch mit dem entsprechenden modellspezifischen Druckertreiber erstellt.

Einstellungen der Richtlinie "Universeller Druckserver"

August 18, 2021

Der Abschnitt "Universeller Druckserver"enthält Richtlinieneinstellungen für die Behandlung des universellen Druckservers.

Universellen Druckserver aktivieren

Diese Einstellung aktiviert oder deaktiviert das Feature "Universeller Druckserver"auf dem virtuellen Desktop oder dem Server, auf dem Anwendungen gehostet werden. Wenden Sie die Richtlinie auf Organisationseinheiten an, die den virtuellen Desktop oder Server enthalten, auf dem Anwendungen gehostet werden.

Standardmäßig ist das Feature deaktiviert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der folgenden Optionen:

- **Aktiviert mit Fallback auf systemeigenen Windows-Remotedruck**. Netzwerkdruckerverbindungen werden nach Möglichkeit vom universellen Druckserver bedient. Wenn dieser nicht verfügbar ist, wird der Windows-Druckanbieter verwendet. Der Windows-Druckanbieter handhabt weiterhin alle Drucker, die vorher mit dem Windows-Druckanbieter erstellt wurden.
- **Aktiviert ohne Fallback auf systemeigenen Windows-Remotedruck**. Netzwerkdruckerverbindungen werden ausschließlich vom universellen Druckserver bedient. Wenn dieser nicht verfügbar ist, schlägt die Netzwerkdruckerverbindung fehl. Mit dieser Einstellung wird der Netzwerkdruck über den Windows-Druckanbieter effektiv deaktiviert. Drucker, die vorher mit dem Windows-Druckanbieter erstellt wurden, werden nicht erstellt, solange eine Richtlinie mit dieser Einstellung aktiv ist.

- **Deaktiviert.** Das Feature "Universeller Druckserver"ist deaktiviert. Beim Herstellen einer Verbindung mit einem Netzwerkdrucker, der einen UNC-Namen hat, wird keine Verbindung mit dem universellen Druckserver versucht. Verbindungen mit Remotedruckern verwenden weiterhin den Windows-Remotedruck.

Port für Druckdatenstrom des universellen Druckservers (CGP)

Diese Einstellung gibt die Nummer des TCP-Ports an, die vom Druckdatenstrom-Listener (CGP) des universellen Druckservers verwendet wird. Wenden Sie diese Richtlinie nur für Organisationseinheiten an, die den Druckserver enthalten.

Die Standardeinstellung der Portnummer ist "7229".

Gültige Portnummern müssen im Bereich von 1 bis 65535 liegen.

Universeller Druckserver - Eingabebandbreitenlimit für Druckdatenstrom (KBit/s)

Diese Einstellung gibt das obere Limit (in Kilobit pro Sekunde) für die Übertragungsrate der Druckdaten an, die von jedem Druckauftrag mit CGP an den universellen Druckserver übergeben werden. Wenden Sie die Richtlinie auf Organisationseinheiten an, die den virtuellen Desktop oder Server enthalten, auf dem Anwendungen gehostet werden.

In der Standardeinstellung ist der Wert 0, was angibt, dass es kein oberes Limit gibt.

Port für universellen Druckserverwebdienst (HTTP/SOAP)

Diese Einstellung gibt die Nummer des TCP-Ports an, die vom HTTP/SOAP-Webdienstlistener des universellen Druckservers verwendet wird. Der universelle Druckserver ist eine optionale Komponente, mit der die Verwendung universeller Druckertreiber von Citrix für den Netzwerkdruck ermöglicht wird. Wird der universelle Druckserver verwendet, werden die Druckbefehle von den XenApp- und XenDesktop-Hosts mit SOAP über HTTP an den universellen Druckserver gesendet. Durch diese Einstellung ändert sich die Nummer des Standard-TCP-Ports, der vom Webdienstlistener des universellen Druckservers für eingehende HTTP/SOAP-Anforderungen überwacht wird.

Sie müssen den gleichen HTTP- Port für Host und Druckserver konfigurieren. Wenn Sie nicht den gleichen Port konfigurieren, stellt die Hostsoftware keine Verbindung mit dem universellen Druckserver her. Durch diese Einstellung ändert sich der VDA unter XenApp und XenDesktop. Außerdem müssen Sie den Standardport auf dem Computer mit dem universellen Druckserver ändern.

Die Standardeinstellung der Portnummer ist 8080.

Gültige Portnummern müssen im Bereich von 0 bis 65535 liegen.

Universelle Druckserver für den Lastausgleich

Mit dieser Einstellung werden die universellen Druckserver aufgelistet, die zum Lastausgleich für am Sitzungsstart erstellte Druckerverbindungen verwendet werden, nachdem andere Citrix Druckrichtlinieneinstellungen bewertet wurden. Zum Optimieren der Erstellungszeit von Druckern empfiehlt Citrix, dass alle Druckserver über denselben Satz freigegebener Drucker verfügen. Es gibt kein Maximum für die Anzahl von Druckservern, die für den Lastausgleich hinzugefügt werden können.

Diese Einstellung implementiert auch Druckserver-Failovererkennung und die Wiederherstellung von Druckerverbindungen. Die Druckserver werden regelmäßig auf Verfügbarkeit überprüft. Wenn ein Serverfehler erkannt wird, wird der Server aus dem Lastausgleichsschema entfernt und Druckerverbindungen auf dem Server werden auf andere verfügbare Druckserver verteilt. Wenn der fehlerhafte Druckserver wiederhergestellt ist, wird er dem Lastausgleichsschema wieder hinzugefügt.

Klicken Sie auf **Server überprüfen**, um zu prüfen, ob die einzelnen Server Druckserver sind, und um sicherzustellen, dass auf allen Druckservern ein identischer Satz freigegebener Drucker installiert ist. Dieser Vorgang kann einige Zeit dauern.

Außer-Betrieb-Schwellenwert für universelle Druckserver

Mit dieser Einstellung wird angegeben, wie lange der Load Balancer auf die Wiederherstellung eines nicht verfügbaren universellen Druckservers wartet, bevor der Server als offline gilt und die Last des Servers auf andere verfügbare Druckserver verteilt wird.

Der Standardschwellenwert ist 180 (Sekunden).

Einstellungen der Richtlinie "Universelles Drucken"

April 30, 2019

Der Abschnitt "Universelles Drucken"enthält Richtlinieneinstellungen für die Verwaltung des universellen Drucks.

Universelles Drucken - EMF-Verarbeitungsmodus

Mit dieser Einstellung steuern Sie die Verarbeitungsmethode für die EMF-Spooldatei auf dem Windows-Benutzergerät.

Standardmäßig werden EMF-Datensätze direkt zum Drucker gespoolt.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- EMF-Datensätze für Drucker neu verarbeiten erzwingt die Neuverarbeitung der EMF-Spooldatei und sendet sie durch das GDI-Teilsystem auf dem Benutzergerät. Sie können diese Einstellung für Treiber verwenden, für die eine EMF-Neuverarbeitung erforderlich ist, die jedoch nicht unbedingt in der Sitzung automatisch ausgewählt werden.
- Wenn Direkt zum Drucker spoolen mit dem universellen Citrix Druckertreiber verwendet wird, werden die EMF-Datensätze garantiert gespoolt und an das Benutzergerät für die Verarbeitung übergeben. Diese EMF-Spooldateien werden normalerweise direkt in die Spoolwarteschlange des Clients gesetzt. Für Drucker und Treiber, die mit dem EMF-Format kompatibel sind, ist dies die schnellste Druckmethode.

Universelles Drucken - Bildkomprimierungslimit

Mit dieser Einstellung geben Sie die maximale Qualität und minimale Komprimierung für Bilder an, die mit dem universellen Citrix Druckertreiber gedruckt werden.

Das Limit für Bildkomprimierung ist standardmäßig auf Beste Qualität (verlustfreie Komprimierung) gesetzt.

Wenn Keine Komprimierung ausgewählt ist, wird die Komprimierung nur für den EMF-Druck deaktiviert.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Keine Komprimierung
- Optimale Qualität (verlustfreie Komprimierung)
- Hohe Qualität
- Standardqualität
- Niedrige Qualität (maximale Komprimierung)

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, die auch die Einstellung "Universelles Drucken - Optimierungsstandards"enthält, achten Sie auf Folgendes:

- Wenn die Komprimierungsstufe in der Einstellung Universelles Drucken - Komprimierungslimit niedriger ist als die in der Einstellung Universelles Drucken - Optimierungsstandards werden Bilder basierend auf der Einstellung Universelles Drucken - Komprimierungslimits komprimiert.
- Wenn die Komprimierung deaktiviert ist, haben die Optionen Gewünschte Bildqualität und Heavyweight-Komprimierung aktivieren in der Einstellung Universelles Drucken - Optimierungsstandards keine Auswirkung in der Richtlinie.

Universelles Drucken - Optimierungsstandards

Mit dieser Einstellung geben Sie die Standardwerte für die Druckoptimierung an, wenn der universelle Druckertreiber für eine Sitzung erstellt wurde.

- Mit Gewünschte Bildqualität geben Sie das standardmäßige Bildkomprimierungslimit an, das auf universelles Drucken angewendet wird. In der Standardeinstellung ist Standardqualität aktiviert, d. h. Benutzer können Bilder nur mit der Standardqualitäts- oder geringeren Qualitätskomprimierung drucken.
- Mit "Heavyweight-Komprimierung aktivieren"aktivieren oder deaktivieren Sie das Verringern der Bandbreite unter den Komprimierungsgrad, der von Gewünschte Bildqualität festgelegt ist; Bildqualität geht nicht verloren. Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.
- Mit den Einstellungen Zwischenspeichern von Bildern und Schriftarten legen Sie fest, ob Bilder und Schriftarten, die mehrmals im Druckdatenstrom vorhanden sind, zwischengespeichert werden. Sie stellen damit sicher, dass jedes eindeutige Bild oder jede Schriftart nur einmal zum Drucker gesendet wird. Standardmäßig werden eingebettete Bilder und Schriftarten zwischengespeichert. Hinweis: Diese Einstellungen gelten nur, wenn das Benutzergerät dieses Verhalten unterstützt.
- Mit Nicht-Administratoren können diese Einstellungen ändern legen Sie fest, ob Benutzer die Standardeinstellungen für die Druckoptimierung in einer Sitzung ändern können. Standardmäßig können Benutzer die Standardeinstellungen für die Druckoptimierung nicht ändern.

Hinweis: Alle diese Optionen werden für den EMF-Druck unterstützt. Für XPS-Druck wird nur die Option Gewünschte Bildqualität unterstützt.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, die auch die Einstellung "Universelles Drucken - Optimierungsstandards"enthält, achten Sie auf Folgendes:

- Wenn die Komprimierungsstufe in der Einstellung Universelles Drucken - Komprimierungslimit niedriger ist als die in der Einstellung Universelles Drucken - Optimierungsstandards werden Bilder basierend auf der Einstellung Universelles Drucken - Komprimierungslimits komprimiert.
- Wenn die Komprimierung deaktiviert ist, haben die Optionen Gewünschte Bildqualität und Heavyweight-Komprimierung aktivieren in der Einstellung Universelles Drucken - Optimierungsstandards keine Auswirkung in der Richtlinie.

Universelles Drucken - Vorschaueinstellung

Mit dieser Einstellung geben Sie an, ob die Druckvorschau für automatisch erstellte oder universelle Drucker verwendet werden soll.

Standardmäßig wird die Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwendet.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Druckvorschau für automatisch erstellte oder generische universelle Drucker nicht verwenden
- Druckervorschau nur für automatisch erstellte Drucker verwenden
- Druckervorschau nur für generische universelle Drucker verwenden
- Druckvorschau für automatisch erstellte und generische universelle Drucker verwenden

Universelles Drucken - Druckqualitätslimit

Diese Einstellung legt den Höchstwert für Punkte pro Zoll (dpi) zum Erstellen von Ausdrucken in einer Sitzung fest.

Standardmäßig ist Kein Limit aktiviert, d. h. Benutzer können die höchste Druckqualität auswählen, die vom Drucker zugelassen wird, mit dem sie eine Verbindung herstellen.

Wenn diese Einstellung konfiguriert ist, wird die maximale Druckqualität, die Benutzern zur Verfügung steht, hinsichtlich Ausgabeauflösung beschränkt. Sowohl die Druckqualität und die Druckqualitätsmerkmale des Druckers, mit dem sich die Benutzer verbinden, werden auf die konfigurierte Einstellung beschränkt. Beispiel: Wenn Mittlere Auflösung (600 dpi) konfiguriert ist, können Benutzer eine Ausgabe nur mit einer maximalen Qualität von 600 drucken, und die Einstellung "Druckqualität" auf der Registerkarte "Erweitert"im Dialogfeld "Universeller Drucker"enthält nur Auflösungseinstellungen bis zu "Mittlere Qualität (600 dpi)".

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Entwurf (150 dpi)
- Niedrige Auflösung (300 dpi)
- Mittlere Auflösung (600 dpi)
- Hohe Auflösung (1200 dpi)
- Kein Limit

Einstellungen der Richtlinie "Sicherheit"

July 1, 2019

Der Abschnitt "Sicherheit"enthält die Richtlinieneinstellung zum Konfigurieren der Sitzungsverschlüsselung und der Anmeldedatenverschlüsselung.

SecureICA-Mindestverschlüsselungsgrad

Mit dieser Einstellung geben Sie das Minimum für den Verschlüsselungsgrad der Sitzungsdaten an, die zwischen dem Server und einem Clientgerät ausgetauscht werden.

Wichtig: Bei Virtual Delivery Agent 7.x kann mit dieser Richtlinieneinstellung nur die Anmeldedatenverschlüsselung mit RC5 128-Bit-Verschlüsselung aktiviert werden. Die anderen Einstellungen werden nur für Abwärtskompatibilität mit älteren Versionen von XenApp und XenDesktop bereitgestellt.

Bei VDA 7.x wird die Sitzungsdatenverschlüsselung mit den Grundeinstellungen der Bereitstellungsgruppe des VDAs festgelegt. Wenn für die Bereitstellungsgruppe die Option "Secure ICA aktivieren" ausgewählt ist, werden Sitzungsdaten mit der RC5-Verschlüsselung (128 Bit) verschlüsselt. Wenn die Option "Secure ICA aktivieren"für die Bereitstellungsgruppe nicht ausgewählt ist, werden Sitzungsdaten mit der Basic-Verschlüsselung verschlüsselt.

Wenn Sie diese Einstellung einer Richtlinie hinzufügen, wählen Sie eine der Optionen:

- Basic verschlüsselt die Clientverbindung mit einem nicht RC5-konformen Algorithmus. Mit diesem Verschlüsselungsverfahren kann der Datenstrom zwar vor direktem Lesen geschützt werden, ein Entschlüsseln ist aber möglich. Standardmäßig verwendet der Server für den Client-Server-Netzwerkverkehr den Verschlüsselungsgrad "Basic".
- RC5 (128 Bit) nur Anmeldung verschlüsselt die Anmeldedaten mit der RC5-128-Bit-Verschlüsselung und die Clientverbindung mit dem Verschlüsselungsgrad "Basic".
- RC5 (40 Bit) verschlüsselt die Verbindung mit der RC5-40-Bit-Verschlüsselung.
- RC5 (56 Bit) verschlüsselt die Verbindung mit der RC5-56-Bit-Verschlüsselung.
- RC5 (128 Bit) verschlüsselt die Verbindung mit der RC5-128-Bit-Verschlüsselung.

Die Einstellungen, die Sie für die Verschlüsselung zwischen Client und Server festlegen, können mit Verschlüsselungseinstellungen des Windows-Betriebssystems interagieren. Wenn ein höherer Verschlüsselungsgrad auf dem Server oder Benutzergerät eingestellt ist, können Einstellungen überschrieben werden, die Sie für veröffentlichte Ressourcen angegeben haben.

Sie können den Verschlüsselungsgrad erhöhen, um die Kommunikation und Datenintegrität für bestimmte Benutzer stärker zu sichern. Wenn für eine Richtlinie ein höherer Verschlüsselungsgrad erforderlich ist, wird Citrix Receivern mit einem niedrigeren Verschlüsselungsgrad die Verbindung verweigert.

SecureICA führt keine Authentifizierung durch und prüft auch nicht die Datenintegrität. Verwenden Sie SecureICA mit TLS-Verschlüsselung, um eine vollständige Verschlüsselung für die Site bereitzustellen.

SecureICA verwendet nicht FIPS-konforme Algorithmen. Wenn dies ein Problem ist, konfigurieren Sie den Server und Citrix Receiver, um zu verhindern, dass SecureICA verwendet wird.

SecureICA verwendet die RC5-Blockverschlüsselung gemäß RFC 2040. Die Blockgröße entspricht 64 Bit (ein Mehrfaches von 32-Bit-Worteinheiten). Die Schlüssellänge ist 128 Bit. Die Zahl der Runden ist 12.

Einstellungen der Richtlinie "Serverlimits"

February 4, 2020

Der Abschnitt "Serverlimits"enthält die Richtlinieneinstellung zum Steuern von Sitzungen im Leerlauf.

Serverleerlauf-Zeitintervall

Mit dieser Einstellung geben Sie in Millisekunden an, wie lange eine ununterbrochene Benutzersitzung erhalten bleibt, wenn keine Benutzereingaben stattfinden.

Standardmäßig werden Leerlaufsitzungen nicht getrennt (Serverleerlaufzeitintervall = 0) Citrix empfiehlt, diesen Wert auf mindestens 60000 Millisekunden (60 Sekunden) festzulegen.

> **Hinweis:**
>
> Bei Verwendung dieser Richtlinie wird Benutzern u. U. ein Dialogfeld mit der Meldung "Leerlauf-Timer abgelaufen"angezeigt, wenn die Sitzung die angegebene Zeit lang im Leerlauf war. Diese Meldung ist ein Microsoft-Dialogfeld, das nicht von Citrix Richtlinieneinstellungen gesteuert wird. Weitere Informationen finden Sie unter CTX118618.

Einstellungen der Richtlinie "Sitzungslimits"

August 18, 2021

Der Abschnitt Sitzungslimits enthält Richtlinieneinstellungen, die steuern, wie lange Sitzungen verbunden bleiben, bevor sie sich abmelden müssen.

> **Wichtig:**
>
> Die in diesem Artikel beschriebenen Einstellungen gelten nicht für VDAs für Windows Server. Weitere Informationen zum Konfigurieren von Sitzungszeitlimits für Server-VDAs finden Sie in der Microsoft-KB unter Session Time Limits.

Timer für getrennte Sitzung

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, der angibt, wie lange ein getrennter, gesperrter Desktop gesperrt bleibt, bevor die Sitzung abgemeldet wird. Wenn der Timer aktiviert ist, wird die getrennte Sitzung abgemeldet, wenn die Zeit abgelaufen ist.

Standardmäßig werden getrennte Sitzungen nicht abgemeldet.

Getrennte Sitzungen - Timerintervall

Mit dieser Einstellung legen Sie fest, wie viele Minuten ein getrennter, gesperrter Desktop gesperrt bleibt, bevor die Sitzung abgemeldet wird.

Standardmäßig sind es 1440 Minuten (24 Stunden).

Sitzungsverbindungstimer

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, mit dem die maximale Dauer einer ununterbrochenen Sitzung zwischen einem Benutzergerät und einem Desktop festgelegt wird. Wenn dieser Timer aktiviert ist, wird eine Sitzung getrennt oder abgemeldet, wenn der Timer abläuft. Die Microsoft-Einstellung **Sitzung beenden, wenn Zeitlimit erreicht wird** bestimmt den nächsten Status der Sitzung.

Standardmäßig ist dieser Timer aktiviert.

Sitzungsverbindung - Timerintervall

Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Desktop in Minuten fest.

Standardmäßig ist die maximale Dauer 1440 Minuten (24 Stunden).

Sitzungsleerlauftimer

Mit dieser Einstellung aktivieren oder deaktivieren Sie einen Timer, der angibt, wie lange eine ununterbrochene Benutzergeräteverbindung mit einem Desktop erhalten bleibt, wenn keine Benutzereingaben stattfinden. Wenn dieser Timer abläuft, wird die Sitzung getrennt und der **Timer für getrennte Sitzung** angewendet. Wenn der **Timer für getrennte Sitzung** deaktiviert ist, wird die Sitzung abgemeldet.

Standardmäßig ist dieser Timer deaktiviert.

Sitzungsleerlauf - Timerintervall

Diese Einstellung legt fest, wie viele Minuten eine ununterbrochene Verbindung zwischen einem Benutzergerät und einem Desktop aufrechterhalten wird, wenn keine Eingabe vom Benutzer erfolgt.

Standardmäßig bleiben Leerlaufsitzungen 1440 Minuten (24 Stunden) erhalten.

Einstellungen der Richtlinie "Sitzungszuverlässigkeit"

March 3, 2022

Der Abschnitt "Sitzungszuverlässigkeit"enthält Richtlinieneinstellungen zum Verwalten von Verbindungen, für die die Sitzungszuverlässigkeit verwendet wird.

Sitzungszuverlässigkeit - Verbindungen

Mit dieser Einstellung legen Sie fest, ob Sitzungen bei dem Verlust der Netzwerkkonnektivität offen bleiben sollen. Die automatische Wiederverbindung von Clients und die Sitzungszuverlässigkeit ermöglichen Benutzern, nach einer Netzwerkunterbrechung automatisch wieder eine Verbindung mit ihren Citrix Receiver-Sitzungen herzustellen. Standardmäßig ist die Sitzungszuverlässigkeit zugelassen.

Die Einstellungen in Citrix Studio werden auf dem Client für Folgendes durchgesetzt:

- Citrix Workspace-App 1808 und später
- Citrix Receiver für Windows 4.7 und höher

Die Citrix Studio-Richtlinie überschreibt das Citrix Receiver-Gruppenrichtlinienobjekt auf den Clients. Bei Änderungen an diesen Richtlinien in Studio wird die Sitzungszuverlässigkeit vom Server an den Client synchronisiert.

> **Hinweis:**
>
> - Citrix Receiver für Windows 4.7 und höher und Citrix Workspace-App für Windows: Stellen Sie die Richtlinie in Studio ein.
> - Citrix Receivers für Windows vor 4.7 —Legen Sie die Richtlinie in Studio fest. Legen Sie außerdem die Citrix Receiver-Gruppenrichtlinienobjektvorlage auf dem Client fest, um ein konsistentes Verhalten zu erzielen.

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkverbindung unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf dem Server aktiv. Als Hinweis darauf, dass die Verbindung unterbrochen wird, wird die Anzeige opak. Der Benutzer sieht während der Unterbrechung möglicherweise eine eingefrorene Sitzung. Der Benutzer kann die Interaktion mit der Anwendung fortsetzen, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

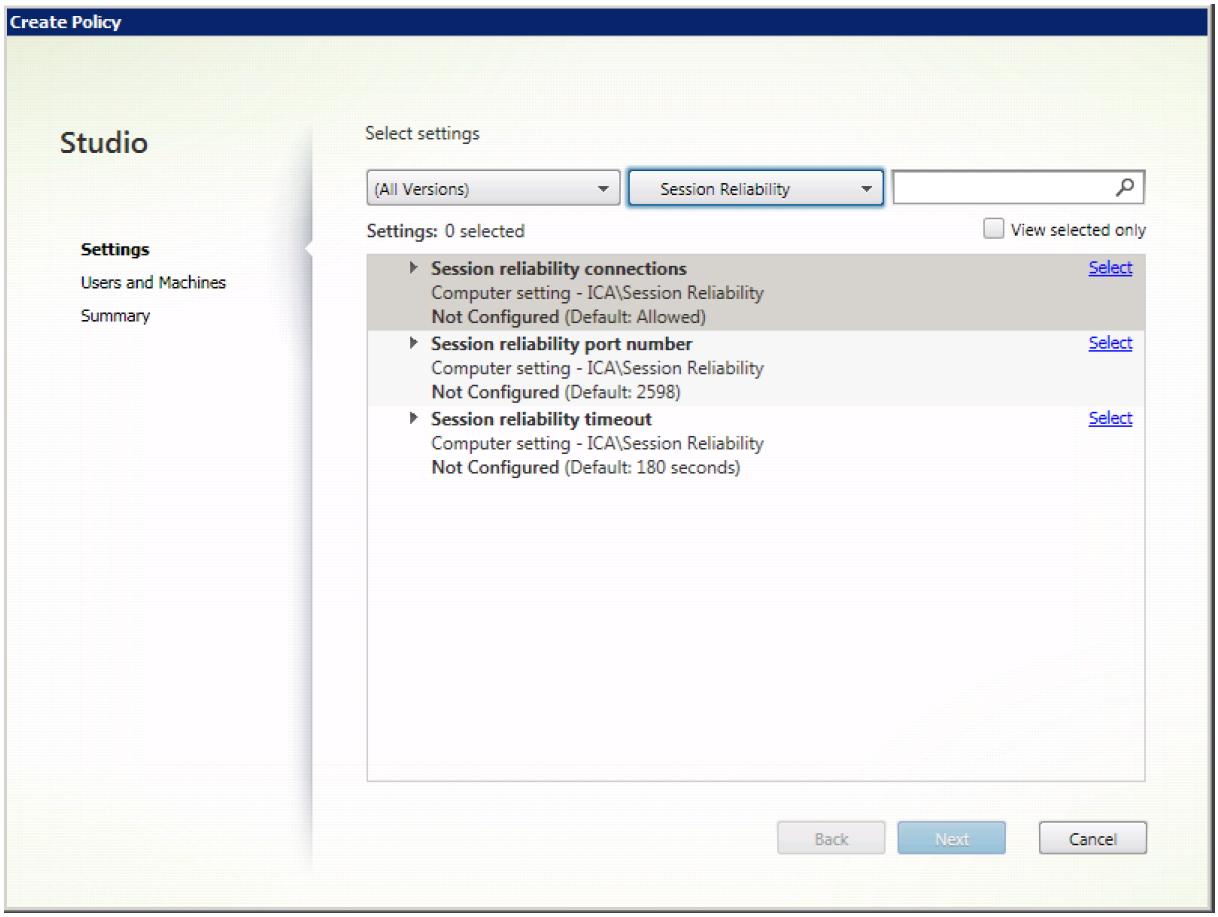
Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, nachdem der mit der Option Sitzungszuverlässigkeit - Timeout festgelegte Zeitraum abgelaufen ist. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, die Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

Standardmäßig ist die Sitzungszuverlässigkeit zugelassen.

> **Hinweis:**
>
> Wenn Citrix ADC verwendet wird, müssen Sie **Sitzungszuverlässigkeit aktivieren** in Citrix StoreFront unter **Citrix Gateways verwalten**/**Secure Ticket Authority** auswählen, um es als Proxy für ICA-Verbindungen einzustellen.

Deaktivieren der Sitzungszuverlässigkeit

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Verbindungen**.
3. Legen Sie für die Richtlinie **Nicht zugelassen** fest.



Sitzungszuverlässigkeit –Portnummer

Mit dieser Einstellung geben Sie die TCP-Portnummer für eingehende Sitzungszuverlässigkeitsverbindungen an.

Die Standardeinstellung der Portnummer ist “2598”.

Ändern der Portnummer für die Sitzungszuverlässigkeit

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Portnummer**.
3. Bearbeiten Sie die Portnummer.
4. Klicken Sie auf **OK**.

Sitzungszuverlässigkeit - Timeout

Diese Einstellung legt die Zeitspanne in Sekunden fest. Zu diesem Zeitpunkt wartet der Sitzungszuverlässigkeitsproxy darauf, dass ein Benutzer die Verbindung wiederherstellt, bevor das Trennen der Sitzung zugelassen wird.

Sie können zwar eine Sitzung länger offen lassen, dies ist jedoch eine Komfortfunktion und der Benutzer wird nicht zu einer Neuauthentifizierung aufgefordert. Je länger eine Sitzung geöffnet bleibt, umso größer ist das Risiko, dass ein Benutzer sein Gerät unbeaufsichtigt lässt und unbefugte Benutzer Zugang erhalten.

Die Standardeinstellung des Timeouts ist 180 Sekunden (drei Minuten).

Ändern des Timeouts für die Sitzungszuverlässigkeit

1. Starten Sie Citrix Studio.
2. Öffnen Sie die Richtlinie **Sitzungszuverlässigkeit - Timeout**.
3. Bearbeiten Sie den Wert für das Timeout.
4. Klicken Sie auf **OK**.

Einstellungen der Richtlinie "Zeitzonensteuerung"

November 29, 2018

Der Abschnitt "Zeitzonensteuerung"enthält Richtlinieneinstellungen für die Zeitzone in Sitzungen.

Lokale Zeitzone für Legacyclients schätzen

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Schätzen der lokalen Zeitzone auf Clientgeräten, die falsche Zeitzoneninformationen an den Server senden.

Standardmäßig schätzt der Server die lokale Zeitzone, wenn erforderlich.

Diese Einstellung ist für die Verwendung mit älteren Citrix Receiver-Versionen oder ICA- Clients vorgesehen, die keine detaillierten Zeitzoneninformationen an den Server senden. Bei Verwendung mit Citrix Receiver-Versionen, die detaillierte Zeitzoneninformationen an den Server senden, beispielsweise die unterstützten Versionen von Citrix Receiver für Windows, hat diese Einstellung keine Auswirkung.

Lokale Zeit des Clients verwenden

Mit dieser Einstellung legen Sie die Zeitzoneneinstellung der Benutzersitzung fest. Dies kann entweder die Zeitzone der Sitzung des Benutzers oder die des Benutzergeräts sein.

Standardmäßig wird die Zeitzone der Sitzung des Benutzers verwendet.

Damit diese Einstellung wirksam wird, aktivieren Sie die Einstellung Zeitzonenumleitung zulassen im Gruppenrichtlinien-Editor (Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Remotesitzungsumgebung > Geräte- und Ressourcenumleitung).

Einstellungen der Richtlinie "TWAIN-Geräte"

August 13, 2020

Der Abschnitt "TWAIN-Geräte"enthält Richtlinieneinstellungen für die Zuordnung von TWAIN-Geräten, wie Digitalkameras oder Scanner, und für das Optimieren der Bildübertragung vom Server zum Client.

> **Hinweis:**
>
> TWAIN 2.0 wird mit Citrix Receiver für Windows 4.5 unterstützt.

TWAIN-Geräteumleitung für Client

Mit dieser Einstellung legen Sie fest, ob Benutzer auf TWAIN-Geräte auf dem Benutzergerät aus Bildverarbeitungsanwendungen auf Servern zugreifen können. Standardmäßig ist die TWAIN-Geräteumleitung zugelassen.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- TWAIN-Komprimierungsgrad
- Bandbreitenlimit für TWAIN-Geräteumleitung
- Bandbreitenlimit für TWAIN-Geräteumleitung (Prozent)

> **Hinweis:**
>
> Die TWAIN-Umleitung wird nicht unterstützt, wenn Sie 64-Bit-Anwendungen verwenden.

TWAIN-Komprimierungsgrad

Mit dieser Einstellung geben Sie den Komprimierungsgrad für Bildübertragungen vom Client zum Server an. Verwenden Sie Gering für die beste Bildqualität, Mittel für eine gute Bilderqualität und Hoch für eine geringe Bildqualität. Standardmäßig wird die mittlere Komprimierung angewendet.

Einstellungen der Richtlinie “USB-Geräte”

December 31, 2019

Der Abschnitt USB-Geräte enthält Richtlinieneinstellungen für die Verwaltung der Dateiumleitung bei USB-Geräten.

Regeln für die Client-USB-Geräteoptimierung

Regeln für die Client-USB-Geräteoptimierung können auf Geräte angewendet werden, um die Optimierung zu deaktivieren oder den Optimierungsmodus zu ändern.

Wenn ein Benutzer ein USB-Gerät anschließt, prüft der Host, ob das Gerät gemäß den USB-Richtlinieneinstellungen zulässig ist. Ist das Gerät zulässig, prüft der Host die **Regeln für die Client-USB-Geräteoptimierung** für das Gerät. Wenn keine Regel angegeben wird, wird das Gerät nicht optimiert. Aufnahmemodus (04) ist der empfohlene Modus für Signaturgeräte. Für andere Geräte, deren Leistung bei höheren Latenzen beeinträchtigt wird, können Administratoren “Interaktiver Modus (02)”aktivieren. Eine Beschreibung der Modi finden Sie unten.

Nützliche Info

- Für die Verwendung von Wacom Signatur-Tablets empfiehlt Citrix, dass Sie den Bildschirmschoner deaktivieren. Anweisungen hierzu finden Sie am Ende dieses Abschnitts.
- Unterstützung für die Optimierung von Wacom-Signatur-Tablets der STU-Reihe ist in der Installation von Richtlinien bei XenApp und XenDesktop vorkonfiguriert.
- Signaturgeräte funktionieren lückenlos in XenApp und XenDesktop und erfordern zur Verwendung als Signaturgerät keine Treiber. Wacom bietet zusätzliche Software an, die zur weiteren Anpassung des Geräts installiert werden kann. Siehe https://www.wacom.com/.
- Grafiktablets: Bestimmte Grafik-Eingabegeräte werden als HID-Gerät an einem PCI/ACPI-Bus präsentiert und nicht unterstützt. Diese Geräte müssen an einen USB-Hostcontroller auf dem Client angeschlossen werden, damit sie innerhalb der XenDesktop-Sitzung umgeleitet werden.

Richtlinienregeln haben das Format von durch Leerzeichen getrennten Tag=Wert-Ausdrücken. Die folgenden Tags werden unterstützt:

Tagname	Beschreibung
Modus	Der Optimierungsmodus wird für Eingabegeräte der Klasse 3 (class=03) unterstützt. Unterstützte Modi sind: keine Optimierung –Wert 01. Interaktiver Modus: Wert 02. Empfohlen für Geräte wie Stift-Tablets und 3D Pro-Mäuse. Erfassungsmodus: Wert 04. Vorzugsmodus für Signatur-Tablets und ähnliche Geräte.
VID	Hersteller-ID aus dem Gerätedeskriptor als vierstellige Hexadezimalzahl.
PID	Produkt-ID aus dem Gerätedeskriptor als vierstellige Hexadezimalzahl.
REV	Revisions-ID aus dem Gerätedeskriptor als vierstellige Hexadezimalzahl.
Klasse	Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor
SubClass	Unterklasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder einem Schnittstellendeskriptor

Beispiele

Mode=00000004 VID=067B PID=1230 class=03 (Eingabegerät im Erfassungsmodus)

Mode=00000002 VID=067B PID=1230 class=03 (Eingabegerät im interaktiven Modus, Standardeinstellung)

Mode=00000001 VID=067B PID=1230 class=03 (Eingabegerät ohne Optimierung)

Mode=00000100 VID=067B PID=1230 (Setupoptimierung deaktiviert, Standardeinstellung)

Mode=00000200 VID=067B PID=1230 (Setupoptimierung aktiviert)

Deaktivieren des Bildschirmschoners für Wacom Signatur-Tablets

Für die Verwendung von Wacom Signatur-Tablets empfiehlt Citrix, den Bildschirmschoner wie folgt deaktivieren:

1. Installieren Sie den **Wacom-STU-Treiber**, nachdem Sie das Gerät umgeleitet haben.

2. Installieren Sie das **Wacom-STU-Display-MSI**, um Zugriff auf die Systemsteuerung des Signatur-Tablets zu erhalten.
3. Navigieren Sie zu **Control Panel > Wacom STU Display > STU430** oder **STU530** und wählen Sie die Registerkarte für das jeweilige Modell aus.
4. Klicken Sie auf **Change** und wählen Sie **Yes**, wenn das Dialogfeld bezüglich der UAC-Sicherheit angezeigt wird.
5. Wählen Sie **Disable slideshow** und klicken Sie auf **Apply**.

Wenn die Einstellung für ein Signatur-Tabletmodell festgelegt ist, wird sie auf alle Modelle angewendet.

Client-USB-Geräteumleitung

Mit dieser Einstellung legen Sie fest, ob die Umleitung von USB-Geräten zu und von Benutzergeräten zulässig ist.

Standardmäßig werden USB-Geräte nicht umgeleitet.

Regeln für die Client-USB-Geräteumleitung

Mit dieser Einstellung legen Sie die Umleitungsregeln für USB-Geräte fest.

In der Standardeinstellung sind keine Regeln angegeben.

Schließt ein Benutzer ein USB-Gerät an, prüft das Hostgerät jede Richtlinienregel, bis eine Übereinstimmung vorliegt. Die erste Übereinstimmung für ein beliebiges Gerät ist entscheidend. Ist es eine Zulassen-Regel, wird das Gerät an den virtuellen Desktop weitergeleitet. Ist es eine Ablehnungsregel, kann das Gerät nur auf dem lokalen Desktop verwendet werden. Wenn keine Übereinstimmung gefunden wird, werden die Standardregeln verwendet.

Richtlinienregeln haben das Format {Allow: | Deny:} plus Tag=Wert, durch Leerzeichen getrennt. Die folgenden Tags werden unterstützt:

Tagname	Beschreibung
VID	Hersteller-ID aus dem Gerätedeskriptor als vierstellige Hexadezimalzahl.
PID	Produkt-ID aus dem Gerätedeskriptor als vierstellige Hexadezimalzahl.
REL	Release-ID aus dem Gerätedeskriptor als vierstellige Hexadezimalzahl.

Tagname	Beschreibung
Klasse	Klasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor
SubClass	Unterklasse vom Gerätedeskriptor oder einem Schnittstellendeskriptor
Prot	Protokoll vom Gerätedeskriptor oder einem Schnittstellendeskriptor

Wenn Sie neue Richtlinienregeln erstellen, beachten Sie Folgendes:

- Bei Regeln wird die Groß- und Kleinschreibung nicht berücksichtigt.
- Regeln können optional von einen Kommentar gefolgt werden, der mit # eingeleitet wird.
- Leere Zeilen und Kommentare werden ignoriert.
- Tags müssen den Übereinstimmungsoperator = verwenden, z. B. VID=067B_.
- Jede Regel muss auf einer neuen Zeile beginnen oder Teil einer durch Semikolon getrennten Liste sein.
- USB-Klassencodes finden Sie auf der Website von USB Implementers Forum, Inc.

Beispiel für administratordefinierte USB-Richtlinienregeln:

- Allow: VID=067B PID=0007 # ANOther Industries, ANOther Flash Drive
- Deny: Class=08 SubClass=05 # Massenspeichergeräte
- Eine Regel, die alle USB-Geräte verweigert, erstellen Sie mit "DENY:"ohne weitere Tags.

Client-USB-Geräteumleitung für Plug & Play-Geräte

Mit dieser Einstellung legen Sie fest, ob Plug & Play-Geräte, wie Kameras oder POS-Geräte (Point of Sale) in einer Clientsitzung verwendet werden können.

In der Standardeinstellung ist die Umleitung von Plug & Play-Geräten zugelassen. Bei der Einstellung Zugelassen werden alle Plug & Play-Geräte für einen bestimmten Benutzer oder eine bestimmte Benutzergruppe umgeleitet. Bei der Einstellung Nicht zugelassen werden keine Geräte umgeleitet.

Einstellungen der Richtlinie "Visuelle Anzeige"

August 18, 2021

Der Abschnitt "Visuelle Anzeige"enthält Richtlinieneinstellungen, mit denen die Qualität der von virtuellen Desktops an das Benutzergerät gesendeten Bilder gesteuert wird.

Bevorzugte Farbtiefe für einfache Grafiken

Diese Richtlinieneinstellung ist in VDAs ab Version 7.6 FP3 verfügbar. Die 8-Bit-Option ist in VDA-Versionen ab 7.12 verfügbar.

Mit dieser Einstellung können Sie für die Übertragung einfacher Grafiken über das Netzwerk eine geringere Farbtiefe wählen. Eine Verringerung der Farbtiefe auf 8 oder 16 Bit pro Pixel verbessert unter geringen Bildqualitätseinbußen die Reaktion bei Verbindungen mit geringer Bandbreite. Die 8-Bit-Farbtiefe wird nicht unterstützt, wenn die Richtlinieneinstellung "Videocodec zur Komprimierung verwenden"auf Für den gesamten Bildschirm festgelegt ist.

Die Standardeinstellung für die Farbtiefe ist 24 Bits pro Pixel.

Wird die Einstellung von 8-Bit auf VDAs bis Version 7.11 angewendet, erfolgt automatisch eine Rückstellung auf 24 Bit (Standard).

Frameratesollwert

Mit dieser Einstellung geben Sie die maximale Anzahl von Frames pro Sekunde an, die vom virtuellen Desktop zum Benutzergerät gesendet werden.

In der Standardeinstellung ist die Höchstanzahl 30 Frames pro Sekunde.

Die Festlegung auf eine hohe Anzahl von Frames pro Sekunde (z. B. 30) führt zu einer besseren Benutzererfahrung, erfordert aber mehr Bandbreite. Wenn Sie die Anzahl von Frames pro Sekunde herabsetzen (z. B. auf 10), wird die Serverskalierbarkeit auf Kosten der Benutzererfahrung erhöht. Bei Benutzergeräten mit langsamen CPUs erzielen Sie durch Festlegen eines niedrigeren Werts eine bessere Benutzererfahrung.

Die maximal unterstützte Framerate pro Sekunde ist 60.

Bildqualität

Mit dieser Einstellung legen Sie die Bildqualität für auf dem Benutzergerät angezeigte Bilder fest.

Die Standardeinstellung ist "Mittel".

Zum Festlegen der Bildqualität wählen Sie eine der folgenden Optionen:

- **Niedrig:** empfohlen für Netzwerke mit eingeschränkter Bandbreite, bei denen zugunsten der Interaktivität auf hohe optische Qualität verzichtet werden kann.
- **Mittel:** bietet die beste Leistung und Bandbreiteneffizienz in den meisten Anwendungsfällen.
- **Hoch:** empfiehlt sich, wenn visuell verlustfreie Bildqualität gewünscht wird.

- **Zu verlustfrei verbessern**: sendet verlustreiche Bilder in Zeiträumen mit hoher Netzwerkaktivität und verlustfreie Bilder bei verringerter Netzwerkaktivität an das Benutzergerät. Mit dieser Einstellung wird die Leistung bei Netzwerkverbindungen mit beschränkter Bandbreite verbessert.
- **Immer verlustfrei:** In Situationen, in denen kein Qualitätsverlust akzeptabel ist (z. B. bei der Anzeige von Röntgenbildern), wählen Sie "Immer verlustfrei", um sicherzustellen, dass keine verlustreichen Daten an das Benutzergerät gesendet werden.

Wenn die Einstellung**Legacygrafikmodus** aktiviert ist, hat die Einstellung**Bildqualität** keine Auswirkungen in der Richtlinie.

Einstellungen der Richtlinie "Bewegtbilder"

February 22, 2019

Der Abschnitt "Bewegtbilder"enthält Einstellungen, mit denen Sie die Komprimierung für dynamische Bilder entfernen oder ändern können.

Mindestbildqualität

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung wird die zulässige Mindestbildqualität für den adaptiven Bildschirm angegeben. Je geringer die verwendete Komprimierung ist, desto höher ist die Qualität der angezeigten Bilder. Es stehen folgende Komprimierungen zur Verfügung: Ultrahoch, Sehr hoch, Hoch, Normal und Niedrig.

Die Standardeinstellung ist "Normal".

Bewegtbildkomprimierung

Mit dieser Einstellung wird angegeben, ob der adaptive Bildschirm aktiviert ist. Der adaptive Bildschirm passt die Bildqualität von Videos und Bildübergängen in Bildschirmpräsentationen auf der Grundlage der verfügbaren Bandbreite automatisch an. Bei aktiviertem adaptivem Bildschirm werden Benutzern gleichmäßig ausgeführte Präsentationen ohne Qualitätseinbußen angezeigt.

Standardmäßig ist der adaptive Bildschirm aktiviert.

Bei VDAs der Version 7.0 bis 7.6 gilt diese Einstellung nur, wenn der Legacygrafikmodus aktiviert ist. Bei VDAs ab Version 7.6 FP1 gilt diese Einstellung, wenn der Legacygrafikmodus aktiviert ist oder wenn

der Legacygrafikmodus deaktiviert ist und kein Videocodec zum Komprimieren von Grafiken verwendet wird.

Wenn der Legacygrafikmodus aktiviert ist, muss die Sitzung neu gestartet werden, damit die Richtlinienänderungen wirksam werden. Adaptive Anzeige und progressive Anzeige schließen einander aus, d. h. durch Aktivieren der adaptiven Anzeige wird die progressive Anzeige deaktiviert und umgekehrt. Allerdings können progressive und adaptive Anzeige zur gleichen Zeit deaktiviert sein. Die progressive Anzeige wird als Legacyfeature für XenApp und XenDesktop nicht empfohlen. Durch Festlegen des Schwellenwerts für die progressive Komprimierung wird die adaptive Anzeige deaktiviert.

Grad der progressiven Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung wird zuerst ein weniger detailliertes Bild angezeigt, das dafür aber schneller dargestellt werden kann.

In der Standardeinstellung wird keine progressive Komprimierung angewendet.

Sobald es verfügbar ist, wird ein detailreicheres Bild anzeigt, das die normale Einstellung für verlustreiche Komprimierung verwendet. Verwenden Sie sehr hohe oder ultrahohe Komprimierung für die verbesserte Anzeige von bandbreitenintensiven Grafiken, wie etwa Fotografien.

Die progressive Komprimierung ist nur wirksam, wenn der Komprimierungsgrad höher ist als die Einstellung für den Grad der verlustreichen Komprimierung.

Hinweis: Der stärkere Komprimierungsgrad für die progressive Komprimierung verbessert auch die Interaktivität von dynamischen Bildern über Clientverbindungen. Die Qualität eines dynamischen Bilds, z. B. ein sich drehendes dreidimensionales Modell, wird temporär verringert, bis das Bild stehen bleibt. Zu dem Zeitpunkt wird dann die reguläre Einstellung der verlustreichen Komprimierung angewendet.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Schwellenwert für progressive Komprimierung
- Progressive Heavyweight-Komprimierung

Schwellenwert für progressive Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, auf die progressive Komprimierung angewendet wird. Die Komprimierung wird nur für Clientverbindungen unter diesem Bandbreitenwert verwendet.

Der Standardschwellenwert ist 2147483647 Kilobits pro Sekunde.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Schwellenwert für progressive Komprimierung
- Progressive Heavyweight-Komprimierung

Mindestframeratesollwert

Mit dieser Einstellung wird die Framerate pro Sekunde eingestellt, die das System für dynamische Bilder in Netzwerken mit geringer Bandbreite versucht beizubehalten.

Die Standardeinstellung für diesen Parameter ist 10 F/s.

Bei VDAs der Version 7.0 bis 7.6 gilt diese Einstellung nur, wenn der Legacygrafikmodus aktiviert ist. Bei VDAs ab Version 7.6 FP1 gilt diese Einstellung, wenn der Legacygrafikmodus deaktiviert oder aktiviert ist.

Einstellungen der Richtlinie "Standbilder"

November 29, 2018

Der Abschnitt "Standbilder"enthält Einstellungen, mit denen Sie die Komprimierung für statische Bilder entfernen oder ändern können.

Zusätzliche Farbkomprimierung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Verwendung der zusätzlichen Farbkomprimierung für Bilder, die über Clientverbindungen mit beschränkter Bandbreite bereitgestellt werden; dies verbessert die Reaktionszeit, da die Bilder in geringerer Qualität angezeigt werden.

Standardmäßig ist die zusätzliche Farbkomprimierung deaktiviert.

Bei Aktivierung wird die zusätzliche Farbkomprimierung nur angewendet, wenn die Bandbreite der Clientverbindung unter dem für Schwellenwert für zusätzliche Farbkomprimierung festgelegten Wert liegt. Wenn die Bandbreite der Clientverbindung über dem Schwellenwert liegt oder Deaktiviert ausgewählt ist, wird die zusätzliche Farbkomprimierung nicht angewendet.

Schwellenwert für zusätzliche Farbkomprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, unter der die zusätzliche Farbkomprimierung angewendet wird. Wenn die Bandbreite der Clientverbindung unter den eingestellten Wert abfällt, wird die zusätzliche Farbkomprimierung (falls aktiviert) angewendet.

Der Standardschwellenwert ist 8192 Kilobits pro Sekunde.

Heavyweight-Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung reduzieren Sie die erforderliche Bandbreite noch stärker als mit der progressiven Komprimierung, ohne dabei an Bildqualität zu verlieren, indem ein verbesserter grafischer Algorithmus verwendet wird, der aber mehr CPU beansprucht.

Standardmäßig ist die Heavyweight-Komprimierung deaktiviert.

Wenn die Heavyweight-Komprimierung aktiviert ist, gilt sie für alle verlustreichen Komprimierungen. Diese Einstellung wird von Citrix Receiver unterstützt, hat aber keine Auswirkung auf andere Plug-Ins.

Die folgenden Richtlinieneinstellungen hängen zusammen:

- Grad der progressiven Komprimierung
- Schwellenwert für progressive Komprimierung

Grad der verlustreichen Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung steuern Sie den Grad der verlustreichen Komprimierung, der für Grafiken verwendet wird, die über Clientverbindungen mit beschränkter Bandbreite bereitgestellt werden. In solchen Fällen kann die Anzeige von Bildern ohne Komprimierung sehr langsam sein.

Standardmäßig wird eine mittlere Komprimierung ausgewählt.

Bessere Reaktionszeiten bei bandbreitenintensiven Bildern erzielen Sie mit hoher Komprimierung. In Fällen, in denen die Bilddaten erhalten bleiben müssen, beispielsweise bei der Anzeige von Röntgen-

bildern, wo kein Qualitätsverlust akzeptabel ist, sollten Sie die verlustreiche Komprimierung nicht einsetzen.

Verwandte Richtlinieneinstellung: Schwellenwert für verlustreiche Komprimierung

Schwellenwert für verlustreiche Komprimierung

Hinweis: Bei Virtual Delivery Agent 7.x gilt diese Richtlinieneinstellung nur, wenn die Richtlinieneinstellung Legacygrafikmodus aktiviert ist.

Mit dieser Einstellung geben Sie die maximale Bandbreite in Kilobits pro Sekunde für eine Verbindung an, auf die die verlustreiche Komprimierung angewendet wird.

Der Standardschwellenwert ist 2147483647 Kilobits pro Sekunde.

Wenn Sie die Einstellung Grad der verlustreichen Komprimierung einer Richtlinie hinzufügen, ohne einen Schwellenwert anzugeben, kann sich dadurch die Anzeigegeschwindigkeit für detailreiche Bitmaps, wie Fotografien, über ein LAN verbessern.

Verwandte Richtlinieneinstellung: Grad der verlustreichen Komprimierung

Einstellungen der Richtlinie "WebSockets"

August 18, 2021

Der Abschnitt "WebSockets"enthält Richtlinieneinstellungen für den Zugriff auf virtuelle Desktops und gehostete Anwendungen mit Citrix Receiver für HTML5. Das Feature WebSockets erhöht die Sicherheit und verringert die Last durch bidirektionale Kommunikation zwischen browserbasierten Anwendungen und Servern ohne Öffnen von mehreren HTTP-Verbindungen.

WebSockets-Verbindungen

Diese Einstellung lässt WebSockets-Verbindungen zu oder lehnt sie ab.

Standardmäßig sind WebSocket-Verbindungen nicht zulässig.

WebSockets-Portnummer

Mit dieser Einstellung wird der Port für eingehende WebSocket-Verbindungen festgelegt.

Standardmäßig ist der Wert 8008.

Vertrauenswürdige WebSockets-Ursprungsserverliste

Diese Einstellung bietet eine durch Trennzeichen getrennte Liste der vertrauenswürdigen Ursprungsserver, normalerweise Citrix Receiver für Web, in Form von URLs. Nur WebSockets-Verbindungen, die von einer dieser Adressen stammen, werden vom Server akzeptiert.

Standardmäßig wird der Platzhalter * verwendet. Damit wird allen Citrix Receiver für Web-URLs vertraut.

Wenn Sie eine Adresse in die Liste eingeben möchten, verwenden Sie folgende Syntax:

```
<protocol>://<Fully qualified domain name of host>:[port]
```

Das Protokoll muss HTTP oder HTTPS sein. Wenn der Port nicht angegeben wird, wird Port 80 für HTTP und Port 443 für HTTPS verwendet.

Der Platzhalter *kann innerhalb der URL verwendet werden, außer als Teil einer IP-Adresse (10.105.**).

Einstellungen der Richtlinie "Lastverwaltung"

August 18, 2021

Der Abschnitt "Lastverwaltung"enthält Richtlinieneinstellungen für das Aktivieren und Konfigurieren des Lastausgleichs zwischen Servern, über die Windows Server-Betriebssystemmaschinen bereitgestellt werden.

Weitere Informationen zum Berechnen des Lastauswertungsindex finden Sie unter CTX202150.

Toleranzwert für gleichzeitige Anmeldungen

Mit dieser Einstellung geben Sie die maximal zulässige Anzahl gleichzeitiger Anmeldungen bei einem Server an.

Die Standardeinstellung ist 2.

Wenn diese Einstellung aktiviert ist, wird durch den Lastausgleich versucht, die Anzahl gleichzeitig aktiver Anmeldungen an einem Server-VDA auf den festgelegten Höchstwert zu begrenzen. Das Limit wird jedoch nicht zwingend angewendet. Um zu erzwingen, dass nach Erreichen des angegebenen Höchstwerts weitere Anmeldeversuche fehlschlagen, erstellen Sie folgenden Registrierungsschlüssel:

HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
Typ: DWORD
Wert: 1

CPU-Nutzung

Mit dieser Einstellung geben Sie den Prozentsatz der CPU-Nutzung an, bei dem der Server Volllast meldet. Ist diese Einstellung aktiviert, beträgt der Standardwert, bei dem der Server Volllast meldet, 90 %.

Standardmäßig ist diese Einstellung deaktiviert und die CPU-Nutzung wird bei der Lastberechnung nicht berücksichtigt.

CPU-Nutzung ausschließlich Prozesspriorität

Mit dieser Einstellung geben Sie die Prioritätsstufe an, bei der die Prozess-CPU-Auslastung vom Lastindex der CPU-Nutzung ausgeschlossen wird.

Die Standardeinstellung ist Unter normal oder Niedrig.

Datenträgernutzung

Mit dieser Einstellung geben Sie die Länge der Datenträgerwarteschlange an, zu der der Server 75 % Volllast meldet. Der Standardwert dieser Einstellung ist 8.

Standardmäßig ist diese Einstellung deaktiviert und die Datenträgernutzung wird bei der Lastberechnung nicht berücksichtigt.

Sitzungshöchstanzahl

Mit dieser Einstellung geben Sie die maximale Anzahl von Sitzungen an, die von einem Server gehostet werden können. Ist die Einstellung aktiviert, ist der Standardwert für die maximale Anzahl Sitzungen, die von einem Server gehostet werden können, 250.

Standardmäßig ist diese Einstellung aktiviert.

Speichernutzung

Mit dieser Einstellung geben Sie den Prozentsatz der Speichernutzung an, bei dem der Server Volllast meldet. Ist diese Einstellung aktiviert, beträgt der Standardwert, bei dem der Server Volllast meldet, 90 %.

Standardmäßig ist diese Einstellung deaktiviert und die Speichernutzung wird bei der Lastberechnung nicht berücksichtigt.

Speichernutzung - Ausgangslast

Mit dieser Einstellung geben Sie einen Näherungswert der Speichernutzung durch das Basisbetriebssystem in MB an, unterhalb dessen die Speichernutzung bei einem Server als Nulllast interpretiert wird.

Standardmäßig sind dies 768 MB.

Einstellungen der Richtlinie "Profilverwaltung"

May 18, 2020

Der Abschnitt "Profilverwaltung"enthält Richtlinieneinstellungen zum Aktivieren der Profilverwaltung und zum Konfigurieren der Gruppen, die in die Verarbeitung der Profilverwaltung eingeschlossen bzw. ausgeschlossen werden sollen.

Weitere Informationen, wie die Namen der entsprechenden INI-Dateieinstellungen und die für eine Richtlinieneinstellung erforderliche Version der Profilverwaltung, finden Sie unter Profilverwaltungsrichtlinien.

Erweiterte Richtlinieneinstellungen

August 18, 2021

Der Abschnitt "Erweitert"enthält Richtlinieneinstellungen für die erweiterte Konfiguration der Profilverwaltung.

Automatische Konfiguration deaktivieren

Mit dieser Einstellung legen Sie fest, dass die Umgebung von der Profilverwaltung untersucht werden kann, z. B., um zu überprüfen, ob persönliche vDisks vorhanden sind, und um die Gruppenrichtlinie entsprechend zu konfigurieren. Nur Richtlinien für die Profilverwaltung mit dem Status "Nicht konfiguriert"werden angepasst, sodass alle zuvor vorgenommenen Anpassungen beibehalten werden. Dieses Feature beschleunigt die Bereitstellung und vereinfacht die Optimierung. Es ist keine Konfiguration des Features ist erforderlich aber Sie können die automatische Konfiguration bei Upgrades (zum Beibehalten der Einstellungen von früheren Versionen) oder bei der Problembehandlung deaktivieren. Die automatische Konfiguration funktioniert in XenApp oder anderen Umgebungen nicht.

Sie können die automatische Konfiguration als dynamische Konfigurationsprüfung betrachten, die die Standardrichtlinieneinstellungen automatisch zur Laufzeit entsprechend der Umgebung konfiguriert. Es entfällt die Notwendigkeit, die Einstellungen manuell zu konfigurieren. Laufzeitumgebungen enthalten:

- Windows-Betriebssystem
- Windows-Betriebssystemversionen
- Vorhandensein von Citrix Virtual Desktops
- Vorhandensein von Personal vDisks

Die automatische Konfiguration ändert möglicherweise die folgenden Richtlinien, wenn sich die Umgebung ändert:

- Aktiv zurückschreiben
- Immer zwischenspeichern
- Lokal zwischengespeicherte Profile nach Abmeldung löschen
- Verzögerung vor dem Löschen von zwischengespeicherten Profilen
- Profilstreaming

In der folgenden Tabelle finden Sie den Standardstatus der oben genannten Richtlinien für verschiedene Betriebssysteme:

	Serverbetriebssystem	Desktopbetriebssystem
Aktiv zurückschreiben	Aktiviert	*Deaktiviert*, wenn Personal vDisk verwendet wird, sonst aktiviert.
Immer zwischenspeichern	Deaktiviert	*Deaktiviert*, wenn Personal vDisk verwendet wird, sonst aktiviert.
Lokal zwischengespeicherte Profile nach Abmeldung löschen	Aktiviert	*Deaktiviert*, wenn Personal vDisk verwendet wird oder wenn Citrix Virtual Desktops zugewiesen werden oder wenn Citrix Virtual Desktops nicht installiert sind, andernfalls aktiviert.
Verzögerung vor dem Löschen von zwischengespeicherten Profilen	0 Sekunden	60 Sekunden, wenn Benutzeränderungen nicht persistent sind, andernfalls 0 Sekunden.

	Serverbetriebssystem	Desktopbetriebssystem
Profilstreaming	Aktiviert	*Deaktiviert*, wenn Personal vDisk verwendet wird, sonst aktiviert.

Wenn jedoch die automatische Konfiguration deaktiviert ist, werden alle oben genannten Richtlinien standardmäßig **deaktiviert**.

In der Standardeinstellung ist die automatische Konfiguration zugelassen.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird die automatische Konfiguration aktiviert. Einstellungen der Profilverwaltung können sich dann möglicherweise ändern, wenn sich die Umgebung ändert.

Benutzer bei Problem abmelden

Mit dieser Einstellung wird eine Abmeldung eines Benutzers durch die Profilverwaltung ermöglicht, wenn ein Problem auftritt, z. B. wenn der Benutzerspeicher nicht verfügbar ist. Wenn diese Einstellung aktiviert ist, wird dem Benutzer eine Fehlermeldung angezeigt, bevor er abgemeldet wird. Wenn diese Einstellung deaktiviert ist, erhalten Benutzer ein temporäres Profil.

Standardmäßig ist diese Einstellung deaktiviert und Benutzer erhalten ein temporäres Profil, wenn ein Problem auftritt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird ein temporäres Profil bereitgestellt.

Anzahl Wiederholungen beim Zugriff auf gesperrte Dateien

Mit dieser Einstellung geben Sie die Anzahl der Zugriffsversuche auf gesperrte Dateien durch die Profilverwaltung an.

Der Standardwert dieser Einstellung ist fünf Versuche.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Internet-Cookiedateien bei Abmeldung verarbeiten

Mit dieser Einstellung legen Sie fest, dass die Datei index.dat beim Abmelden von der Profilverwaltung verarbeitet werden kann, damit Internet-Cookies im Dateisystem nach längerem Browsen entfernt werden. Auf diese Weise wird eine Aufblähung von Profilen vermieden. Eine Aktivierung der Einstellung verlängert die Abmeldezeiten. Aktivieren Sie sie daher nur, wenn das entsprechende Problem bei Ihnen auftritt.

Standardmäßig ist diese Einstellung deaktiviert und die Profilverwaltung verarbeitet die Datei index.dat beim Abmelden nicht.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird Index.dat nicht verarbeitet.

Grundlegende Richtlinieneinstellungen

February 4, 2020

Der Abschnitt "Grundlegend"enthält Richtlinieneinstellungen für die grundlegende Konfiguration der Profilverwaltung.

Aktiv zurückschreiben

Mit dieser Einstellung können geänderte Dateien und Ordner (aber keine Registrierungseinträge) während einer Sitzung mit dem Benutzerspeicher synchronisiert werden bevor die Abmeldung erfolgt.

Standardmäßig ist die Synchronisierung mit dem Benutzerspeicher während laufender Sitzungen deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie aktiviert.

Profilverwaltung aktivieren

Mit dieser Einstellung wird die Profilverwaltung zur Verarbeitung von An- und Abmeldungen aktiviert.

Standardmäßig ist diese Einstellung deaktiviert, um die Bereitstellung zu vereinfachen.

Wichtig: Citrix empfiehlt, eine Aktivierung der Profilverwaltung erst dann durchzuführen, wenn alle anderen Setupaufgaben ausgeführt wurden und getestet wurde, wie sich Citrix Benutzerprofile in der Umgebung verhalten.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, verarbeitet die Profilverwaltung keine Windows-Benutzerprofile.

Ausgeschlossene Gruppen

Mit dieser Einstellung geben Sie an, welche lokalen Computergruppen und welche Domänengruppen (lokale, globale und universelle) nicht von der Profilverwaltung verarbeitet werden sollen.

Wenn diese Option aktiviert ist, verarbeitet die Profilverwaltung keine Mitglieder der angegebenen Benutzergruppen.

Standardmäßig ist diese Einstellung deaktiviert und Mitglieder aller Benutzergruppen werden verarbeitet.

Geben Sie Domänengruppen im Format <DOMÄNENNAME>\<GRUPPENNAME> an.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Mitglieder aller Benutzergruppen verarbeitet.

Unterstützung von Offlineprofilen

Mit dieser Einstellung wird die Unterstützung von Offlineprofilen aktiviert, durch die Profile nach einer Unterbrechung der Verbindung mit dem Netzwerk zum frühestmöglichen Zeitpunkt mit dem Benutzerspeicher synchronisiert werden.

Standardmäßig ist die Unterstützung von Offlineprofilen deaktiviert.

Diese Einstellung gilt für Benutzer von Laptops und mobile Benutzer im Roamingmodus. Wenn die Verbindung zum Netzwerk unterbrochen wird, bleiben die Profile auf dem Laptop oder Gerät intakt, selbst wenn das Gerät neu gestartet wird oder im Ruhezustand gewesen ist. Während mobile Benutzer arbeiten, werden ihre Profile lokal aktualisiert und am Ende mit dem Benutzerspeicher synchronisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist die Unterstützung von Offlineprofilen deaktiviert.

Pfad zu Benutzerspeicher

Mit dieser Einstellung geben Sie den Pfad zu dem Verzeichnis (Benutzerspeicher) an, in dem Benutzereinstellungen, z. B. Registrierungseinstellungen und synchronisierte Dateien, gespeichert werden.

Standardmäßig wird das Windows-Verzeichnis auf dem Basislaufwerk verwendet.

Wenn diese Einstellung deaktiviert ist, werden die Benutzereinstellungen im Windows-Unterverzeichnis des Basisverzeichnisses gespeichert.

Mögliche Pfade:

- **Relativer Pfad:** Dieser Pfad muss relativ zum Stammverzeichnis sein (normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert).
- **Absoluter UNC-Pfad:** Hiermit wird üblicherweise eine Serverfreigabe oder ein DFS-Namespace angegeben.
- **Deaktiviert oder nicht konfiguriert:** In diesem Fall wird als Wert #homeDirectory#\Windows angenommen.

Verwenden Sie die folgenden Variablentypen beim Konfigurieren dieser Richtlinieneinstellung:

- Systemumgebungsvariablen in Prozentzeichen (z. B. %ProfVer%). Beachten Sie, dass Systemumgebungsvariablen normalerweise weitere Einrichtung erfordern.
- Attribute des Active Directory-Benutzerobjekts in Rauten (z. B. #sAMAccountName#).
- Profilverwaltungsvariablen. Weitere Informationen finden Sie in der Dokumentation zur Profilverwaltung.

Sie können auch mit den Benutzerumgebungsvariablen %username% und %userdomain% benutzerdefinierte Attribute erstellen, um Organisationsvariablen wie Standort und Benutzer vollständig zu definieren. Bei Attributen muss Groß- und Kleinschreibung beachtet werden.

Beispiele:

- \\server\share#sAMAccountName# speichert die Benutzereinstellungen unter dem UNC-Pfad \\server\share\JohnSmith (wenn #sAMAccountName# zu JohnSmith als aktuellem Benutzer aufgelöst wird).
- \\server\profiles$%USERNAME%.%USERDOMAIN%\!CTX_PROFILEVER!!CTX_OSBITNESS! kann zu \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64 aufgelöst werden.

Wichtig: Unabhängig davon, welche Attribute oder Variablen Sie verwenden, müssen Sie sicherstellen, dass diese Einstellung zu einem Ordner über dem Ordner, der NTUSER.DAT enthält, aufgelöst wird. Ist diese Datei z. B. in \\server\profiles$\JohnSmith.Finance\v2x64\UPM_Profile, geben Sie den Pfad zum Benutzerspeicher als \\server\profiles$\JohnSmith.Finance\v2x64 an (ohne den Unterordner \UPM_Profile) an.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird das Windows-Verzeichnis auf dem Basislaufwerk verwendet.

Anmeldungen lokaler Administratoren verarbeiten

Mit dieser Einstellung wird angegeben, ob Anmeldungen von Mitgliedern der Gruppe "BUILTIN\Administrators" verarbeitet werden. Dies ermöglicht es Domänenbenutzern mit lokalen Administratorrechten, d. h. normalerweise Benutzer mit zugewiesenen virtuellen Desktops, die Verarbeitung zu umgehen, sich anzumelden und Probleme mit der Profilverwaltung bei einem Desktop zu behandeln.

Wenn diese Einstellung unter Serverbetriebssystemen deaktiviert oder nicht konfiguriert ist, nimmt die Profilverwaltung an, dass Anmeldungen von Domänenbenutzern, aber nicht von lokalen Administratoren, verarbeitet werden müssen. Unter Desktopbetriebssystemen werden Anmeldungen lokaler Administratoren verarbeitet.

Diese Einstellung ist standardmäßig deaktiviert und Anmeldungen lokaler Administratoren werden nicht verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Anmeldungen lokaler Administratoren nicht verarbeitet.

Verarbeitete Gruppen

Mit dieser Einstellung geben Sie an, welche lokalen Computergruppen und welche Domänengruppen (lokale, globale und universelle) von der Profilverwaltung verarbeitet werden sollen.

Wenn diese Option aktiviert ist, verarbeitet die Profilverwaltung nur Mitglieder der angegebenen Benutzergruppen.

Standardmäßig ist diese Einstellung deaktiviert und Mitglieder aller Benutzergruppen werden verarbeitet.

Geben Sie Domänengruppen im Format <DOMÄNENNAME><GRUPPENNAME> an.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Mitglieder aller Benutzergruppen verarbeitet.

Plattformübergreifende Richtlinieneinstellungen

November 29, 2018

Der Abschnitt "Plattformübergreifende Einstellungen"enthält Richtlinieneinstellungen für die Konfiguration der plattformübergreifenden Einstellungen der Profilverwaltung.

Benutzergruppen für plattformübergreifende Einstellungen

Mit dieser Einstellung geben Sie die Benutzergruppen an, deren Profile verarbeitet werden sollen, wenn das Feature für plattformübergreifende Einstellungen aktiviert ist.

Standardmäßig ist diese Einstellung deaktiviert und alle Benutzergruppen in der Richtlinieneinstellung Verarbeitete Gruppen werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Benutzergruppen verarbeitet.

Plattformübergreifende Einstellungen aktivieren

Mit dieser Einstellung aktivieren oder deaktivieren Sie das Feature "Plattformübergreifende Einstellungen". Dieses ermöglicht das Migrieren und Roamen von Benutzerprofilen, wenn ein Benutzer eine Verbindung mit einer Anwendung herstellt, die unter mehreren Betriebssystemen ausgeführt wird.

Standardmäßig ist das Feature "Plattformübergreifende Einstellungen"deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine plattformübergreifenden Einstellungen angewendet.

Pfad zu plattformübergreifenden Definitionen

Mit dieser Einstellung geben Sie in Form eines UNC-Pfads den Netzwerkspeicherort an, der die aus dem Downloadpaket kopierten Definitionsdateien enthält.

Hinweis: Benutzer benötigen Lesezugriff und Administratoren Schreibzugriff auf diesen Speicherort, bei dem es sich entweder um eine Server Message Block-Dateifreigabe (SMB) oder eine Common Internet File System-Dateifreigabe (CIFS) handeln muss.

In der Standardeinstellung ist kein Pfad angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine plattformübergreifenden Einstellungen angewendet.

Pfad zum Speicher für plattformübergreifende Einstellungen

Diese Einstellung gibt den Pfad zum Speicher für plattformübergreifende Einstellungen an. Hier werden die plattformübergreifenden Einstellungen der Benutzer gespeichert. Der Pfad kann ein UNC-Pfad oder ein relativer Pfad zum Basisverzeichnis sein.

Hinweis: Benutzer müssen über Schreibzugriff auf den Speicher für plattformübergreifende Einstellungen verfügen.

Standardmäßig ist diese Einstellung deaktiviert und der Pfad "Windows\PM_CP"wird verwendet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Quelle für Erstellung plattformübergreifender Einstellungen

Mit dieser Einstellung legen Sie eine Plattform als Basisplattform fest, wenn die entsprechende Einstellung für die Organisationseinheit der Plattform aktiviert ist. Daten von den Profilen der Basisplattform werden in den Speicher für plattformübergreifende Einstellungen migriert.

Die Profile jeder Plattform werden in einer separaten Organisationseinheit gespeichert. Dies bedeutet, dass Sie die Plattform auswählen müssen, deren Profildaten zum Füllen des Speichers für plattformübergreifende Einstellungen verwendet werden sollen. Dies wird als Basisplattform bezeichnet.

Wenn diese Option aktiviert ist, migriert die Profilverwaltung die Daten des Einzelplattformprofils in den Speicher, wenn der Speicher für plattformübergreifende Einstellungen eine Definitionsdatei ohne Daten enthält oder die zwischengespeicherten Daten eines Einzelplattformprofils neuer sind als die Definitionsdaten im Speicher.

Wichtig: Wenn diese Einstellung in mehreren Organisationseinheiten für mehrere Benutzer oder Maschinenobjekte aktiviert ist, wird die Plattform, bei der sich der erste Benutzer anmeldet, zum Basisprofil.

Standardmäßig ist diese Einstellung deaktiviert und die Profilverwaltung migriert die Daten des Einzelplattformprofils nicht in den Speicher.

Einstellungen der Richtlinie "Dateisystem"

November 29, 2018

Der Abschnitt "Dateisystem"enthält Richtlinieneinstellungen zum Angeben der Dateien und Verzeichnisse in einem Benutzerprofil, die zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden sollen.

Einstellungen der Richtlinie "Ausschlüsse"

November 29, 2018

Der Abschnitt "Ausschlüsse"enthält Richtlinieneinstellungen zum Konfigurieren der Dateien und Verzeichnisse in einem Benutzerprofil, die von der Synchronisierung ausgeschlossen werden sollen.

Ausschlussliste - Verzeichnisse

Mit dieser Einstellung geben Sie eine Liste der Ordner im Benutzerprofil an, die bei der Synchronisierung ignoriert werden sollen.

Geben Sie die Ordnernamen als Pfad relativ zum Benutzerprofil (% USERPROFILE%) an.

Standardmäßig ist diese Einstellung deaktiviert und alle Ordner in Benutzerprofilen werden synchronisiert.

Beispiel: Desktop ignoriert den Ordner "Desktop"im Benutzerprofil.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Ordner im Benutzerprofil synchronisiert.

Ausschlussliste - Dateien

Mit dieser Einstellung geben Sie eine Liste der Dateien im Benutzerprofil an, die bei der Synchronisierung ignoriert werden sollen.

Standardmäßig ist diese Einstellung deaktiviert und alle Dateien in Benutzerprofilen werden synchronisiert.

Geben Sie die Dateinamen als Pfad relativ zum Benutzerprofil (% USERPROFILE%) an. Hinweis: Platzhalter sind zulässig und werden rekursiv angewendet.

Beispiel: "Desktop\Desktop.ini"ignoriert die Datei Desktop.ini im Verzeichnis "Desktop".

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Dateien im Benutzerprofil synchronisiert.

Synchronisierung - Richtlinieneinstellungen

December 5, 2023

Der Abschnitt Synchronisierung enthält Richtlinieneinstellungen, um festzulegen, welche Dateien und Ordner in einem Benutzerprofil zwischen dem System, auf dem das Profil installiert ist, und dem Benutzerspeicher synchronisiert werden.

Zu synchronisierende Verzeichnisse

Diese Einstellung gibt die Verzeichnisse an, die in ausgeschlossenen Ordnern sind und von der Profilverwaltung in die Synchronisierung eingeschlossen werden sollen. Standardmäßig synchronisiert die Profilverwaltung alle Elemente im Benutzerprofil. Es ist nicht erforderlich, Unterordner des Benutzerprofils einzuschließen, indem Sie sie dieser Liste hinzufügen. Weitere Informationen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein.

Beispiel: Desktop\ausschließen\aufnehmen gibt den Unterordner "aufnehmen"des Verzeichnisses Desktop\ausschließen an.

Standardmäßig ist diese Einstellung deaktiviert und keine Ordner sind angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur nicht ausgeschlossene Ordner im Benutzerprofil synchronisiert.

Zu synchronisierende Dateien

Diese Einstellung gibt die Dateien an, die sich in ausgeschlossenen Ordnern befinden und von der Profilverwaltung in die Synchronisierung eingeschlossen werden sollen. Standardmäßig synchronisiert

die Profilverwaltung alle Elemente im Benutzerprofil. Es ist nicht erforderlich, Dateien in dem Benutzerprofil einzuschließen, indem Sie sie dieser Liste hinzufügen. Weitere Informationen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Pfade in dieser Liste müssen relativ zum Benutzerprofil sein. Relative Pfade werden als relativ zum Benutzerprofil interpretiert. Platzhalter können nur für Dateinamen verwendet werden. Platzhalter können nicht verschachtelt werden und werden rekursiv angewendet.

Beispiele:

- AppData\Local\Microsoft\Office\Access.qat gibt eine Datei unter einem Ordner an, der in der Standardkonfiguration ausgeschlossen wurde.
- AppData\Local\MyApp*.cfg gibt alle Dateien mit der Erweiterung .cfg im Profilordner Anwendungsdaten\Lokal\Anwendungen und dessen Unterordnern an.

Standardmäßig ist diese Einstellung deaktiviert und keine Dateien sind angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur nicht ausgeschlossene Dateien im Benutzerprofil synchronisiert.

Zu spiegelnde Ordner

Mit dieser Einstellung geben Sie an, welche Ordner relativ zum Stammordner eines Benutzerprofils gespiegelt werden sollen. Diese Richtlinie kann beim Lösen von Problemen bei Transaktionsordnern (auch “Referenzordner”genannt) helfen. Dies sind Ordner, die voneinander abhängige Dateien enthalten, wobei eine Datei Verweise auf andere Dateien enthält.

Durch das Spiegeln von Ordnern kann die Profilverwaltung einen Transaktionsordner und seinen Inhalt als eine Entität verarbeiten. So wird das Aufblähen von Profilen verhindert. In diesen Situationen hat der letzte Schreibvorgang Priorität, daher werden Dateien in gespiegelten Ordnern, die in mehr als einer Sitzung geändert wurden, von der letzten Aktualisierung überschrieben. Hierdurch gehen Profiländerungen verloren.

Sie können z. B. den Ordner Internet Explorer-Cookies spiegeln, damit Index.dat mit den Cookies synchronisiert wird, auf die die Datei verweist.

Wenn ein Benutzer zwei Internet Explorer-Sitzungen auf unterschiedlichen Servern hat und er in jeder Sitzung auf andere Websites zugreift, werden Cookies dieser Sites auf dem entsprechenden Server hinzugefügt. Wenn sich der Benutzer von der ersten Sitzung abmeldet (oder auch mitten in der Sitzung, wenn das Feature für aktives Zurückschreiben konfiguriert ist), sollten die Cookies der zweiten Sitzung die Cookies der ersten Sitzung ersetzen. Stattdessen werden sie jedoch zusammengeführt und die Verweise auf die Cookies in Index.dat sind infolgedessen veraltet. Weiteres

Browsen in neuen Sitzungen kann zum wiederholten Zusammenführen und einem aufgeblähten Cookie-Ordner führen.

Durch Spiegeln des Cookie-Ordners wird dieses Problem gelöst, indem Cookies, jedes Mal wenn der Benutzer sich abmeldet, mit denen der letzten Sitzung überschrieben werden. So bleibt Index.dat aktuell.

Standardmäßig ist diese Einstellung deaktiviert und es werden keine Ordner gespiegelt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Richtlinie weder hier noch in der INI-Datei konfiguriert ist, werden keine Ordner gespiegelt.

Einstellungen der Richtlinie "Ordnerumleitung"

November 29, 2018

Der Abschnitt "Ordnerumleitung"enthält Richtlinieneinstellungen für die Angabe, ob häufig in Profilen erscheinende Ordner an einen freigegebenen Speicherort im Netzwerk umgeleitet werden sollen.

Administratorzugriff gewähren

Diese Einstellung ermöglicht einem Administrator den Zugriff auf den Inhalt von umgeleiteten Ordnern der Benutzer.

Diese Einstellung ist standardmäßig deaktiviert und es haben ausschließlich Benutzer Zugriff auf den Inhalt ihrer umgeleiteten Ordner.

Domänennamen einschließen

Diese Einstellung ermöglicht die Verwendung der Umgebungsvariablen %userdomain% als Teil des für umgeleitete Ordner angegebenen UNC-Pfads.

Standardmäßig ist diese Einstellung deaktiviert und die Umgebungsvariable %userdomain% ist nicht Teil der UNC-Pfad-Angabe für umgeleitete Ordner.

Einstellungen der Richtlinie "AppData(Roaming)"

August 18, 2021

Der Abschnitt "AppData(Roaming)"enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "AppData(Roaming)"an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

AppData(Roaming)-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners AppData(Roaming) umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für AppData(Roaming)

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners AppData(Roaming) umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Kontakte"

August 18, 2021

Der Abschnitt "Kontakte"enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Kontakte"an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Kontakte'-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners Kontakte umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für ‘Kontakte’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Kontakte umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Desktop”

August 18, 2021

Der Abschnitt “Desktop”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Desktop”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

‘Desktop’-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem der Inhalt des Ordners Desktop umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für ‘Desktop’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Desktop umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Dokumente”

August 18, 2021

Der Abschnitt “Dokumente”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Dokumente”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

‘Dokumente’-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem die Dateien im Ordner Dokumente umgeleitet werden sollen.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Die Einstellung Dokumente-Pfad muss aktiviert sein, damit Dateien sowohl in den Ordner Dokumente als auch in die Ordner Musik, Bilder und Videos umgeleitet werden.

Umleitungseinstellungen für ‘Dokumente’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Dokumente umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners Dokumente umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: leitet den Inhalt zu dem in der Richtlinieneinstellung ‘Dokumente’-Pfad angegebenen UNC-Pfad.
- Zum Basisverzeichnis des Benutzers umleiten: leitet den Inhalt zu dem Basisverzeichnis des Benutzers. Dieses ist normalerweise mit dem Attribut #homeDirectory# für einen Benutzer in Active Directory konfiguriert.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Downloads”

August 18, 2021

Der Abschnitt “Downloads”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Downloads”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

‘Downloads’-Pfad

Mit dieser Einstellung geben Sie den Netzwerkspeicherort an, zu dem die Dateien im Ordner Downloads umgeleitet werden.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Downloads'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Downloads umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Favoriten"

August 18, 2021

Der Abschnitt "Favoriten"enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Favoriten"an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

'Favoriten'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Favoriten umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für 'Favoriten'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Favoriten umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Links”

August 18, 2021

Der Abschnitt “Links”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Links”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

‘Links’-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Links umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für ‘Links’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Links umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Musik”

August 18, 2021

Der Abschnitt “Musik”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Musik”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

‘Musik’-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Musik umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für ‘Musik’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Musik umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners Musik umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung ‘Musik’-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner Dokumente umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner Dokumente um.

Damit Inhalte in einen Ordner relativ zum Ordner Dokumente umgeleitet werden, muss die Einstellung ‘Dokumente’-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Bilder”

August 18, 2021

Der Abschnitt “Bilder”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Bilder”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

‘Bilder’-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Bilder umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Umleitungseinstellungen für ‘Bilder’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Bilder umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners Bilder umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung 'Bilder'-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner Dokumente umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner Dokumente um.

Damit Inhalte in einen Ordner relativ zum Ordner Dokumente umgeleitet werden, muss die Einstellung 'Dokumente'-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Gespeicherte Spiele"

August 18, 2021

Der Abschnitt "Gespeicherte Spiele"enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners "Gespeicherte Spiele"an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

Umleitungseinstellungen für 'Gespeicherte Spiele'

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Gespeicherte Spiele umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

'Gespeicherte Spiele'-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Gespeicherte Spiele umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Startmenü”

August 18, 2021

Der Abschnitt “Startmenü”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Startmenü”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

Umleitungseinstellungen für ‘Startmenü’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Startmenü umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Startmenü-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Startmenü umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Suchen”

August 18, 2021

Der Abschnitt “Suchen”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Suchen”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

Umleitungseinstellungen für ‘Suchen’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Suchen umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

‘Suchen’-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Suchen umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie “Videos”

August 18, 2021

Der Abschnitt “Videos”enthält Richtlinieneinstellungen für die Angabe, ob der Inhalt des Ordners “Videos”an einen freigegebenen Speicherort im Netzwerk umgeleitet werden soll.

Umleitungseinstellungen für ‘Videos’

Mit dieser Einstellung geben Sie an, wie der Inhalt des Ordners Videos umgeleitet werden soll.

Standardmäßig erfolgt die Umleitung an einen UNC-Pfad.

Wählen Sie eine der folgenden Optionen, um zu steuern, wie der Inhalt des Ordners Videos umgeleitet werden soll:

- Zum folgenden UNC-Pfad umleiten: Leitet den Inhalt zu dem in der Richtlinieneinstellung ‘Videos’-Pfad angegebenen UNC-Pfad.
- Relativ zum Ordner Dokumente umleiten: Leitet den Inhalt in einen Ordner relativ zu dem Ordner Dokumente um.

Damit Inhalte in einen Ordner relativ zum Ordner Dokumente umgeleitet werden, muss die Einstellung ‘Dokumente’-Pfad aktiviert sein.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

‘Videos’-Pfad

Mit dieser Einstellung geben Sie die Netzwerkfreigabe an, zu der der Inhalt des Ordners Videos umgeleitet werden soll.

Standardmäßig ist diese Einstellung deaktiviert und kein Speicherort wird angegeben.

Wenn diese Einstellung hier nicht konfiguriert ist, erfolgt keine Umleitung durch die Profilverwaltung.

Einstellungen der Richtlinie "Protokollierung"

November 29, 2018

Der Abschnitt "Protokollierung"enthält Richtlinieneinstellungen zum Konfigurieren der Protokollierung der Profilverwaltung.

Active Directory-Aktionen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der in Active Directory ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Allgemeine Informationen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung allgemeiner Informationen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Allgemeine Warnungen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung allgemeiner Warnungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Protokollierung aktivieren

Mit dieser Einstellung aktivieren oder deaktivieren Sie die Protokollierung der Profilverwaltung im Debugmodus (ausführliche Protokollierung). Im Debugmodus werden umfangreiche Statusinformationen in den Protokolldateien unter "%SystemRoot%\System32\Logfiles\UserProfileManager"aufgezeichnet.

Standardmäßig ist diese Einstellung deaktiviert und es werden nur Fehler protokolliert.

Citrix empfiehlt, dass Sie diese Einstellung nur aktivieren, wenn Sie eine Problembehandlung für die Profilverwaltung durchführen.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden nur Fehler protokolliert.

Dateisystemaktionen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der im Dateisystem ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Dateisystembenachrichtigungen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Dateisystembenachrichtigungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Abmeldung

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Benutzerabmeldungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Anmeldebildschirm

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung von Benutzeranmeldungen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Maximale Größe der Protokolldatei

Mit dieser Einstellung geben Sie die maximal zulässige Größe für die Protokolldatei der Profilverwaltung in Bytes an.

Der Standardwert dieser Einstellung ist 1048576 Bytes (1 MB).

Citrix empfiehlt, dass die Größe dieser Datei auf 5 MB oder mehr erhöht wird, sofern Sie ausreichend Speicherplatz auf dem Datenträger haben. Wenn die Protokolldatei die maximale Größe überschreitet, wird eine vorhandene Sicherungskopie der Datei (.bak) gelöscht, die Protokolldatei erhält die Erweiterung .bak und eine neue Protokolldatei wird erstellt.

Die Protokolldatei wird unter "%SystemRoot%\System32\Logfiles\UserProfileManager"erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Pfad zur Protokolldatei

Mit dieser Einstellung geben Sie einen alternativen Pfad an, der zum Speichern der Protokolldatei der Profilverwaltung verwendet wird.

Standardmäßig ist diese Einstellung deaktiviert und Protokolldateien werden im Standardspeicherort %SystemRoot%\System32\Logfiles\UserProfileManager gespeichert.

Der Pfad kann zu einem lokalen Laufwerk oder einem Remotelaufwerk im Netzwerk (UNC-Pfad) führen. Remotepfade können in großen, verteilten Umgebungen von Nutzen sein, können aber zu erheblichem Netzwerkverkehr führen, was für Protokolldateien unangebracht ist. Geben Sie für bereitgestellte virtuelle Maschinen mit einer beständigen Festplatte einen lokalen Pfad zu diesem Laufwerk an. Hierdurch wird sichergestellt, dass Protokolldateien beim Neustart der Maschine beibehalten werden. Geben Sie für virtuelle Maschinen ohne eine beständige Festplatte einen UNC-Pfad an. So werden Protokolldateien beibehalten. Das Systemkonto für die Maschinen muss aber Schreibzugriff auf die UNC-Freigabe haben. Verwenden Sie für Laptops, die vom Feature für Offlineprofile verwaltet werden, einen lokalen Pfad.

Wenn für Protokolldateien ein UNC-Pfad verwendet wird, empfiehlt Citrix, entsprechende Zugriffssteuerungslisten auf den Ordner mit den Protokolldateien anzuwenden, um sicherzustellen, dass nur autorisierte Benutzer- oder Computerkonten auf die gespeicherten Dateien zugreifen können.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardspeicherort "%SystemRoot%\System32\Logfiles\UserProfileManager"verwendet.

Persönliche Benutzerinformationen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung persönlicher Benutzerinformationen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Richtlinienwerte bei Anmeldung und Abmeldung

Mit dieser Einstellung aktivieren oder deaktivieren Sie ausführliche Protokollierung der Richtlinienwerte beim An- und Abmelden von Benutzern.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Registrierungsaktionen

Mit dieser Einstellung aktivieren oder deaktivieren Sie die ausführliche Protokollierung der in der Registrierung ausgeführten Aktionen.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Registrierungsunterschiede bei der Abmeldung

Mit dieser Einstellung aktivieren oder deaktivieren Sie ausführliche Protokollierung aller Registrierungsunterschiede bei der Abmeldung von Benutzern.

Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie diese Einstellung aktivieren, stellen Sie sicher, dass die Einstellung Protokollierung aktivieren auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden Fehler und allgemeine Informationen protokolliert.

Einstellungen der Richtlinie "Profilverarbeitung"

August 18, 2021

Der Abschnitt "Profilverarbeitung"enthält Richtlinieneinstellungen zum Konfigurieren, wie die Profilverwaltung Benutzerprofile verarbeitet.

Verzögerung vor dem Löschen von zwischengespeicherten Profilen

Mit dieser Einstellung geben Sie optional eine Verlängerung für die Verzögerung (in Minuten) ein, nach der die Profilverwaltung lokal zwischengespeicherte Profile bei der Abmeldung löscht.

Bei einem Wert von 0 werden die Profile am Ende der Abmeldung sofort gelöscht. Die Profilverwaltung prüft jede Minute auf Abmeldungen, sodass ein Wert von 60 sicherstellt, dass Profile zwischen einer und zwei Minuten (je nachdem, wann die letzte Überprüfung stattgefunden hat) nach dem Abmelden gelöscht werden. Das Erweitern der Verzögerung ist nützlich, wenn Sie wissen, dass ein Prozess Dateien oder die Registrierungsstruktur während der Abmeldung geöffnet hält. Bei großen Profilen kann dies auch den Abmeldungsvorgang beschleunigen.

Die Standardeinstellung ist 0, lokal zwischengespeicherte Profile werden von der Profilverwaltung sofort gelöscht.

Wenn Sie diese Einstellung aktivieren, müssen Sie sicherstellen, dass die Einstellung Lokal zwischengespeicherte Profile nach Abmeldung löschen auch aktiviert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden die Profile sofort gelöscht.

Lokal zwischengespeicherte Profile nach Abmeldung löschen

Mit dieser Einstellung geben Sie an, ob lokal zwischengespeicherte Profile gelöscht werden, nachdem Benutzer sich abmelden.

Wenn diese Einstellung aktiviert ist, wird der lokale Profilcache der Benutzer nach der Abmeldung gelöscht. Citrix empfiehlt, dass Sie diese Einstellung für Terminalserver aktivieren.

Standardmäßig ist diese Einstellung deaktiviert und der lokale Profilcache von Benutzern wird nach der Abmeldung beibehalten.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden zwischengespeicherte Profile nicht gelöscht.

Behandlung von Konflikten lokaler Profile

Mit dieser Einstellung wird konfiguriert, wie die Profilverwaltung verfährt, wenn ein Benutzerprofil sowohl im Benutzerspeicher als auch als lokales Windows-Benutzerprofil (kein Citrix Benutzerprofil) vorhanden ist.

Standardmäßig verwendet die Profilverwaltung lokale Windows-Profile, ohne diese jedoch zu ändern.

Zum Steuern, wie die Profilverwaltung verfahren soll, wählen Sie eine der folgenden Optionen:

- Lokales Profil verwenden. Die Profilverwaltung verwendet lokale Windows-Profile, ohne diese jedoch zu ändern.
- Lokales Profil löschen. Die Profilverwaltung löscht das lokale Windows-Benutzerprofil und importiert dann das Citrix Benutzerprofil aus dem Benutzerspeicher.
- Lokales Profil umbenennen. Die Profilverwaltung benennt das lokale Windows-Benutzerprofil um (als Sicherungskopie) und importiert dann das Citrix Benutzerprofil aus dem Benutzerspeicher.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden vorhandene lokale Profile verwendet.

Migration vorhandener Profile

Mit dieser Einstellung geben Sie den Typ des Profils an, das bei der Anmeldung eines Benutzers in den Benutzerspeicher migriert wird, wenn der Speicher kein aktuelles Profil für den Benutzer enthält.

Die Profilverwaltung kann vorhandene Profile während der Anmeldung spontan migrieren, wenn der Benutzer kein Profil im Benutzerspeicher hat. Anschließend verwendet die Profilverwaltung das Profil im Benutzerspeicher in der aktuellen Sitzung und in allen künftigen Sitzungen, die mit dem Pfad zu demselben Benutzerspeicher konfiguriert sind.

Standardmäßig werden lokale Profile und Roamingprofile während der Anmeldung in den Benutzerspeicher migriert.

Um anzugeben welche Profiltypen bei der Anmeldung in den Benutzerspeicher migriert werden sollen, wählen Sie eine der folgenden Optionen:

- Lokal und Roaming
- Lokal
- Roaming
- Keine (deaktiviert)

Wenn Sie Keine auswählen, wird der vorhandene Windows-Mechanismus für die Erstellung neuer Profile verwendet, genau wie in einer Umgebung, in der die Profilverwaltung nicht installiert ist.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden vorhandene lokale und servergespeicherte Profile migriert.

Pfad zum Vorlagenprofil

Mit dieser Einstellung geben Sie den Pfad zu dem Profil an, das die Profilverwaltung als Vorlage zum Erstellen neuer Benutzerprofile verwenden soll.

Dies muss der vollständige Pfad zu dem Ordner sein, der die Registrierungsdatei NTUSER.DAT und sämtliche anderen für das Vorlagenprofil erforderlichen Dateien und Ordner enthält.

Hinweis: Geben Sie mit dem Pfad nicht NTUSER.DAT ein. Geben Sie für die Datei \\Server\Profile\Vorlage\ntuser.dat den Speicherort als \\Server\Profile\Vorlage an.

Verwenden Sie einen absoluten Pfad (entweder einen UNC-Pfad oder einen Pfad auf dem lokalen Computer). Sie können einen lokalen Pfad verwenden, um z. B. ein Vorlagenprofil auf einem Citrix Provisioning Services-Image dauerhaft anzugeben. Relative Pfade werden nicht unterstützt.

Hinweis: Beachten Sie, dass diese Richtlinie nicht die Erweiterung von Active Directory-Attributen, Systemumgebungsvariablen oder der Variablen %USERNAME% und %USERDOMAIN% unterstützt.

Standardmäßig ist diese Einstellung deaktiviert und neue Benutzerprofile werden auf der Basis des Standardbenutzerprofils auf dem Gerät, auf dem sich der Benutzer als erstes anmeldet, erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Vorlagenprofil überschreibt lokales Profil

Diese Einstellung ermöglicht eine Überschreibung des lokalen Profils durch das Vorlagenprofil bei der Erstellung neuer Benutzerprofile.

Wenn ein Benutzer kein Citrix Benutzerprofil hat, aber ein lokales Windows-Benutzerprofil vorhanden ist, wird standardmäßig das lokale Profil verwendet (und in den Benutzerspeicher migriert, wenn diese Option nicht deaktiviert ist). Durch Aktivieren dieser Einstellung kann das Vorlagenprofil das lokale Profil bei der Erstellung neuer Benutzerprofile überschreiben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Vorlagenprofil überschreibt Roamingprofil

Diese Einstellung ermöglicht eine Überschreibung eines Roamingprofils durch das Vorlagenprofil bei der Erstellung neuer Benutzerprofile.

Wenn ein Benutzer kein Citrix Benutzerprofil hat aber ein lokales Windows-Benutzerprofil vorhanden ist, wird standardmäßig das Roamingprofil verwendet (und in den Benutzerspeicher migriert, wenn diese Option nicht deaktiviert ist). Durch Aktivieren dieser Einstellung kann das Vorlagenprofil das Roamingprofil bei der Erstellung neuer Benutzerprofile überschreiben.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Als verbindliche Citrix Profil für alle Anmeldungen verwendete Vorlagenprofil

Bei Auswahl dieser Einstellung verwendet die Profilverwaltung das Vorlagenprofil als Standardprofil bei der Erstellung aller neuen Benutzerprofile.

Standardmäßig ist diese Einstellung deaktiviert und neue Benutzerprofile werden auf der Basis des Standardbenutzerprofils auf dem Gerät, auf dem sich der Benutzer als erstes anmeldet, erstellt.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Vorlagen verwendet.

Einstellungen der Richtlinie "Registrierung"

November 29, 2018

Der Abschnitt "Registrierung"enthält Richtlinieneinstellungen, mit denen Sie festlegen können, welche Registrierungsschlüssel bei der Verarbeitung der Profilverwaltung berücksichtigt und welche ausgeschlossen werden sollen.

Ausschlussliste

Mit dieser Einstellung geben Sie die Liste der Registrierungsschlüssel in der HKCU-Struktur an, die nicht von der Profilverwaltung verarbeitet werden sollen, wenn sich ein Benutzer abmeldet.

Wenn diese Option aktiviert ist, werden die in dieser Liste aufgeführten Schlüssel von der Verarbeitung ausgeschlossen, wenn sich ein Benutzer abmeldet.

Standardmäßig ist diese Einstellung deaktiviert, und alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden keine Registrierungsschlüssel von der Verarbeitung ausgeschlossen.

Aufnahmeliste

Mit dieser Einstellung geben Sie die Liste der Registrierungsschlüssel in der HKCU-Struktur an, die von der Profilverwaltung verarbeitet werden sollen, wenn sich ein Benutzer abmeldet.

Wenn diese Option aktiviert ist, werden die in dieser Liste aufgeführten Schlüssel in die Verarbeitung eingeschlossen, wenn sich ein Benutzer abmeldet.

Standardmäßig ist diese Einstellung deaktiviert, und alle Registrierungsschlüssel in der HKCU-Struktur werden verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird die gesamte HKCU-Struktur verarbeitet.

Einstellungen der Richtlinie "Gestreamte Benutzerprofile"

November 15, 2022

Der Abschnitt "Gestreamte Benutzerprofile"enthält Richtlinieneinstellungen zum Konfigurieren, wie die Profilverwaltung Benutzerprofile verarbeitet.

Immer zwischenspeichern

Mit dieser Einstellung geben Sie an, ob die Profilverwaltung gestreamte Dateien so bald wie möglich zwischenspeichern soll, wenn sich ein Benutzer anmeldet. Durch das Zwischenspeichern von Dateien, nachdem sich ein Benutzer anmeldet, wird Netzwerkbandbreite gespart und die Benutzererfahrung optimiert.

Verwenden Sie diese Einstellung mit der Einstellung Profilstreaming.

Standardmäßig ist diese Einstellung deaktiviert und gestreamte Dateien werden nicht so schnell wie möglich zwischengespeichert, wenn sich ein Benutzer anmeldet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

Immer Cachegröße

Mit dieser Einstellung geben Sie eine Untergrenze (in Megabytes) für die Größe der Dateien an, die gestreamt werden. Die Profilverwaltung speichert Dateien dieser Größe bzw. größere Dateien so bald wie möglich zwischen, wenn ein Benutzer sich anmeldet.

Die Standardeinstellung ist 0 (null) und die Funktion zum Zwischenspeichern des gesamten Profils wird verwendet. Wenn das Feature zum Zwischenspeichern des gesamten Profils aktiviert ist, ruft die Profilverwaltung den gesamten Inhalt des Profils im Benutzerspeicher als Hintergrundaufgabe ab, nachdem sich ein Benutzer anmeldet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

Profilstreaming

Diese Einstellung aktiviert oder deaktiviert das Feature für gestreamte Citrix Benutzerprofile. Wenn diese Option aktiviert ist, werden Dateien und Ordner in einem Profil nur dann aus dem Benutzerspeicher auf den lokalen Computer abgerufen, wenn auf sie von Benutzern nach der Anmeldung zugegriffen wird. Registrierungseinträge und Dateien im Bereich für ausstehende Dateien werden sofort abgerufen.

Standardmäßig ist das Profilstreaming ist deaktiviert.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, ist sie deaktiviert.

Gestreamte Benutzerprofilgruppen

Mit dieser Einstellung geben Sie die Benutzerprofile in einer Organisationseinheit gestreamt werden, basierend auf Windows Benutzergruppen.

Wenn diese Option aktiviert ist, werden nur die Benutzerprofile in den angegebenen Benutzergruppen gestreamt. Alle anderen Benutzerprofile werden normal verarbeitet.

Standardmäßig ist diese Einstellung deaktiviert und alle Dateien in Benutzerprofilen werden normal verarbeitet.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, werden alle Benutzergruppen verarbeitet.

Aktivieren des Profilstreamingausschlusses

Wenn der Profilstreamingausschluss aktiviert ist, streamt die Profilverwaltung die in der Ausschlussliste angegebenen Ordner nicht und alle Ordner werden sofort vom Benutzerspeicher auf den lokalen Computer, bei dem sich der Benutzer anmeldet, abgerufen.

Weitere Informationen finden Sie unter Aktivieren des Profilstreamingausschlusses.

Timeout für gesperrte Dateien im ausstehenden Bereich

Mit dieser Einstellung geben Sie einen Zeitraum (in Tagen) an, nach dem Dateien der Benutzer aus dem Bereich für ausstehende Dateien in den Benutzerspeicher zurückgeschrieben werden, wenn ein Server nicht mehr reagiert und der Benutzerspeicher gesperrt bleibt. Dies verhindert ein Aufblähen des ausstehenden Bereichs und stellt sicher, dass der Benutzerstore immer die aktuellen Dateien enthält.

Die Standardeinstellung ist 1 Tag.

Wenn diese Einstellung hier nicht konfiguriert ist, wird der Wert in der INI-Datei verwendet.

Wenn diese Einstellung weder hier noch in der INI-Datei konfiguriert ist, wird der Standardwert verwendet.

Einstellungen der Richtlinie "Receiver"

November 29, 2018

Hinweis: Wenn nicht anders angegeben, bezieht sich "Receiver"auf Citrix Receiver.

Der Abschnitt "Receiver"enthält Richtlinieneinstellungen zum Angeben einer Liste von StoreFront-Adressen, die für auf dem virtuellen Desktop ausgeführte Windows-Betriebssysteme per Push an Citrix Receiver für Windows übertragen werden sollen.

StoreFront-Kontenliste

Mit dieser Einstellung geben Sie eine Liste der StoreFront-Stores an, die Administratoren für die Übertragung per Push an Citrix Receiver für Windows auswählen können. Beim Erstellen einer Bereitstellungsgruppe können Administratoren auswählen, welche Stores für Citrix Receiver für Windows auf virtuellen Desktops, die in dieser Gruppe ausgeführt werden, per Push übertragen werden sollen.

In der Standardeinstellung sind keine Stores angegeben.

Geben Sie für jeden Store die folgenden Informationen in Form eines durch Semikolons getrennten Eintrags an:

- Storename: der Name des Stores wie er Benutzern angezeigt wird.
- Store-URL: die URL des Stores.
- Storeaktivierungszustand: Ob der Store für Benutzer verfügbar ist. Dies ist entweder ein oder aus.
- Store-Beschreibung: die Beschreibung des Stores, die Benutzern angezeigt wird.

Beispiel: Vertriebs-Store;`https://sales.mycompany.com/Citrix/Store/discovery;On;Store` für Vertriebspersonal

Einstellungen der Richtlinie "Virtual Delivery Agent"

August 18, 2021

Der Abschnitt "Virtual Delivery Agent"(VDA) enthält Richtlinieneinstellungen, mit denen Sie die Kommunikation zwischen VDA und Controllern einer Site steuern können.

Wichtig: Der VDA benötigt die in diesen Einstellungen enthaltenen Informationen für die Registrierung bei einem Delivery Controller, wenn das Feature für automatische Controllerupdates nicht verwendet wird. Da die Informationen für die Registrierung erforderlich sind, müssen Sie sie mit dem Gruppenrichtlinien-Editor konfigurieren, sofern Sie sie nicht bei der VDA-Installation angeben.

- IPv6-Netzwerkmaske für Controllerregistrierung
- Controllerregistrierungsport
- Controller-SIDs
- Controller
- Nur IPv6-Controllerregistrierung verwenden
- Site-GUID

IPv6-Netzwerkmaske für Controllerregistrierung

Mit dieser Richtlinieneinstellung kann der VDA auf ein bevorzugtes Subnetz (anstelle einer globalen IP, sofern registriert) limitiert werden. Mit dieser Einstellung geben Sie die IPv6-Adresse und das Netzwerk an, in dem der VDA registriert wird. Der VDA wird nur an der ersten Adresse registriert, die mit der angegebenen Netzmaske übereinstimmt. Diese Einstellung ist nur gültig, wenn die Richtlinieneinstellung Nur IPv6-Controllerregistrierung verwenden aktiviert ist.

Diese Einstellung ist standardmäßig leer.

Controllerregistrierungsport

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Mit dieser Einstellung geben Sie die TCP/IP-Portnummer an, die der VDA für die Registrierung bei einem Controller verwendet, wenn die registrierungsbasierte Registrierung verwendet wird.

Die Standardeinstellung der Portnummer ist “80”.

Controller-SIDs

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Mit dieser Einstellung geben Sie eine durch Leerzeichen getrennte Liste von Controller-SIDs an, die der VDA für die Registrierung bei einem Controller verwendet, wenn die registrierungsbasierte Registrierung verwendet wird. Dies ist eine optionale Einstellung, die mit der Einstellung “Controller”verwendet werden kann, um die für die Registrierung verwendete Liste von Controllern zu beschränken.

Diese Einstellung ist standardmäßig leer.

Controller

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Mit dieser Einstellung geben Sie eine durch Leerzeichen getrennte Liste von vollständig qualifizierten Domänennamen (FQDN) für Controller an, die der VDA für die Registrierung bei einem Controller verwendet, wenn die registrierungsbasierte Registrierung verwendet wird. Dies ist eine optionale Einstellung, die mit der Einstellung "Controller-SIDs"verwendet werden kann.

Diese Einstellung ist standardmäßig leer.

Automatische Controllerupdates aktivieren

Mit dieser Einstellung ist eine automatische Registrierung des VDAs bei einem Controller nach der Installation möglich.

Nach der Registrierung wird von dem Controller, bei dem der VDA registriert ist, eine Liste der aktuellen Controller-FQDNs und -SIDs an den VDA gesendet. Diese Liste wird in den persistenten Speicher des VDAs geschrieben. Jeder Controller prüft die Datenbank alle 90 Minuten auf Controllerinformationen. Wurde seit der letzten Prüfung ein Controller hinzugefügt oder entfernt oder ist eine Richtlinienänderung erfolgt, sendet der Controller eine aktualisierte Liste an die bei ihm registrierten VDAs. Der VDA nimmt alle Verbindungen von allen Controllern in der aktuellen Liste an.

Standardmäßig ist diese Einstellung aktiviert.

Nur IPv6-Controllerregistrierung verwenden

Diese Einstellung steuert das Format der Adresse, die vom VDA für die Registrierung beim Controller verwendet wird:

- Ist die Einstellung aktiviert, wird der VDA mit der IPv6-Adresse der Maschine beim Controller registriert. Wenn der VDA mit dem Controller kommuniziert, wird eine Adresse verwendet, deren Auswahl folgender Reihenfolge unterliegt: globale IP-Adresse, ULA-Adresse, Link-Local-Adresse (wenn keine anderen IPv6-Adressen verfügbar sind).
- Ist die Einstellung deaktiviert, wird der VDA mit der IPv4-Adresse der Maschine für die Kommunikation beim Controller registriert.

Diese Einstellung ist standardmäßig deaktiviert.

Site-GUID

Verwenden Sie diese Einstellung nur, wenn die Einstellung Automatische Controllerupdates aktivieren deaktiviert ist.

Diese Einstellung gibt den Globally Unique Identifier (GUID) der Site an, den der VDA für die Registrierung bei einem Controller verwendet, wenn die Active Directory-basierte Registrierung verwendet wird.

Diese Einstellung ist standardmäßig leer.

Einstellungen der Richtlinie "HDX 3D Pro"

July 1, 2019

Der Bereich "HDX 3D Pro"enthält Richtlinieneinstellungen, mit denen Sie das Tool zum Konfigurieren der Bildqualität für Benutzer aktivieren und konfigurieren können. Mit dem Tool können Benutzer die Verwendung der verfügbaren Bandbreite durch Anpassen des Verhältnisses zwischen Bildqualität und Reaktionszeit in Echtzeit optimieren.

Verlustfrei aktivieren

Mit dieser Einstellung wird angegeben, ob Benutzer verlustfreie Komprimierung mit dem Tool zum Konfigurieren der Bildqualität aktivieren oder deaktivieren können. In der Standardeinstellung wird den Benutzern die Möglichkeit zum Aktivieren der verlustfreien Komprimierung nicht eingeräumt.

Aktiviert ein Benutzer die verlustfreie Komprimierung, wird die Bildqualität automatisch auf den höchsten Wert eingestellt, der im Bildkonfigurationstool verfügbar ist. Standardmäßig kann je nach Leistungsfähigkeit des Benutzergeräts und des Hostcomputers entweder die GPU-basierte oder die CPU-basierte Komprimierung verwendet werden.

HDX 3D Pro-Qualitätseinstellungen

Mit dieser Einstellung geben Sie den Mindest- und den Höchstwert an, mit denen der Bildqualitätsanpassungsbereich, der den Benutzern im Tool zum Konfigurieren der Bildqualität zur Verfügung steht, festgelegt wird.

Geben Sie für die Bildqualität Werte zwischen 0 und 100 an. Der Höchstwert muss größer oder gleich dem Mindestwert sein.

Einstellungen der Überwachungsrichtlinie

August 18, 2021

Der Abschnitt "Überwachung"enthält Richtlinieneinstellungen für die Prozess-, Ressourcen- und Anwendungsfehlerüberwachung.

Der Bereich dieser Richtlinien kann basierend auf Site, Bereitstellungsgruppe, Bereitstellungsgruppentyp, Organisationseinheit und Tags definiert werden.

Richtlinien für die Prozess- und Ressourcenüberwachung

Jeder Datenpunkt für CPU, Arbeitsspeicher und Prozesse wird auf dem VDA gesammelt und in der Überwachungsdatenbank gespeichert. Das Senden der Datenpunkte vom VDA verbraucht Netzwerkbandbreite und deren Speicherung verbraucht beträchtlichen Platz in der Überwachungsdatenbank. Wenn Sie Ressourcen- und/oder Prozessdaten für einen bestimmten Bereich (z. B. eine Bereitstellungsgruppe oder Organisationseinheit) nicht überwachen möchten, empfiehlt es sich, die Richtlinie zu deaktivieren.

Prozessüberwachung aktivieren

Aktivieren Sie diese Einstellung, um die auf Maschinen mit VDAs ausgeführten Prozesse zu überwachen. Statistikwerte wie CPU- und Speicherauslastung werden an den Überwachungsdienst gesendet. Die Statistik wird für Echtzeitbenachrichtigungen und die Erstellung von Verlaufsberichten in Director verwendet.

Standardmäßig ist diese Einstellung deaktiviert.

Ressourcenüberwachung aktivieren

Aktivieren Sie diese Einstellung, um kritische Leistungsindikatoren auf Maschinen mit VDAs zu überwachen. Statistikwerte wie CPU- und Speichernutzung, IOPS und Latenz werden an den Überwachungsdienst gesendet. Die Statistik wird für Echtzeitbenachrichtigungen und die Erstellung von Verlaufsberichten in Director verwendet.

Standardmäßig ist diese Einstellung aktiviert.

Skalierbarkeit

CPU- und Speicherdaten werden alle 5 Minuten von den VDAs an die Datenbank gesendet, Prozessdaten (sofern deren Überwachung aktiviert ist) alle 10 Minuten. Daten zu IOPS und Datenträgerlatenz werden in Zeitintervallen von 1 Stunde an die Datenbank gesendet.

CPU- und Speicherdaten

Die Sammlung der CPU- und Speicherdaten ist standardmäßig **aktiviert**. Die Daten werden für folgende Zeiträume aufbewahrt (Platinum-Lizenz):

Datengranularität	Zeitraum in Tagen
5-minütige Daten	1 Tag
10-minütige Daten	7 Tage
Stündliche Daten	30 Tage
Tägliche Daten	90 Tage

Daten zu IOPS und Datenträgerlatenz

Daten zu IOPS und Datenträgerlatenz sind standardmäßig **aktiviert**. Die Daten werden für folgende Zeiträume aufbewahrt (Platinum-Lizenz):

Datengranularität	Zeitraum in Tagen
Stündliche Daten	3 Tage
Tägliche Daten	90 Tage

Mit den oben angegebenen Einstellungen für die Datenaufbewahrung werden zum Speichern der CPU-, Speicher, IOPS und Latenzdaten für einen VDA über einen Zeitraum von einem Jahr ca. 276 KB Speicherplatz benötigt.

Anzahl Maschinen	Erforderlicher Speicher (ca.)
1	276 KB
1.000	270 MB
40.000	10,6 GB

Prozessdaten

Die Sammlung der Prozessdaten ist standardmäßig **deaktiviert**. Es wird empfohlen, die Sammlung von Prozessdaten nur für Teilgruppen von Maschinen nach Bedarf zu aktivieren. Die Daten werden standardmäßig für folgende Zeiträume aufbewahrt:

Datengranularität	Zeitraum in Tagen
10-minute Data	1 Tag
Stündliche Daten	7 Tage

Wenn die Sammlung der Prozessdaten mit den Standardeinstellungen für die Aufbewahrung aktiviert ist, belegen die Prozessdaten über einen Zeitraum von einem Jahr pro VDA ca. 1,5 MB und pro Terminaldienste-VDA (TS-VDA) ca. 3 MB.

Anzahl Maschinen	Erforderlicher Speicher pro VDA (ca.)	Erforderlicher Speicher pro TS-VDA (ca.)
1	1,5 MB	3 MB
1.000	1,5 GB	3 GB

> **Hinweis:**
>
> Die oben angegebenen Zahlen umfassen nicht den Indexspeicher. Sämtliche Werte sind Näherungswerte und können je nach Bereitstellung variieren.

Optionale Konfigurationen

Sie können die Standardeinstellungen für die Datenaufbewahrung nach Bedarf ändern. Dadurch wird jedoch zusätzlicher Speicher belegt. Durch Aktivieren der unten aufgeführten Einstellungen erhalten Sie genauere Prozessauslastungsdaten. Sie können folgende Konfigurationen aktivieren:

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

Diese Konfigurationen können über das PowerShell-Cmdlet für die Überwachung aktiviert werden: Set-MonitorConfiguration

Richtlinien für die Überwachung auf Anwendungsfehler

Auf der Registerkarte **Anwendungsausfälle** werden standardmäßig nur Anwendungsfehler auf Serverbetriebssystem-VDAs angezeigt. Die Einstellungen für die Überwachung auf Anwendungsfehler können mit den folgenden Überwachungsrichtlinien geändert werden:

Überwachung von Anwendungsausfällen aktivieren

Verwenden Sie diese Einstellung zum Konfigurieren der Überwachung auf Anwendungsfehler oder Ausfälle (Abstürze und unbehandelten Ausnahmen) oder auf beides.
Deaktivieren Sie die Überwachung auf Anwendungsfehler durch Festlegen des **Werts** auf **None**.
In der Standardeinstellung erfolgt die ausschließliche Überwachung auf Anwendungsfehler.

Überwachung von Ausfällen auf Desktop-OS-VDAs

Standardmäßig werden nur Anwendungen auf Serverbetriebssystem-VDAs überwacht. Um Anwendungen auf Desktopbetriebssystem-VDAs zu überwachen, legen Sie die Richtlinie auf **Zugelassen** fest.
Die Standardeinstellung ist **Nicht zugelassen**.

Von der Fehlerüberwachung ausgeschlossene Anwendungen

Geben Sie eine Liste der Anwendungen an, die nicht auf Fehler überwacht werden sollen.
In der Standardeinstellung ist die Liste leer.

Tipps für die Speicherplanung

Gruppenrichtlinie: Wenn Sie die Ressourcendaten und/oder die Prozessdaten nicht überwachen möchten, können Sie die Überwachung für eine oder beide Datenarten mit der Gruppenrichtlinie deaktivieren. Weitere Informationen finden Sie unter Erstellen von Richtlinien im Abschnitt "Gruppenrichtlinie".

Datenbereinigung: Die Standardeinstellungen für die Datenaufbewahrung können geändert werden, um die Daten früher zu bereinigen und Speicherplatz freizugeben. Weitere Informationen zu den Bereinigungseinstellungen finden Sie unter Zugriff auf Daten mit der API im Abschnitt zu Datengranularität und -aufbewahrung.

Einstellungen der Richtlinie “Virtuelle IP”

March 19, 2020

Der Abschnitt “Virtuelle IP”enthält Richtlinieneinstellungen für die Angabe, ob Sitzungen eine eigene virtuelle Loopbackadresse haben.

Virtuelle IP - Loopbackunterstützung

Wenn diese Einstellung aktiviert ist, hat jede Sitzung eine eigene virtuelle Loopbackadresse. Wenn diese Einstellung deaktiviert ist, haben Sitzungen keine individuellen Loopbackadressen.

Diese Einstellung ist standardmäßig deaktiviert.

Virtuelle IP - Programme für virtuelles Loopback

Mit dieser Einstellung geben Sie die ausführbaren Dateien der Anwendungen an, die virtuelle Loopbackadressen verwenden können. Wenn Sie der Liste Programme hinzufügen, geben Sie nur den Namen der ausführbaren Datei an. Sie müssen nicht den gesamten Pfad angeben.

Zum Hinzufügen mehrerer ausführbarer Dateien fügen Sie jede in einer eigenen Zeile hinzu.

In der Standardeinstellung sind keine ausführbaren Dateien angegeben.

Konfigurieren von COM-Port- und LPT-Portumleitungseinstellungen in der Registrierung

March 19, 2020

In den VDA-Versionen 7.0 bis 7.8 können COM- und LPT-Porteinstellungen nur über die Registrierung konfiguriert werden. In VDA-Versionen vor 7.0 und ab Version 7.9 können Sie diese Einstellungen in Studio konfigurieren. Weitere Informationen finden Sie unter Einstellungen der Richtlinie “Portumleitung” und Einstellungen der Richtlinie “Bandbreite”.

Richtlinieneinstellungen für COM-Port- und LPT-Portumleitung befinden sich unter HKLM\Software\Citrix\GroupPo
auf dem VDA-Image oder Computer.

Zum Aktivieren der COM-Port- und LPT-Portumleitung, fügen Sie neue Registrierungsschlüssel vom Typ REG_DWORD wie folgt hinzu:

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Registrierungsschlüssel	Beschreibung	Zulässige Werte
AllowComPortRedirection	Zulassen oder Verhindern der COM-Portumleitung	1 (Zulassen) oder 0 (Verhindern)
LimitComBw	Bandbreitenlimit für COM-Portumleitungskanal	Numerischer Wert
LimitComBWPercent	Bandbreitenlimit für COM-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite	Numerischer Wert zwischen 0 und 100
AutoConnectClientComPorts	Automatische Verbindung von COM-Ports auf dem Benutzergerät	1 (Zulassen) oder 0 (Verhindern)
AllowLptPortRedirection	Zulassen oder Verhindern der LPT-Portumleitung	1 (Zulassen) oder 0 (Verhindern)
LimitLptBw	Bandbreitenlimit für LPT-Portumleitungskanal	Numerischer Wert
LimitLptBwPercent	Bandbreitenlimit für LPT-Portumleitungskanal als Prozentsatz der Gesamtsitzungsbandbreite	Numerischer Wert zwischen 0 und 100
AutoConnectClientLptPorts	Automatische Verbindung von LPT-Ports auf dem Benutzergerät	1 (Zulassen) oder 0 (Verhindern)

Nach dem Konfigurieren dieser Einstellungen ändern Sie die Maschinenkataloge, damit sie das neue Masterimage oder die aktualisierte physische Maschine verwenden. Wenn sich die Benutzer das nächste Mal abmelden, werden die Desktops mit den neuen Einstellungen aktualisiert.

Richtlinieneinstellungen für Connector für Configuration Manager 2012

August 23, 2019

Der Abschnitt "Connector für Configuration Manager 2012"enthält Richtlinieneinstellungen zum Konfigurieren des Citrix Connector 7.5-Agents.

Wichtig: Richtlinien für Warnungs-, Abmeldungs- und Neustartmeldungen gelten nur für Bereitstellungen für Serverbetriebssystemmaschinenkataloge, die manuell oder über Provisioning Services verwaltetet werden. Bei solchen Maschinenkatalogen benachrichtigt der Connector-Dienst Benutzer über ausstehende Anwendungsinstallationen oder Softwareupdates.

Verwenden Sie bei über MCS verwalteten Katalogen Studio zur Benachrichtigung der Benutzer. Verwenden Sie bei manuell verwalteten Maschinenkatalogen mit Desktopbetriebssystemmaschinen Configuration Manager zur Benachrichtigung der Benutzer. Verwenden Sie bei mit Provisioning Services verwalteten Maschinenkatalogen mit Desktopbetriebssystemmaschinen Provisioning Services zur Benachrichtigung der Benutzer.

Häufigkeit für Vorabwarnung

Diese Einstellung gibt das Intervall an, mit dem Benutzern Vorabmeldungen angezeigt werden.

Intervalle werden im Format ttt.hh:mm:ss festgelegt. Dabei gilt Folgendes:

- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.
- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

Das Standardintervall ist 1 Stunde (01:00:00).

Meldungsfeldtext für Vorabwarnung

Diese Einstellung enthält den editierbaren Text für die Vorabmeldung, die Benutzer vor anstehenden Softwareupdates oder Wartungsaufgaben erhalten, für die sie sich abmelden müssen.

Die Standardmeldung lautet: {TIMESTAMP} Please save your work. Der Server wird in {TIMELEFT} zu Wartungszwecken heruntergefahren.

Meldungsfeldtitel für Vorabwarnung

Diese Einstellung enthält den editierbaren Titel für die Titelleiste der Vorabmeldung, die Benutzer erhalten.

Der Standardtitel ist: Upcoming Maintenance

Zeitraum für Vorabwarnung

Diese Einstellung definiert, wie lange vor Wartungsaufgaben die Vorabwarnmeldung zum ersten Mal angezeigt wird.

Der Zeitraum wird im Format ttt.hh:mm:ss angegeben, mit den folgenden Variablen:

- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.
- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

In der Standardeinstellung ist der Wert 16 Stunden (16:00:00), d. h. dass die erste Vorabwarnmeldung ca. 16 Stunden vor der Wartung angezeigt wird.

Feldtitel für letzte Meldung für erzwungenes Abmelden

Diese Einstellung enthält den editierbaren Text für die Meldung, die Benutzer warnt, dass die Abmeldung erzwungen wird.

Die Standardmeldung lautet: The server is currently going offline for maintenance

Feldtitel für letzte Meldung für erzwungenes Abmelden

Diese Einstellung enthält den editierbaren Titel für die Titelleiste der letzten Meldung für Abmeldung erzwingen.

Der Standardtitel lautet: Notification From IT Staff

Kulanzzeitraum für erzwungenes Abmelden

Diese Einstellung definiert den Kulanzzeitraum, der Benutzern zugestanden wird, nachdem sie gewarnt wurden, dass die Abmeldung erzwungen wird, und dem tatsächlichen erzwungenen Abmelden, damit die ausstehenden Wartungsaufgaben gestartet werden können.

Der Zeitraum wird im Format ttt.hh:mm:ss angegeben, mit den folgenden Variablen:

- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.

- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

In der Standardeinstellung ist der Kulanzzeitraum für erzwungenes Abmelden auf 5 Minuten (00:05:00) festgelegt.

Meldungsfeldtext für erzwungenes Abmelden

Diese Einstellung enthält den editierbaren Text für die letzte Warnmeldung, die Benutzer auffordert, ihre Arbeit zu speichern und sich vor der erzwungenen Abmeldung abzumelden.

Die Standardmeldung enthält den folgenden Text: {TIMESTAMP} Please save your work and log off. Der Server wird in {TIMELEFT} zu Wartungszwecken heruntergefahren.

Meldungsfeldtitel für erzwungenes Abmelden

Diese Einstellung enthält den editierbaren Text für die Titelleiste der Meldung für Abmeldung erzwingen.

Der Standardtitel lautet: Notification From IT Staff

Imageverwalteter Modus

Der Connector-Agent erkennt automatisch, wenn er auf einem von Provisioning Services oder MCS verwalteten Maschinenklon ausgeführt wird. Der Agent blockiert Configuration Manager-Updates auf imageverwalteten Klonen und installiert die Updates automatisch auf dem Masterimage des Katalogs.

Nachdem ein Masterimage aktualisiert wurde, verwenden Sie Studio zum Orchestrieren des Neustarts der MCS-Klone. Der Connector-Agent orchestriert automatisch den Neustart von PVS-Katalogklonen während der Configuration Manager-Wartung. Zur Außerkraftsetzung dieses Verhaltens, damit Software auf Katalogklonen von Configuration Manager installiert wird, ändern Sie den Modus von "Imageverwaltet"in Deaktiviert.

Meldungsfeldtext für Neustarten

Diese Einstellung enthält den editierbaren Text der Benutzermeldung, dass der Server bald neu gestartet wird.

Die Standardmeldung lautet: The server is currently going offline for maintenance

Normales Zeitintervall, in dem die Agent-Aufgabe ausgeführt wird

Durch diese Einstellung wird festgelegt, wie häufig der Citrix Connector Agent-Aufgabe ausgeführt wird.

Der Zeitraum wird im Format ttt.hh:mm:ss angegeben, mit den folgenden Variablen:

- ttt steht für die Tage. Dieser Parameter ist optional und kann Werte von 0 bis 999 annehmen.
- hh steht für die Stunden und kann Werte von 0 bis 23 annehmen.
- mm steht für Minuten und kann Werte von 0 bis 59 annehmen.
- ss steht für Sekunden und kann Werte von 0 bis 59 annehmen.

In der Standardeinstellung ist das Intervall auf 5 Minuten (00:05:00) festgelegt.

Verwalten

August 18, 2021

Die Verwaltung einer XenApp- oder XenDesktop-Site hat vielfältige Aspekte.

Lizenzierung

Eine gültige Verbindung mit dem Citrix Lizenzserver ist zum Erstellen einer Site erforderlich. Anschließend können Sie Aufgaben wie das Hinzufügen von Lizenzen, das Ändern von Lizenztyp oder -modell und das Verwalten von Lizenzierungsadministratoren über Studio erledigen. Über Studio können Sie auch auf die License Administration Console zugreifen.

Anwendungen

Anwendungen werden in Bereitstellungsgruppen und optional in Anwendungsgruppen verwaltet.

Zonen

In geografisch verteilten Bereitstellungen führen Sie Anwendungen und Desktops mithilfe von Zonen näher am Benutzer, um die Leistung zu verbessern. Beim Installieren und Konfigurieren einer Site sind alle Controller, Maschinenkataloge und Hostverbindungen in der primären Zone. Später können Sie mit Studio Satellitenzonen für diese Elemente erstellen. Wenn Sie mehrere Zonen haben, können Sie angeben, in welcher Zone neu erstellte Maschinenkataloge, Hostverbindungen und Controller hinzugefügt werden sollen. Sie können Elemente auch zwischen Zonen verschieben.

Verbindungen und Ressourcen

Wenn die Maschinen, über die Anwendungen und Desktops für Benutzer bereitgestellt werden, von einem Hypervisor oder Clouddienst gehostet werden, richten Sie die erste Verbindung beim Erstellen einer Site mit dem Hypervisor bzw. Clouddienst ein. Der Speicher und die Netzwerkdetails der

Verbindung bilden die *Ressourcen*. Später können Sie die Verbindung und ihre Ressourcen ändern und neue Verbindungen erstellen. Sie können auch die Maschinen verwalten, die eine konfigurierte Verbindung verwenden.

Lokaler Hostcache

Der lokale Hostcache ermöglicht die Fortsetzung des Verbindungsbrokerings in einer Site, wenn die Verbindung zwischen einem Delivery Controller und der Sitedatenbank getrennt wird. Es ist das umfassendste Feature für hohe Verfügbarkeit von Citrix für XenApp und XenDesktop.

Verbindungsleasing

Citrix empfiehlt, den lokalen Hostcache anstatt des Verbindungsleasings auszuprobieren. Der lokale Hostcache ist die leistungsstärkere Alternative.

Virtuelle IP und virtuelles Loopback

Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugeordnete IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature des virtuellen Loopbacks können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).

Delivery Controller

In diesem Artikel werden Überlegungen und Verfahren für das Hinzufügen und Entfernen von Controllern zu/aus einer Site erläutert. Außerdem wird beschrieben, wie Controller in andere Zonen oder Sites verschoben werden und wie ein VDA in eine andere Site verschoben wird.

VDA-Registrierung bei Delivery Controllern

Bevor ein VDA die Bereitstellung von Anwendungen und Desktops unterstützen kann, muss er bei einem Controller zum Aufbau der Kommunikation registriert werden. Controlleradressen können auf verschiedene Weise angegeben werden. Dies wird im vorliegenden Artikel beschrieben. Es ist wichtig, dass die VDAs beim Hinzufügen, Verschieben und Entfernen von Controllern immer über aktuelle Informationen verfügen.

Sitzungen

Aufrechterhalten der Sitzungsaktivität ist wichtig für die beste Benutzererfahrung. Mit diversen Features können Sie die Sitzungszuverlässigkeit optimieren und damit das Risiko von Problemen, Ausfallzeiten und Produktivitätsverlusten verringern.

- Sitzungszuverlässigkeit
- Automatische Wiederverbindung von Clients
- ICA-Keep-Alive
- Workspace Control
- Sitzungsroaming

Durchführung einer Suche in Studio

Um bestimmte Maschinen, Sitzungen, Maschinenkataloge, Anwendungen oder Bereitstellungsgruppen in Studio zu finden, verwenden Sie die flexible Suchfunktion.

Tags

Tags werden zur Identifizierung von Elementen wie z. B. Maschinen, Anwendungen, Gruppen und Richtlinien verwendet. Sie können Vorgänge mit einem Tag konfigurieren, sodass sie auf spezifische Objekte angewendet werden.

IPv4/IPv6

XenApp und XenDesktop unterstützen reines IPv4, reines IPv6 und duale Bereitstellungen, bei denen IPv4- und IPv6-Netzwerke einander überlagern. Dieser Artikel beschreibt und veranschaulicht diese Bereitstellungen. Außerdem werden die Citrix Richtlinieneinstellungen vorgestellt, mit denen die Verwendung von IPv4 bzw. IPv6 gesteuert wird.

Benutzerprofile

Standardmäßig wird die Citrix Profilverwaltung automatisch bei der Installation eines VDA installiert. Wenn Sie diese Lösung verwenden, lesen Sie diesen Artikel mit allgemeinen Hinweisen und die Dokumentation zur Profilverwaltung mit umfassenden Informationen.

Citrix Insight Services

Citrix Insight Services (CIS) ist eine Plattform von Citrix für Instrumentierung, Telemetrie und Ablaufverfolgung.

Lizenzierung

August 29, 2022

> **Hinweis**
>
> Studio und Director unterstützen Citrix Lizenzserver VPX nicht. Weitere Informationen zu Citrix Lizenzserver VPX finden Sie in der Citrix Lizenzierungsdokumentation.

Sie können die Lizenzierung in Studio verwalten und nachverfolgen, wenn der Lizenzserver in derselben Domäne wie Studio oder in einer vertrauenswürdigen Domäne ist. Informationen zu anderen Lizenzierungsaufgaben finden Sie in der Dokumentation zur Lizenzierung und unter Multityplizenzierung.

Sie müssen für die nachfolgend beschriebenen Aufgaben Volladministrator für die Lizenzierung sein, außer um die Lizenzinformationen anzuzeigen. Zum Anzeigen der Lizenzinformationen in Studio

muss der Administrator mindestens Lesezugriff als delegierter Administrator für die Lizenzierung haben. Die integrierten Rollen des Volladministrators und des Administrators mit Leserechten haben diese Berechtigung.

In der folgenden Tabelle werden die unterstützten Editionen und Lizenzierungsmodelle aufgeführt:

Produkte	Editionen	Lizenzmodelle
XenApp	Platinum, Enterprise, Advanced	CCU
XenDesktop	Platinum, Enterprise, App, VDI	Benutzer/Gerät, Gleichzeitig

> **Wichtig:**
>
> Lizenzserver VPX ist veraltet und erhält keine weiteren Wartungs- oder Sicherheitsfixes. Kunden, die Lizenzserver VPX 11.16.6 oder frühere Versionen verwenden, wird empfohlen, so bald wie möglich auf die neueste Version von License Server für Windows zu migrieren.

Unterstützte Long Term Service Release (LTSRs)-Version

Informationen zu unterstützten Versionen von Current Release (CRs), Long Term Service Release (LTSRs) und mindestens kompatiblen LS-Versionen finden Sie in der Dokumentation von aktuellen Version von Citrix Virtual Apps and Desktops.

Anzeigen der Lizenzinformationen

Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**. Eine Zusammenfassung der Lizenznutzung sowie Einstellungen für die Site werden zusammen mit einer Liste aller Lizenzen angezeigt, die aktuell auf dem angegebenen Lizenzserver installiert sind.

Herunterladen einer Lizenz von Citrix:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Lizenzen zuteilen**.
3. Geben Sie den Lizenzzugangscode an, der per E-Mail von Citrix bereitgestellt wird.
4. Wählen Sie ein Produkt aus und klicken Sie auf **Lizenzen zuteilen**. Alle Lizenzen, die für das Produkt verfügbar sind, sind zugeteilt und heruntergeladen. Wenn Sie alle Lizenzen für einen bestimmten Lizenzzugangscode zuteilen und herunterladen, können Sie den Lizenzzugangscode nicht erneut verwenden. Zum Durchführen weiterer Transaktionen mit diesem Code melden Sie sich bei My Account an.

Hinzufügen von Lizenzen, die auf dem lokalen Computer oder im Netzwerk gespeichert sind:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Lizenzen hinzufügen**.
3. Navigieren Sie zu einer Lizenzdatei und fügen Sie sie dem Lizenzserver hinzu.

Ändern des Lizenzservers:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Lizenzserver ändern**.
3. Geben Sie die Adresse des Lizenzservers im Format "Name:Port"an ("Name"= DNS-, NetBIOS- oder IP-Adresse). Wenn Sie keine Portnummer angeben, wird der Standardport (27000) verwendet.

Auswählen des Lizenztyps:

- Beim Konfigurieren der Site werden Sie nach Angabe des Lizenzservers aufgefordert, den zu verwendenden Lizenztyp auszuwählen. Stehen auf dem Server keine Lizenzen zur Verfügung, wird automatisch die Option zur Verwendung des Produkts während einer 30-tägigen Testphase ohne Lizenz ausgewählt.
- Stehen auf dem Server Lizenzen zur Verfügung, werden die entsprechenden Informationen angezeigt. Der Benutzer kann dann die gewünschte Lizenz auswählen. Alternativ können Sie dem Server eine Lizenzdatei hinzufügen und diese dann auswählen.

Ändern von Produktedition und Lizenzierungsmodell:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Wählen Sie im Aktionsbereich **Produktedition bearbeiten**.
3. Aktualisieren Sie die entsprechenden Optionen.

Um auf die License Administration Console zuzugreifen, wählen Sie im Aktionsbereich die Option **License Administration Console**. Die Konsole wird normalerweise sofort angezeigt. Wenn das Dashboard jedoch mit Kennwortschutz konfiguriert wurde, werden Sie aufgefordert, die Anmeldeinformationen für die License Administration Console einzugeben. Informationen zur Verwendung der Konsole finden Sie in der Dokumentation zur Lizenzierung.

Hinzufügen eines Lizenzadministrators:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Klicken Sie im mittleren Bereich auf die Registerkarte "Lizenzierungsadministratoren".
3. Wählen Sie im Aktionsbereich **Lizenzierungsadministrator hinzufügen**.
4. Navigieren Sie zu dem Benutzer, den Sie als Administrator hinzufügen möchten, und wählen Sie die Berechtigungen.

Ändern der Berechtigungen eines Lizenzierungsadministrators oder Löschen eines Lizenzierungsadministrators:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Klicken Sie im mittleren Bereich auf die Registerkarte "Lizenzierungsadministratoren"und wählen Sie den Administrator.
3. Wählen Sie im Aktionsbereich **Lizenzierungsadministrator bearbeiten** bzw. **Lizenzierungsadministrator löschen**.

Hinzufügen einer Lizenzierungsadministratorgruppe:

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Klicken Sie im mittleren Bereich auf die Registerkarte "Lizenzierungsadministratoren".
3. Wählen Sie im Aktionsbereich **Lizenzierungsadministratorengruppe hinzufügen**.
4. Navigieren Sie zu der Gruppe, deren Mitglieder Sie als Administratoren hinzufügen möchten, und wählen Sie die Berechtigungen. Beim Hinzufügen einer Active Directory-Gruppe werden den Benutzern dieser Gruppe Lizenzierungsadministratorberechtigungen erteilt.

Ändern der Berechtigungen einer Lizenzierungsadministratorengruppe oder Löschen einer Lizenzierungsadministratorengruppe

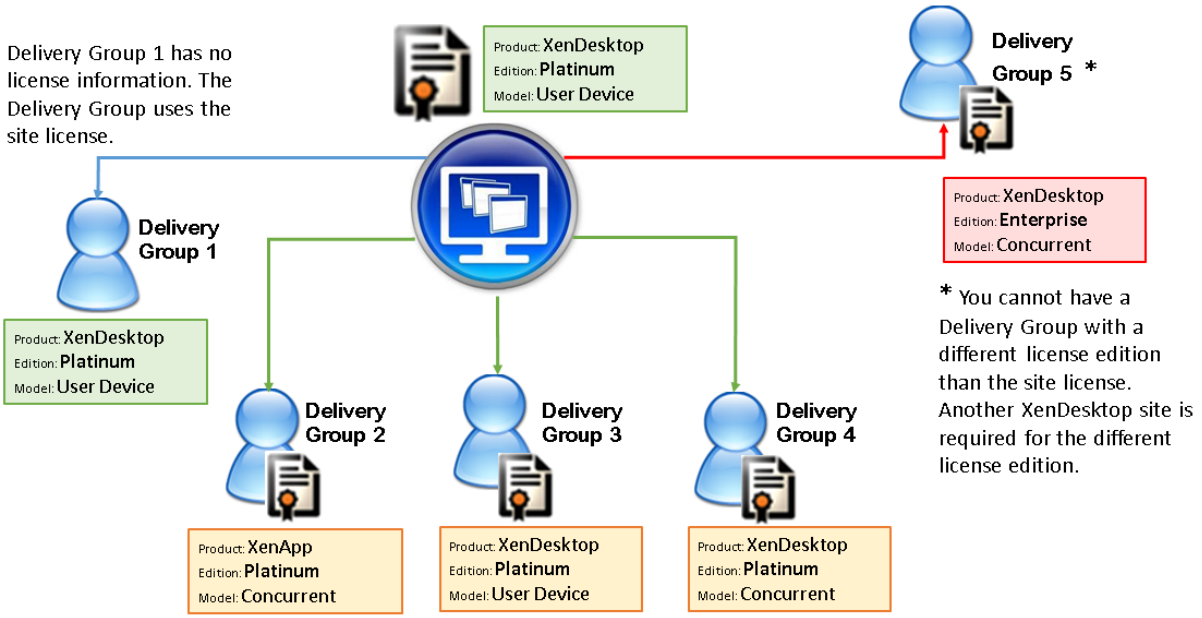
1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Lizenzierung**.
2. Klicken Sie im mittleren Bereich auf die Registerkarte "Lizenzierungsadministratoren"und wählen Sie die Administratorengruppe.
3. Wählen Sie im Aktionsbereich **Lizenzierungsadministratorengruppe bearbeiten** bzw. **Lizenzierungsadministratorengruppe löschen**.

Multityplizenzierung

August 18, 2021

Die Multityplizenzierung unterstützt den Verbrauch verschiedenartiger Lizenzen für Bereitstellungsgruppen in derselben XenApp- oder XenDesktop-Site. Ein **Typ** ist eine Einzelkombination aus Produkt-ID (XDT, MPS) und Modell (UserDevice, Concurrent). Für die Bereitstellungsgruppe muss die für die Site festgelegte Produktedition verwendet werden.

Wenn die Multityplizenzierung nicht konfiguriert ist, können unterschiedliche Lizenztypen nur dann verwendet werden, wenn sie für vollständig separate Sites konfiguriert sind. Für die Bereitstellungsgruppen wird die Sitelizenz verwendet.



Zur Suche von Bereitstellungsgruppen, die verschiedene Arten von Lizenzen verbrauchen, verwenden Sie folgende Broker-PowerShell-Cmdlets:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Zum Installieren von Lizenzen verwenden Sie:

- Citrix Studio
- Citrix Licensing Manager
- License Administration Console
- citrix.com

Das Subscription Advantage-Datum ist spezifisch für die Lizenzdatei, jedes Produkt und das Modell. Bereitstellungsgruppen mit unterschiedlichen Einstellungen können unterschiedliche Subscription Advantage-Daten haben.

Broker PowerShell SDK

Das Objekt **DesktopGroup** hat zwei Eigenschaften, die Sie mit den Cmdlets “New-BrokerDesktopGroup” und “Set-BrokerDesktopGroup”bearbeiten können.

Name	Wert	Einschränkung
LicenseModel	Auflistung (Concurrent oder UserDevice) des Lizenzierungsmodells für die Gruppe	Wenn die Featureumschaltung deaktiviert ist, kann keine Eigenschaft festgelegt werden.
ProductCode	Textzeichenfolge mit der Produkt-ID für die Gruppe (XDT bei XenDesktop oder MPS bei XenApp)	Wenn die Featureumschaltung deaktiviert ist, kann keine Eigenschaft festgelegt werden.

New-BrokerDesktopGroup

Erstellt eine Desktopgruppe zur Verwaltung der Vermittlung von Desktopgruppen. Weitere Informationen zu diesem Cmdlet finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/.

Set-BrokerDesktopGroup

Deaktiviert oder aktiviert die vorhandene Broker-Desktopgruppe oder ändert deren Einstellungen. Weitere Informationen zu diesem Cmdlet finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

Get-BrokerDesktopGroup

Ruft Desktopgruppen ab, die den angegebenen Kriterien entsprechen. Die Ausgabe des Cmdlets "Get-BrokerDesktopGroup"enthält die Eigenschaften ProductCode und LicenseModel der Gruppe. Wenn die Eigenschaften nicht mit New-BrokerDesktopGroup oder Set-BrokerDesktopGroup festgelegt wurden, werden Null-Werte zurückgegeben. Im Fall eines Null-Werts werden das Site-übergreifende Lizenzierungsmodell und der Site-übergreifende Produktcode verwendet. Weitere Informationen zu diesem Cmdlet finden Sie unter https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

Konfigurieren verschiedener Lizenzprodukte und -modelle pro Bereitstellungsgruppe

1. Öffnen Sie PowerShell mit Administratorrechten und fügen Sie das Citrix Snap-In hinzu.

2. Führen Sie den Befehl **Get-BrokerDesktopGroup –Name "DeliveryGroupName"**, um die aktuelle Lizenzkonfiguration anzuzeigen. Suchen Sie die Parameter **LicenseModel** und **ProductCode**. Wenn Sie diese Parameter noch nicht konfiguriert haben, sind sie möglicherweise leer.

   > Hinweis:
   >
   > Wenn für eine Bereitstellungsgruppe keine Lizenzinformationen festgelegt sind, wenden Sie die **Sitelizenz auf Siteebene** an.

3. Um das Lizenzmodell zu ändern, führen Sie den Befehl **Set-BrokerDesktopGroup –Name "DeliveryGroupName"–LicenseModel LicenseModel** aus.
4. Um das Lizenzprodukt zu ändern, führen Sie den Befehl **Set-BrokerDesktopGroup –Name "DeliveryGroupName"–ProductCode ProductCode** aus.
5. Geben Sie den Befehl **Get-BrokerDesktopGroup –Name "DeliveryGroupName"** ein, um die Änderungen zu überprüfen.

   > Hinweis:
   >
   > Sie können keine Editionen mischen (z. B. Premium und Advanced).

6. Um die Lizenzkonfiguration zu entfernen, führen Sie oben beschriebenen **Set-BrokerDesktopGroup**-Befehle aus und legen Sie den Wert auf **$null** fest.

   > Hinweis:
   >
   > In Studio wird die Lizenzkonfiguration nicht für jede Bereitstellungsgruppe angezeigt. Verwenden Sie PowerShell, um die aktuelle Konfiguration anzuzeigen.

Beispiel

Das nachfolgende PowerShell-Cmdlet-Beispiel zeigt die Einstellung der Multityplizenzierung für zwei bestehende Bereitstellungsgruppen und die Erstellung und Einstellung einer dritten Bereitstellungsgruppe.

Zum Ermitteln von Lizenzprodukt und Lizenzmodell einer Bereitstellungsgruppe verwenden Sie das PowerShell-Cmdlet **Get-BrokerDesktopGroup**.

1. Zunächst werden die erste Bereitstellungsgruppe für XenApp sowie "Concurrent"festgelegt. **Set-BrokerDesktopGroup -Name "Bereitstellungsgruppe für XenApp Platinum Concurrent"-ProductCode MPS -LicenseModel Concurrent**
2. Nun werden die zweite Bereitstellungsgruppe für XenDesktop sowie "Concurrent"festgelegt. **Set-BrokerDesktopGroup -Name "Bereitstellungsgruppe für XenDesktop Platinum Concurrent"-ProductCode XDT -LicenseModel Concurrent**

3. Anschließend wird die dritte Bereitstellungsgruppe für XenDesktop und “UserDevice”erstellt und eingerichtet.
   New-BrokerDesktopGroup -Name “Bereitstellungsgruppe für Bereitstellungsgruppe für XenDesktop Platinum UserDevice”-PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Besondere Erwägungen

Die Multityplizenzierung funktioniert anders als die normale XenApp- und XenDesktop-Lizenzierung.

Es gibt keine Warnungen und Benachrichtigungen von Director oder Studio:

- Keine Informationen über ein mögliches Erreichen des Lizenzlimits und des Auslösens bzw. Ablaufs des Zusatzkulanzzeitraums
- Keine Benachrichtigung bei Problemen mit einer bestimmten Gruppe

Anwendungen

August 18, 2021

Einführung

Wenn in Ihrer Bereitstellung nur Bereitstellungsgruppen (und keine Anwendungsgruppen) verwendet werden, fügen Sie den Bereitstellungsgruppen Anwendungen hinzu. Wenn Sie auch Anwendungsgruppen verwenden, sollten Sie die Anwendungen den Anwendungsgruppen hinzufügen. Diese Vorgehensweise vereinfacht die Verwaltung. Eine Anwendung muss immer zu mindestens einer Bereitstellungsgruppe oder Anwendungsgruppe gehören.

Im Assistenten zum Hinzufügen von Anwendungen können Sie Bereitstellungsgruppen oder Anwendungsgruppen auswählen, aber nicht beides. Sie können zwar später die Gruppenzuordnung einer Anwendung ändern (z. B. können Sie eine Anwendung von einer Anwendungsgruppe in eine Bereitstellungsgruppe verschieben), jedoch wird vom Hinzufügen dieser Komplexität abgeraten. Ihre Anwendungen sollten in einem Gruppentyp sein.

Wenn Sie eine Anwendung mehreren Bereitstellungsgruppen oder Anwendungsgruppen zuordnen, kann ein Anzeigeproblem auftreten, falls Sie nicht für alle betroffenen Bereitstellungsgruppen die Berechtigung zum Anzeigen der Anwendung haben. Wenden Sie sich in diesem Fall an einen Administrator mit mehr Berechtigungen oder bitten Sie um eine Ausweitung Ihrer Berechtigungen auf alle Gruppen, denen die Anwendung zugeordnet wurde.

Wenn Sie zwei Anwendungen mit dem gleichen Namen (möglicherweise aus verschiedenen Gruppen) den gleichen Benutzern bereitstellen, ändern Sie in Studio die Eigenschaft "Anwendungsname (Benutzer)", sonst wird den Benutzern der Name in Citrix Receiver doppelt angezeigt.

Sie können Anwendungseigenschaften (Einstellungen) beim Hinzufügen oder später ändern. Beim Hinzufügen der Anwendung oder später können Sie zudem den Anwendungsordner ändern, in dem die Anwendung gespeichert wird.

Weitere Informationen:

- Informationen zu Bereitstellungsgruppen finden Sie unter Erstellen von Bereitstellungsgruppen.
- Informationen zu Anwendungsgruppen finden Sie unter Erstellen von Anwendungsgruppen.
- Informationen zu Tags, die Sie Anwendungen hinzufügen können, finden Sie unter Tags.

Hinzufügen von Anwendungen

Beim Erstellen einer Bereitstellungsgruppe oder Anwendungsgruppe können Sie der Gruppe Anwendungen hinzufügen. Die dazu erforderlichen Schritte werden in den Artikeln "Erstellen von Bereitstellungsgruppen"und "Erstellen von Anwendungsgruppen"beschrieben. Im Folgenden wird beschrieben, wie Sie Anwendungen nach dem Erstellen einer Gruppe hinzufügen.

Nützliche Info:

- Sie können Remote-PC-Zugriff-Bereitstellungsgruppen keine Anwendungen hinzufügen.
- Sie können mit dem Assistenten zum Hinzufügen von Anwendungen keine Anwendungen aus Bereitstellungsgruppen oder Anwendungsgruppen entfernen. Dies ist ein separater Vorgang.

Hinzufügen von Anwendungen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und dann im Aktionsbereich **Anwendungen hinzufügen**.
2. Der Assistent zum Hinzufügen von Anwendungen wird mit der **Einführungsseite** gestartet, die Sie für zukünftige Starts des Assistenten deaktivieren können.
3. Der Assistent führt Sie durch die im Folgenden beschriebenen Seiten "Gruppen", "Anwendungen"und "Zusammenfassung". Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur Seite "Zusammenfassung"gelangen.

Alternativen für Schritt 1, wenn Sie Anwendungen einer einzelnen Bereitstellungsgruppe oder Anwendungsgruppe hinzufügen möchten:

- Zum Hinzufügen von Anwendungen zu einer einzelnen Bereitstellungsgruppe wählen Sie in Schritt 1 im Studio-Navigationsbereich **Bereitstellungsgruppe**, wählen Sie dann im mittleren Bereich eine Bereitstellungsgruppe aus und im Aktionsbereich **Anwendungen hinzufügen**. Der Assistent zeigt die Seite **Gruppen** nicht an.

- Zum Hinzufügen von Anwendungen zu einer Anwendungsgruppe wählen Sie in Schritt 1 im Studio-Navigationsbereich **Anwendungen**, wählen Sie dann im mittleren Bereich eine **Anwendungsgruppe** aus und wählen Sie im Aktionsbereich unter dem Namen der Anwendungsgruppe den Eintrag **Anwendungen hinzufügen**. Der Assistent zeigt die Seite **Gruppen** nicht an.

Gruppen

Auf dieser Seite werden alle Bereitstellungsgruppen der Site aufgelistet. Wenn Sie auch Anwendungsgruppen erstellt haben, werden die Anwendungsgruppen und Bereitstellungsgruppen aufgeführt. Sie können in einer der Gruppen eine Auswahl treffen, aber nicht in beiden Gruppen. Das heißt, Sie können Anwendungen nicht gleichzeitig einer Anwendungsgruppe und einer Bereitstellungsgruppe hinzufügen. Im Allgemeinen gilt, wenn Sie Anwendungsgruppen verwenden, sollten Anwendungen Anwendungsgruppen und nicht Bereitstellungsgruppen hinzugefügt werden.

Beim Hinzufügen einer Anwendung müssen Sie das Kontrollkästchen mindestens einer Bereitstellungsgruppe (oder Anwendungsgruppe, falls verfügbar) aktivieren, da eine Anwendung immer mindestens einer Gruppe zugeordnet sein muss.

Anwendungen

Klicken Sie auf die Dropdownliste **Hinzufügen**, um die Anwendungsquellen anzuzeigen.

- **Vom Startmenü:** Anwendungen, die auf einer Maschine in den ausgewählten Bereitstellungsgruppen erkannt werden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf OK.

Diese Quelle kann nicht ausgewählt werden, wenn Sie (1) Anwendungsgruppen gewählt haben, denen keine Bereitstellungsgruppen zugeordnet sind, (2) Anwendungsgruppen gewählt haben, deren zugeordnete Bereitstellungsgruppen keine Maschinen enthalten, oder (3) eine Bereitstellungsgruppe gewählt haben, die keine Maschinen enthält.

- **Manuell definiert:** Anwendungen in der Site oder an einem anderen Ort in Ihrem Netzwerk. Wenn Sie diese Quelle auswählen, wird eine neue Seite geöffnet. Geben Sie hier den Pfad zur ausführbaren Datei, das Arbeitsverzeichnis, optionale Befehlszeilenargumente und Anzeigenamen für Administratoren und Benutzer ein. Wenn Sie diese Informationen eingegeben haben, klicken Sie auf OK.
- **Vorhandene:** Anwendungen, die der Site bereits hinzugefügt wurden. Wenn Sie diese Quelle wählen, wird eine neue Seite mit der Liste der erkannten Anwendungen angezeigt. Aktivieren Sie die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf OK.

Diese Quelle kann nicht ausgewählt werden, wenn es in der Site keine Anwendungen gibt.

- **App-V:** Anwendungen in App-V-Paketen. Wenn Sie diese Quelle wählen, wird eine neue Seite geöffnet, in der Sie den App-V-Server oder die Anwendungsbibliothek auswählen. Aktivieren Sie dort die Kontrollkästchen der gewünschten Anwendungen und klicken Sie auf OK. Weitere Informationen finden Sie im Artikel App-V.

Diese Quelle kann nicht ausgewählt werden, wenn App-V nicht für die Site konfiguriert ist.

- **Anwendungsgruppe:** Anwendungsgruppen. Wenn Sie diese Quelle auswählen, wird eine neue Seite mit einer Liste der Anwendungsgruppen gestartet. (Zwar werden auch die Anwendungen jeder Gruppe angezeigt, aber Sie können nur die Gruppe, nicht die einzelnen Anwendungen auswählen.) Alle aktuellen und zukünftigen Anwendungen in den ausgewählten Gruppen werden hinzugefügt. Aktivieren Sie die Kontrollkästchen der Anwendungsgruppen, die Sie hinzufügen möchten, und klicken Sie auf OK.

Diese Quelle kann nicht ausgewählt werden, (1) wenn keine Anwendungsgruppen vorhanden sind oder (2) wenn die ausgewählten Bereitstellungsgruppen keine Anwendungsgruppen unterstützen (z. B. Bereitstellungsgruppen mit statisch zugewiesenen Maschinen).

In der Tabelle wurde schon darauf hingewiesen, dass einige Quellen in der Dropdownliste “Hinzufügen”nicht ausgewählt werden können, wenn keine gültige Quelle des Typs vorhanden ist. Quellen, die nicht kompatibel sind (z. B. können Sie Anwendungsgruppen keine Anwendungsgruppen hinzufügen), werden nicht in der Dropdownliste angezeigt. Anwendungen, die den ausgewählten Gruppen bereits hinzugefügt wurden, können nicht ausgewählt werden.

Um eine Anwendung von einer zugeordneten AppDisk hinzuzufügen, wählen Sie **Vom Startmenü**. Wenn die Anwendung dort nicht verfügbar ist, wählen Sie **Manuell** und geben Sie die Details an. Wenn ein Ordnerzugriffsfehler auftritt, konfigurieren Sie den Ordner als freigegeben und versuchen Sie erneut, die Anwendung unter Auswahl von **Manuell** hinzuzufügen.

Sie können die Eigenschaften einer Anwendung (Einstellungen) auf dieser Seite oder später ändern.

Standardmäßig werden hinzugefügte Anwendungen in einem Anwendungsordner mit dem Namen “Applications”abgelegt. Sie können die Anwendung auf dieser Seite oder später ändern. Wenn Sie eine Anwendung hinzufügen und es bereits eine Anwendung mit dem gleichen Namen im gleichen Ordner gibt, werden Sie aufgefordert, die neue Anwendung umzubenennen. Übernehmen Sie den angebotenen neuen Namen oder lehnen Sie ihn ab und benennen Sie die Anwendung um oder wählen Sie einen anderen Ordner. Wenn beispielsweise “App”im Ordner “Applications”bereits vorhanden ist und Sie versuchen, dem Ordner eine andere Anwendung mit demselben Namen hinzuzufügen, wird der neue Name “App_1”angeboten.

Zusammenfassung

Wenn Sie 10 oder weniger Anwendungen hinzufügen, werden ihre Namen in der Liste **Hinzuzufügende Anwendungen** aufgeführt. Wenn Sie mehr als 10 Anwendungen hinzufügen, wird die Gesamtzahl angegeben.

Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Ändern der Gruppenzuordnung einer Anwendung

Nach dem Hinzufügen einer Anwendung können Sie die Bereitstellungsgruppen und Anwendungsgruppen ändern, denen die Anwendung zugeordnet ist.

Mit Drag & Drop können Sie eine Anwendung einer zusätzlichen Gruppe zuordnen. Dies ist eine Alternative zum Verwenden der Befehle im Aktionsbereich.

Wenn eine Anwendung mehr als einer Bereitstellungsgruppe oder mehr als einer Anwendungsgruppe zugeordnet ist, können Sie mit der Gruppenpriorität die Reihenfolge angeben, in der Gruppen nach Anwendungen durchsucht werden. Standardmäßig haben alle Gruppen Priorität 0 (die höchste Priorität). Für Gruppen mit derselben Priorität erfolgt Lastausgleich.

Eine Anwendung kann Bereitstellungsgruppen zugeordnet sein, die freigegebene (nicht private) Maschinen zum Bereitstellen von Anwendungen enthalten. Sie können auch Bereitstellungsgruppen mit freigegebenen Maschinen auswählen, die nur Desktops bereitstellen, wenn (1) die Bereitstellungsgruppe freigegebene Maschinen enthält und mit einer früheren XenDesktop 7.x-Version erstellt wurde und (2) Sie die Berechtigung zum Bearbeiten von Bereitstellungsgruppen haben. Der Bereitstellungsgruppentyp wird automatisch in "Desktops und Anwendungen"konvertiert, wenn für das Eigenschaftendialogfeld ein Commit ausgeführt wird.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und dann im mittleren Bereich die Anwendung.
2. Wählen Sie im Aktionsbereich **Eigenschaften** aus.
3. Wählen Sie die Seite **Gruppen** aus.
4. Zum Hinzufügen einer Gruppe klicken Sie auf die Dropdownliste **Hinzufügen** und wählen Sie **Anwendungsgruppen** oder **Bereitstellungsgruppen**. (Wenn Sie keine Anwendungsgruppen erstellt haben, werden nur Bereitstellungsgruppen angezeigt.) Wählen Sie dann mindestens eine verfügbare Gruppe. Gruppen, die mit der Anwendung nicht kompatibel oder der Anwendung bereits zugeordnet sind, können nicht ausgewählt werden.
5. Zum Entfernen von Gruppen wählen Sie mindestens eine Gruppe aus und klicken Sie auf **Entfernen**. Wenn das Löschen einer Gruppenzuordnung dazu führt, dass die Anwendung keiner Anwendungsgruppe oder Bereitstellungsgruppe mehr zugeordnet ist, werden Sie vor dem Löschen der Anwendung gewarnt.

6. Zum Ändern der Priorität einer Gruppe wählen Sie eine Gruppe aus und klicken Sie auf **Priorität bearbeiten**. Wählen Sie einen Wert für die Priorität aus und klicken Sie auf **OK**.
7. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Duplizieren, Aktivieren, Deaktivieren, Umbenennen und Löschen von Anwendungen

Folgende Aktionen sind verfügbar:

- **Duplizieren:** Sie können Anwendungen duplizieren, um eine Anwendungsversion mit anderen Parametern oder Eigenschaften zu erstellen. Wenn Sie eine Anwendung duplizieren, wird diese automatisch mit einem eindeutigen Suffix umbenannt und neben die ursprüngliche Anwendung platziert. Sie können eine Anwendung auch duplizieren und einer anderen Gruppe hinzufügen. (Neben dem Duplizieren ist die einfachste Möglichkeit zum Verschieben einer Datei Drag & Drop.)
- **Aktivieren oder Deaktivieren:** Das Aktivieren und Deaktivieren einer Anwendung ist eine andere Aktion als das Aktivieren und Deaktivieren einer Bereitstellungsgruppe oder Anwendungsgruppe.
- **Umbenennen:** Sie können jeweils nur eine Anwendung umbenennen. Wenn Sie eine Anwendung umbenennen und eine Anwendung mit demselben Namen ist bereits im gleichen Ordner oder in der gleichen Gruppe vorhanden, dann werden Sie aufgefordert, einen anderen Namen anzugeben.
- **Löschen:** Beim Löschen einer Anwendung wird sie aus den Bereitstellungsgruppen und Anwendungsgruppen entfernt, denen sie zugeordnet war, aber nicht aus der Quelle, aus der sie ursprünglich hinzugefügt wurde. Das Löschen einer Anwendung ist nicht dasselbe wie das Entfernen einer Anwendung aus einer Bereitstellungsgruppe oder Anwendungsgruppe.

Duplizieren, Aktivieren, Deaktivieren, Umbenennen und Löschen von Anwendungen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie mindestens eine Anwendung im mittleren Bereich aus und dann die gewünschte Aufgabe im Aktionsbereich.
3. Bestätigen Sie die Aktion, wenn Sie dazu aufgefordert werden.

Entfernen von Anwendungen aus einer Bereitstellungsgruppe

Eine Anwendung muss mindestens einer Bereitstellungsgruppe oder Anwendungsgruppe zugeordnet sein. Wenn Sie versuchen, eine Anwendung aus einer Bereitstellungsgruppe zu entfernen und dies bedeuten würde, dass die Anwendung keiner Bereitstellungsgruppe oder Anwendungsgruppe mehr

zugeordnet wäre, werden Sie gewarnt, dass die Anwendung gelöscht wird, wenn Sie fortfahren. Wenn die Anwendung gelöscht wird und Sie möchten sie bereitstellen, müssen Sie die Anwendung erneut aus einer gültigen Quelle hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich **Bereitstellungsgruppen** aus.
2. Wählen Sie eine Bereitstellungsgruppe aus. Wählen Sie im mittleren Bereich unten die Registerkarte **Anwendungen** und dann die Anwendung, die Sie löschen möchten.
3. Wählen Sie im Aktionsbereich **Anwendungsgruppe entfernen**.
4. Bestätigen Sie das Entfernen.

Entfernen von Anwendungen aus einer Anwendungsgruppe

Eine Anwendung muss mindestens zu einer Bereitstellungsgruppe oder Anwendungsgruppe gehören. Wenn Sie versuchen, eine Anwendung aus einer Anwendungsgruppe zu entfernen und dies bedeuten würde, dass die Anwendung keiner Bereitstellungsgruppe oder Anwendungsgruppe mehr zugeordnet wäre, werden Sie gewarnt, dass die Anwendung gelöscht wird, wenn Sie fortfahren. Wenn die Anwendung gelöscht wird und Sie möchten sie bereitstellen, müssen Sie die Anwendung erneut aus einer gültigen Quelle hinzufügen.

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie im mittleren Bereich die Anwendungsgruppe und wählen Sie dann mindestens eine Anwendung aus.
3. Wählen Sie im Aktionsbereich **Aus Anwendungsgruppe entfernen**.
4. Bestätigen Sie das Entfernen.

Ändern der Anwendungseigenschaften

Sie können jeweils nur die Eigenschaften einer Anwendung ändern.

Ändern der Eigenschaften einer Anwendung

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen**.
2. Wählen Sie die Anwendung und dann im Aktionsbereich **Anwendungseigenschaften bearbeiten**.
3. Wählen Sie die Seite mit der Eigenschaft, die Sie ändern möchten.
4. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

In der folgenden Liste wird die Seite in Klammern angegeben.

- Kategorie/Ordner, in der/dem die Anwendung in Receiver angezeigt wird (Bereitstellung)

- Befehlszeilenargumente –siehe Abschnitt "Übergeben von Parametern an veröffentlichte Anwendungen"(Standort)
- Bereitstellungsgruppen und Anwendungsgruppen, in denen die Anwendung verfügbar ist (Gruppen)
- Beschreibung (Identifizierung)
- Dateinamenerweiterungen und Dateitypzuordnung: die Erweiterungen, die von der Anwendung automatisch geöffnet werden (Dateitypzuordnung)
- Symbol (Bereitstellung)
- Schlüsselwörter für StoreFront (Identifizierung)
- Limits –weitere Informationen finden Sie unter "Konfigurieren von Anwendungslimits"(Bereitstellung)
- Name: die Namen, die Benutzer und Administrator sehen (Identifizierung)
- Pfad zur ausführbaren Datei –siehe Abschnitt "Übergeben von Parametern an veröffentlichte Anwendungen"(Standort)
- Verknüpfung auf dem Desktop des Benutzers: aktivieren oder deaktivieren (Bereitstellung)
- Sichtbarkeit: legt fest, welche Benutzer die Anwendung in Citrix Receiver sehen; eine unsichtbare Anwendung kann trotzdem gestartet werden, damit sie auch nicht verfügbar ist, fügen Sie sie einer anderen Gruppe hinzu (Sichtbarkeit beschränken)
- Arbeitsverzeichnis (Standort)

Anwendungsänderungen werden evtl. für aktuelle Anwendungsbenutzer erst wirksam, wenn diese ihre Sitzung abmelden.

Konfigurieren von Anwendungslimits

Durch Konfigurieren von Anwendungslimits können Sie die Anwendungsnutzung verwalten. Sie können z. B. die Zahl der Benutzer, die gleichzeitig auf eine Anwendung zugreifen, beschränken. Analog dazu können Sie über Anwendungslimits die Zahl gleichzeitiger Instanzen ressourcenintensiver Anwendungen limitieren, um die Serverleistung zu gewährleisten und eine Dienstverschlechterung zu vermeiden.

Diese Funktion limitiert die Anzahl der vom Controller vermittelten Anwendungsstarts (z. B. von Citrix Receiver und StoreFront) und nicht die Anzahl ausgeführter Anwendungen, die auf andere Weise gestartet werden konnten. Anwendungslimits helfen daher bei der Verwaltung der gleichzeitigen Nutzung, gestatten jedoch nicht in allen Szenarios eine Erzwingung. Anwendungslimits können beispielsweise nicht angewendet werden, wenn der Controller eine geleaste Verbindung hat.

Standardmäßig besteht kein Limit für die Anzahl gleichzeitig ausgeführter Anwendungsinstanzen. Sie können eines oder auch beide der zwei möglichen Anwendungslimits konfigurieren:

- Maximale Anzahl gleichzeitiger Instanzen einer Anwendung für alle Benutzer in der Bereitstellungsgruppe

- Eine Anwendungsinstanz pro Benutzer in der Bereitstellungsgruppe

Wenn ein Limit konfiguriert ist und ein Benutzer versucht, eine Anwendungsinstanz zu starten, durch die das Limit überschritten würde, wird eine Fehlermeldung generiert.

Beispiele für Anwendungslimits:

- **Maximale Anzahl gleichzeitiger Instanzen:** Sie konfigurieren für eine Bereitstellungsgruppe die maximal zulässige Anzahl gleichzeitiger Instanzen der Anwendung "Alpha"mit 15. Anschließend werden in der Bereitstellungsgruppe 15 Instanzen dieser Anwendung gleichzeitig ausgeführt. Versucht nun ein Benutzer in der Bereitstellungsgruppe, Alpha zu starten, wird eine Fehlermeldung generiert und Alpha wird nicht gestartet, da hierdurch das konfigurierte Limit von 15 überschritten würde.
- **Limit von einer Instanz pro Benutzer:** In einer anderen Bereitstellungsgruppe haben Sie für die Anwendung "Beta"das Limit von einer Instanz pro Benutzer festgelegt. Benutzer Hermann startet die Anwendung Beta. Eine Weile später versucht er eine weitere Instanz von Beta zu starten. Eine Fehlermeldung wird generiert und Beta wird nicht gestartet, da dadurch das Limit überschritten würde.
- **Maximale Anzahl gleichzeitiger Instanzen plus Limit von einer Instanz pro Benutzer:** In einer anderen Bereitstellungsgruppe legen Sie die maximal zulässige Anzahl gleichzeitiger Instanzen der Anwendung "Delta"auf 10 fest und aktivieren außerdem das Limit von einer Instanz pro Benutzer. Werden anschließend alle zehn Instanzen von Delta ausgeführt, wird bei jedem weiteren Versuch, die Anwendung in der Bereitstellungsgruppe zu starten, eine Fehlermeldung angezeigt und Delta nicht gestartet. Versucht ein Benutzer, der bereits eine Delta-Instanz gestartet hat, eine zweite Instanz zu starten, wird eine Fehlermeldung angezeigt und die zweite Instanz wird nicht gestartet.

Werden Anwendungsinstanzen auch über andere Methoden als das Controllerbrokering gestartet (z. B. wenn ein Controller eine geleaste Verbindung hat) und die festgelegten Limits werden überschritten, können Benutzer erst dann wieder Instanzen starten, wenn zuvor entsprechend viele Instanzen geschlossen wurden und kein Limit mehr überschritten wird. Die Instanzen, die das Limit überschreiten, werden nicht zwangsweise geschlossen, sondern können weiterlaufen, bis die Benutzer sie schließen.

Wenn Sie das Sitzungsroaming deaktivieren, deaktivieren auch das Limit einer Anwendungsinstanz pro Benutzer. Wenn Sie das Limit einer Anwendungsinstanz pro Benutzer aktivieren, konfigurieren Sie keinen der beiden Werte, durch die neue Sitzungen auf neuen Geräten zugelassen werden. Weitere Informationen zum Roaming finden Sie im Artikel Sitzungen.

Konfigurieren von Anwendungslimits

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und dann eine Anwendung.
2. Wählen Sie im Aktionsbereich **Anwendungseigenschaften bearbeiten**.

3. Wählen Sie auf der Seite **Bereitstellung** eine der folgenden Optionen aus: Wenn Sie fertig sind, klicken Sie auf **OK**, um die Änderung anzuwenden und das Dialogfeld **Anwendungseigenschaften bearbeiten** zu schließen, oder auf **Anwenden**, um die Änderung anzuwenden und das Dialogfeld **Anwendungseigenschaften bearbeiten** geöffnet zu lassen.

- Uneingeschränkte Verwendung der Anwendung zulassen. Es gibt kein Limit für die Anzahl der gleichzeitig ausgeführten Instanzen. Dies ist die Standardeinstellung.
- Limits für die Anwendung festlegen. Es sind zwei Limits, die Sie einzeln oder beide festlegen können.
  - Anzahl der gleichzeitig ausgeführten Instanzen beschränken auf:
  - Auf eine Instanz pro Benutzer beschränken

Übergeben von Parametern an veröffentlichte Anwendungen

Auf der Seite Speicherort der Eigenschaften einer Anwendung geben Sie die Befehlszeile ein und übergeben Parameter an veröffentlichte Anwendungen.

Wenn Sie einer veröffentlichten Anwendung bestimmte Dateitypen zuordnen, werden die Zeichen "%*"(Prozentzeichen und Sternchen in Anführungszeichen) an das Ende der Anwendungsbefehlszeile angehängt. Diese Symbole sind Platzhalter für Parameter, die an Benutzergeräte übergeben werden.

Sollte eine veröffentlichte Anwendung nicht wunschgemäß starten, prüfen Sie, ob in der Befehlszeile die richtigen Zeichen eingetragen sind. Standardmäßig werden die von Benutzergeräten angegebenen Parameter validiert, wenn die Symbole "%*"angehängt werden. Veröffentlichten Anwendungen, die benutzerdefinierte Parameter verwenden, die vom Benutzergerät bereitgestellt werden, werden die Zeichen "%**"an die Befehlszeile angehängt, damit die Befehlszeilenüberprüfung übersprungen wird. Sollte die Befehlszeile der betreffenden Anwendung diese Zeichen nicht enthalten, können Sie sie manuell hinzufügen.

Wenn der Pfad zur ausführbaren Datei der Anwendung Verzeichnisnamen mit Leerzeichen enthält (z. B. "C:\Program Files"), setzen Sie die Befehlszeile der Anwendung in Anführungszeichen, um anzuzeigen, dass das Leerzeichen zur Befehlszeile gehört. Setzen Sie hierfür vor und nach dem Pfad sowie vor und nach den Symbolen %* Anführungszeichen. Zwischen dem Anführungszeichen nach dem Pfad und dem Anführungszeichen vor dem Prozentzeichen muss ein Leerzeichen stehen.

Die Befehlszeile für die veröffentlichte Anwendung Windows Media Player wäre beispielsweise:

"C:\Programme\Windows Media Player\mplayer1.exe"*"%*"

Verwalten von Anwendungsordnern

Standardmäßig werden Bereitstellungsgruppen neu hinzugefügte Anwendungen in einem Ordner mit dem Namen **Applications** abgelegt. Sie können bei der Erstellung der Bereitstellungsgruppe, beim Hinzufügen einer Anwendung oder zu einem anderen Zeitpunkt einen anderen Ordner angeben.

Nützliche Info:

- Sie können den Ordner "Applications"nicht umbenennen oder löschen. Sie können aber alle Anwendungen in diesem Ordner in andere von Ihnen erstellte Ordner verschieben.
- Ein Ordnername darf 1-64 Zeichen enthalten. Leerstellen sind zugelassen.
- Ordner können bis zu fünffach verschachtelt werden.
- Ordner müssen keine Anwendungen enthalten, leere Ordner sind zugelassen.
- Ordner werden in Studio alphabetisch aufgelistet, es sei denn, Sie verschieben sie oder geben beim Erstellen einen anderen Speicherort an.
- Sie können mehr als einen Ordner mit dem gleichen Namen haben, sofern jeder einen anderen übergeordneten Ordner hat. Sie können mehr als eine Anwendung mit dem gleichen Namen haben, sofern jede in einem anderen Ordner ist.
- Zum Entfernen, Umbenennen und Löschen eines Ordners, der Anwendungen enthält, benötigen Sie für alle enthaltenen Anwendungen die Berechtigung zum Anzeigen von Anwendungen in Ordnern und die Berechtigung zum Bearbeiten der Anwendungseigenschaften.
- Die meisten der folgenden Verfahren umfassen Aktionen aus dem Bereich "Aktionen"in Studio. Alternativ können Sie Kontextmenüs oder Drag & Drop verwenden. Wenn Sie beispielsweise einen Ordner am falschen Speicherort erstellen oder ihn dorthin verschieben, können Sie ihn per Drag & Drop an den korrekten Speicherort ziehen.

Zum Verwalten von Anwendungsordnern wählen Sie im Studio-Navigationsbereich **Anwendungen**. Orientieren Sie sich an der nachfolgenden Liste.

- Zum Anzeigen aller Ordner (unter Ausschluss verschachtelter Ordner) klicken Sie oberhalb der Ordnerliste auf **Alle anzeigen**.
- Zum Erstellen eines (unverschachtelten) Ordners auf der höchsten Ebene wählen Sie den Anwendungsordner aus. Um einen neuen Ordnen unter einem vorhandenen Ordner außer Applications zu platzieren, wählen Sie diesen Ordner aus. Wählen Sie dann im Aktionsbereich **Ordner erstellen**. Geben Sie einen Namen ein.
- Zum Verschieben eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner verschieben**. Sie können immer nur einen Ordner verschieben, es sei denn, der Ordner enthält Unterordner. Tipp: Die einfachste Möglichkeit zum Verschieben von Ordnern ist das Drag & Drop.
- Zum Umbenennen eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner umbenennen**. Geben Sie einen Namen ein.

- Zum Löschen eines Ordners wählen Sie den Ordner und dann im Aktionsbereich **Ordner löschen**. Beim Löschen eines Ordners, der Anwendungen und andere Ordner enthält, werden diese Objekte auch gelöscht. Beim Löschen einer Anwendung wird die Anwendungszuweisung aus der Bereitstellungsgruppe aber nicht aus der Maschine entfernt.
- Zum Verschieben von Anwendungen in einen Ordner wählen Sie eine oder mehrere Anwendungen. Wählen Sie dann im Aktionsbereich **Anwendungsgruppe verschieben**. Wählen Sie den Ordner aus.

In den Assistenten zum Erstellen von Bereitstellungsgruppen und Anwendungsgruppen können Sie Anwendungen, die Sie hinzufügen, auf der Seite **Anwendung** auch in einem bestimmten (auch hier neu angelegten) Ordner platzieren. Standardmäßig werden hinzugefügte Anwendungen im Ordner "Applications"abgelegt. Klicken Sie auf **Ändern**, um einen Ordner auszuwählen oder zu erstellen.

Apps für die Universelle Windows-Plattform

August 18, 2021

XenApp und XenDesktop unterstützen die Verwendung von UWP-Apps (Universelle Windows-Plattform) mit VDAs auf Windows 10- und Windows Server 2016-Maschinen. Informationen zu UWP-Apps finden Sie in der folgenden Dokumentation von Microsoft:

- What is a Universal Windows Platform (UWP) app?
- Distribute offline apps
- Guide to Universal Windows Platform (UWP) apps

Der Begriff "universelle App"bezeichnet im vorliegenden Artikel durchgängig UWP-Apps.

Anforderungen und Einschränkungen

Universelle Apps werden für VDAs auf Windows 10- und Windows Server 2016-Maschinen unterstützt.

Die VDAs müssen mindestens in Version 7.11 vorliegen.

Folgende XenApp- und XenDesktop-Features werden entweder nicht unterstützt oder unterliegen Einschränkungen, wenn universelle Apps verwendet werden:

- Die Dateitypzuordnung wird nicht unterstützt.
- Der lokale App-Zugriff wird nicht unterstützt.
- Dynamische Vorschau: Bei in der Sitzungsüberlagerung ausgeführten Apps wird in der Vorschau das Standardsymbol angezeigt. Die für die dynamische Vorschau verwendeten Win32-APIs werden in universellen Apps nicht unterstützt.

- Wartungscenter-Remoting: Universelle Apps können das Wartungscenter zur Anzeige der Meldungen in der Sitzung nutzen. Leiten Sie die Meldungen zur Anzeige für den Benutzer an den Endpunkt weiter.

Das Starten universeller und anderer Apps vom gleichen Server aus wird für Windows 10-VDAs nicht unterstützt. Für Windows Server 2016 müssen universelle und andere Apps separaten Bereitstellungs- bzw. Anwendungsgruppen zugewiesen werden.

Alle auf einer Maschine installierten universellen Apps werden enumeriert. Aus diesem Grund empfiehlt Citrix, den Benutzerzugriff auf den Windows Store zu deaktivieren. Dadurch wird verhindert, dass andere Benutzer auf eine von einem Benutzer installierte universelle App zugreifen.

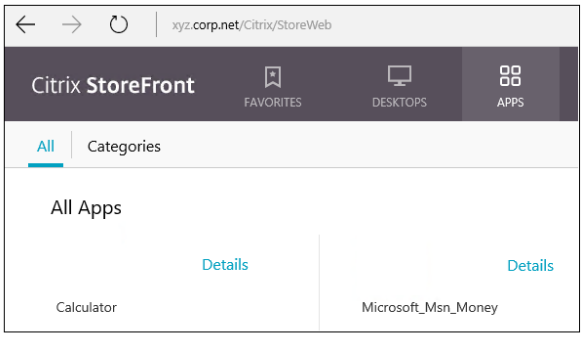
Beim Sideloading werden universelle Apps auf der Maschine installiert und sind für andere Benutzer verfügbar. Wenn ein beliebiger anderer Benutzer die App startet, wird sie installiert. Die AppX-Datenbank des Betriebssystems wird dann durch die Kennzeichnung "wie installiert"für den Benutzer aktualisiert, der die App gestartet hat.

Bei einer ordnungsgemäßen Abmeldung von einer veröffentlichten universellen App, die in einem Seamless- oder festen Fenster gestartet wurde, wird die Sitzung möglicherweise nicht geschlossen. In diesem Fall verhindern mehrere Prozesse in der Sitzung deren ordnungsgemäßes Schließen. Zur Problemlösung ermitteln Sie, welche Prozesse das Schließen der Sitzung verhindern, und fügen Sie diese dann dem Wert des Registrierungsschlüssels "LogoffCheckSysModules"hinzu. Folgen Sie hierfür den Anweisungen unter CTX891671.

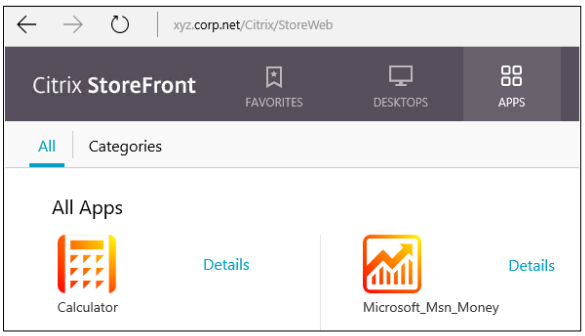
Namen und Beschreibungen universeller Apps in der Anwendungsanzeige sind möglicherweise nicht korrekt. Korrigieren Sie die betroffenen Eigenschaften beim Hinzufügen der Apps zur Bereitstellungsgruppe.

Bei jeglichen anderen Problemen lesen Sie den Artikel Bekannte Probleme.

Derzeit haben mehrere universelle Apps ein weißes Symbol, für das Transparenz aktiviert ist. Diese Symbole sind vor dem weißen Hintergrund von StoreFront nicht sichtbar. Um dieses Problem zu vermeiden, können Sie den Hintergrund ändern. Bearbeiten Sie hierfür beispielsweise auf der StoreFront-Maschine die Datei C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css. Fügen Sie am Ende der Datei Folgendes hinzu: **.storeapp-icon {background-image: radial-gradient(circle at top right, yellow, red); }**. Die Abbildung unten zeigt die Anzeige vor und nach dieser Korrektur.



Before



After

Unter Windows Server 2016 wird beim Starten einer universellen App ggf. der Server-Manager gestartet. Um dies zu verhindern, können Sie den automatischen Start des Server-Managers über den Registrierungsschlüssel "HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon" deaktivieren. Einzelheiten finden Sie unter https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

Installieren und Veröffentlichen universeller Apps

Unterstützung für universelle Apps ist standardmäßig aktiviert.

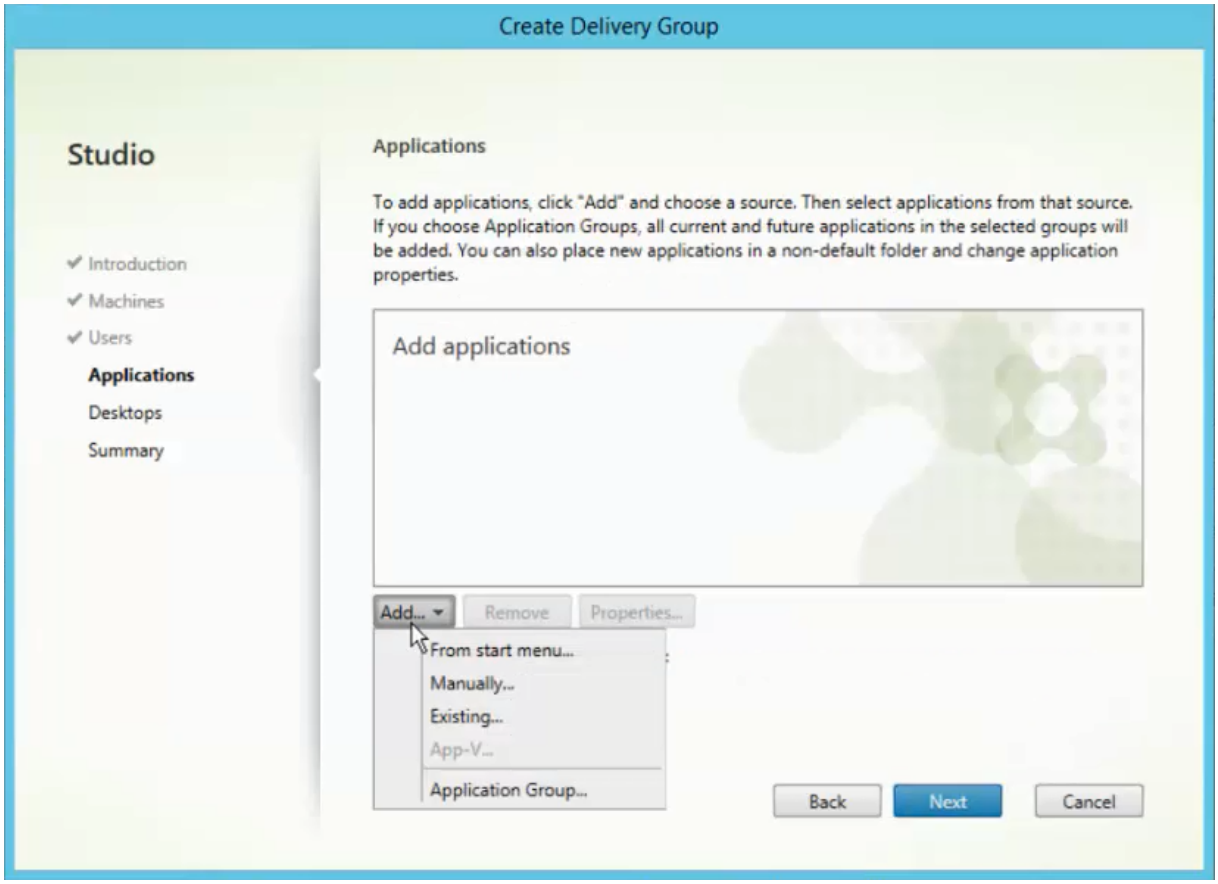
Um die Verwendung universeller Apps auf einem VDA zu deaktivieren, fügen Sie die Registrierungseinstellung **EnableUWASeamlessSupport** in HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle hinzu und legen Sie sie auf **0** fest.

Verwenden Sie zum Installieren einer oder mehrerer universeller Apps auf VDAs (oder einem Masterimage) eines der folgenden Verfahren:

- Führen Sie mit einem Tool wie der Abbildverwaltung für die Bereitstellung (DISM) eine Offlineinstallation der App aus dem Windows Store für Unternehmen für das Desktopimage durch. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/microsoft-store/distribute-offline-apps?redirectedfrom=MSDN.
- Laden Sie die Apps per Sideloading. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10?redirectedfrom=MSDN.

Zum Hinzufügen (Veröffentlichen) universeller Apps in XenApp oder XenDesktop führen Sie folgende Schritte aus:

Fügen Sie die universelle App nach deren Installation einer Bereitstellungsgruppe oder Anwendungsgruppe hinzu. Sie können dies beim Erstellen der Gruppe oder später tun. Wählen Sie auf der Seite "Anwendungen"des Assistenten als Quelle **Vom Startmenü**.



Wenn die Liste der Anwendungen angezeigt wird, aktivieren Sie die Kontrollkästchen der universellen Apps, die Sie veröffentlichen möchten. Klicken Sie auf **Weiter**.

Deinstallieren universeller Apps

Wenn Sie eine universelle App mit einem Befehl wie "Remove-AppXPackage"deinstallieren, wird diese nur für Administratoren deinstalliert. Zum Entfernen der App von Maschinen, auf denen Benutzer die App gestartet und verwendet haben, müssen Sie den Befehl zum Deinstallieren auf der jeweiligen Maschine ausführen. Sie können das AppX-Paket nicht mit einem Befehl von allen Maschinen der Benutzer deinstallieren.

Zonen

August 18, 2021

In Bereitstellungen mit weit auseinanderliegenden Standorten in einem WAN kann es zu Latenz- und Zuverlässigkeitsproblemen kommen. Es gibt zwei Möglichkeiten, diesen Herausforderungen zu

begegnen:

- Bereitstellen mehrerer Sites mit eigener SQL Server-Sitedatenbank:

Diese Option empfiehlt sich für große Unternehmen. Mehrere Sites können einzeln verwaltet werden und erfordern alle eine eigene SQL Server-Sitedatenbank. Jede Site ist eine eigenständige XenApp-Bereitstellung.

- Konfigurieren mehrerer Zonen in einer einzelnen Site:

Mit Zonen können Benutzer an entfernten Standorten eine Verbindung mit Ressourcen herstellen, ohne dass die Verbindungen durch große WAN-Segmente laufen müssen. Zonen gestatten eine effektive Siteverwaltung über eine einzelne Citrix Studio-Konsole, Citrix Director und die Sitedatenbank. Auf diese Weise können die Kosten für Bereitstellung, Personalbesetzung, Lizenzierung und Betrieb zusätzlicher Sites mit eigenen Datenbanken an entfernten Standorten gespart werden.

Zonen können bei Bereitstellungen aller Größen nützlich sein. Mit Zonen können Sie Anwendungen und Desktops näher an den Benutzern ansiedeln und so die Leistung verbessern. Aus Redundanz- und Flexibilitätsgründen ist die Installation eines oder mehrerer Controller zonenlokal möglich, jedoch nicht erforderlich.

Die Zahl der für die Site konfigurierten Controller kann die Leistung bei einigen Vorgängen (z. B. beim Hinzufügen von neuen Controllern) beeinträchtigen. Um dies zu vermeiden, sollten Sie die Zahl der Zonen in Ihrer XenApp- oder XenDesktop-Site auf maximal 50 beschränken.

> **Hinweis:**
>
> Wenn die Netzwerklatenz Ihrer Zonen 250 ms (RTT) übersteigt, empfiehlt Citrix die Bereitstellung mehrerer Sites anstelle von Zonen.

In diesem Artikel bezieht sich der Begriff "lokal"auf die jeweils behandelte Zone. "Ein VDA registriert sich bei einem lokalen Controller"bedeutet beispielsweise, dass sich der VDA bei einem Controller in der Zone registriert, in der der VDA ist.

Die Zonen in diesem Release ähneln denen in XenApp 6.5 und Vorversionen, sind mit ihnen jedoch nicht identisch. Beispielsweise gibt es in dieser Zonenimplementierung keine Datensammelpunkte. Alle Controller in einer Site kommunizieren mit einer Sitedatenbank in der primären Zone. Auch Failover und bevorzugte Zonen funktionieren in diesem Release anders.

Zonentypen

Eine Site hat immer eine primäre Zone. Sie kann auch eine oder mehrere Satellitenzonen haben. Satellitenzonen können für die Notfallwiederherstellung, entfernte Datencenter, Zweigstellen, eine Cloud oder eine Availability Zone in einer Cloud verwendet werden.

Primäre Zone

Die primäre Zone hat den Standardnamen “Primär”und umfasst SQL Server-Sitedatenbank (sowie ggf. hoch verfügbare SQL Server-Computer), Studio, Director, Citrix StoreFront, Citrix Lizenzserver und NetScaler Gateway. Die Sitedatenbank muss immer in der primären Zone sein.

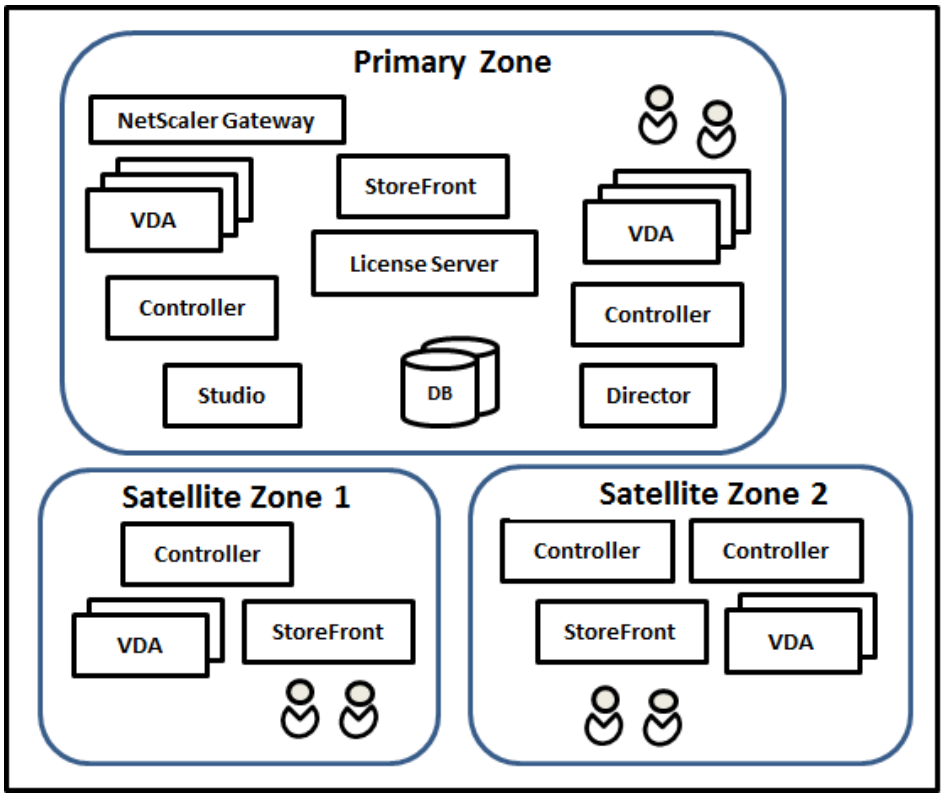
Die primäre Zone sollte aus Redundanzgründen außerdem mindestens zwei Controller enthalten und kann einen oder mehrere VDAs mit Anwendungen umfassen, die eng an die Datenbank und Infrastruktur gekoppelt sind.

Satellitenzonen

Eine Satellitenzone enthält einen oder mehrere VDAs, Controller und StoreFront- sowie NetScaler Gateway-Server. Im Normalbetrieb kommunizieren Controller in einer Satellitenzone direkt mit der Datenbank in der primären Zone.

Satellitenzonen, insbesondere große, können auch einen Hypervisor für die Bereitstellung und/oder Speicherung von Maschinen enthalten. Beim Konfigurieren einer Satellitenzone können Sie dieser eine Hypervisor- oder Clouddienstverbindung zuweisen. Alle Maschinenkataloge, die diese Verbindung verwenden, müssen in der gleichen Zone sein.

Eine Site kann je nach Anforderungen und Umgebung Satellitenzonen verschiedener Konfigurationen enthalten. Die folgende Abbildung zeigt eine primäre Zone und Beispiele von Satellitenzonen.



- Die primäre Zone enthält zwei Controller, Studio, Director, StoreFront, den Lizenzserver und die Sitedatenbank (sowie hoch verfügbare SQL Server-Bereitstellungen). Die primäre Zone enthält außerdem mehrere VDAs und ein NetScaler Gateway.
- Satellitenzone 1 –VDAs mit Controller

Satellitenzone 1 enthält einen Controller, VDAs und einen StoreFront-Server. Die VDAs in dieser Satellitenzone registrieren sich bei dem lokalen Controller. Der lokale Controller kommuniziert mit der Sitedatenbank und dem Lizenzserver in der primären Zone.

Wenn das WAN ausfällt, kann der Controller in der Satellitenzone dank Verbindungsleasing weiterhin Verbindungen mit VDAs in dieser Zone vermitteln. Eine solche Bereitstellung ist beispielsweise an Standorten nützlich, an denen Mitarbeiter über die lokale StoreFront-Site und den lokalen Controller auf ihre lokalen Ressourcen zugreifen, was möglich ist, selbst wenn die WAN-Verbindung zwischen dem Standort und dem Unternehmensnetzwerk ausfällt.

- Satellitenzone 2 –VDAs mit redundanten Controllern

Satellitenzone 2 enthält zwei Controller, VDAs und einen StoreFront-Server. Dieser Zonentyp bietet die größte Resilienz bei gleichzeitigem Ausfall des WANs und eines lokalen Controllers.

VDAs-Registrierung und Controllerfailover

Site mit primärer Zone und Satellitenzonen und VDAs, deren Version mindestens 7.7 ist:

- Ein VDA in der primären Zone registriert sich bei einem Controller in der primären Zone. Ein VDA in der primären Zone versucht nie eine Registrierung bei einem Controller in einer Satellitenzone.
- Ein VDA in einer Satellitenzone registriert sich bei einem lokalen Controller, sofern möglich. Dies ist der bevorzugte Controller. Sind keine lokalen Controller verfügbar (z. B. weil sie keine weiteren VDA-Registrierungen annehmen können oder weil sie ausgefallen sind), versucht der VDA die Registrierung bei einem Controller in der primären Zone. In diesem Fall bleibt der VDA in der primären Zone registriert, selbst wenn wieder ein Controller in der Satellitenzone verfügbar wird. Ein VDA in einer Satellitenzone versucht nie eine Registrierung bei einem Controller in einer anderen Satellitenzone.
- Wenn für die VDA-Ermittlung von Controllern die automatische Aktualisierung aktiviert ist und Sie bei der VDA-Installation eine Liste von Controlleradressen angegeben haben, wird aus dieser nach dem Zufallsprinzip ein Controller für die erste Registrierung ausgewählt, unabhängig davon, in welcher Zone der Controller residiert. Wenn die Maschine mit dem VDA neu gestartet wird, versucht dieser die Registrierung bei einem Controller in der lokalen Zone.
- Wenn ein Controller in einer Satellitenzone ausfällt, erfolgt, sofern möglich, ein Failover zu einem anderen lokalen Controller. Ist kein lokaler Controller verfügbar, erfolgt ein Failover auf einen Controller in der primären Zone.

- Wenn Sie einen Controller in eine Zone oder aus einer Zone verschieben und die automatische Aktualisierung aktiviert ist, erhalten die VDAs eine aktualisierte Liste der lokal und in der primären Zone angesiedelten Controller, anhand derer die Registrierung und die Annahme von Verbindungen erfolgt.
- Wenn Sie einen Maschinenkatalog in eine andere Zone verschieben, registrieren sich die VDAs in diesem Katalog bei Controllern in der Zone, in die Sie den Katalog verschoben haben. (Wenn Sie einen Katalog in eine Zone verschieben, die nur schlecht mit der aktuellen Zone verbunden ist (z. B. über ein Netzwerk mit hoher Latenz oder geringer Bandbreite), sollten Sie auch alle zugeordneten Hostverbindungen in dieselbe Zone verschieben.)
- Auf Controllern in der primären Zone werden Verbindungsleasingdaten für alle Zonen gespeichert. Auf Controllern in Satellitenzonen werden Verbindungsleasingdaten für die eigene Zone und die primäre Zone, jedoch nicht für die anderen Satellitenzonen gespeichert.

Wenn alle Controller in einer Site fehlschlagen:

- kann Studio keine Verbindung mit der Site herstellen.
- können keine Verbindungen mit VDAs in der primären Zone hergestellt werden.
- verschlechtert sich die Siteleistung kontinuierlich, bis die Controller in der primären Zone verfügbar werden.

Sites mit VDAs vor Version 7.7:

- VDAs in einer Satellitenzone akzeptieren Anforderungen von Controllern in der lokalen Zone und der primären Zone. (VDAs ab Version 7.7 können Controlleranforderungen aus anderen Satellitenzonen akzeptieren.)
- VDAs in einer Satellitenzone registrieren sich nach dem Zufallsprinzip bei einem Controller in der lokalen Zone oder der primären Zone. Bei VDAs ab Version 7.7 ist die lokale die bevorzugte Zone.

Zonenpräferenz

> **Wichtig:**
>
> Zur Verwendung des Zonenpräferenz-Features müssen Sie mindestens StoreFront 3.7 und NetScaler Gateway 11.0-65.x ausführen.

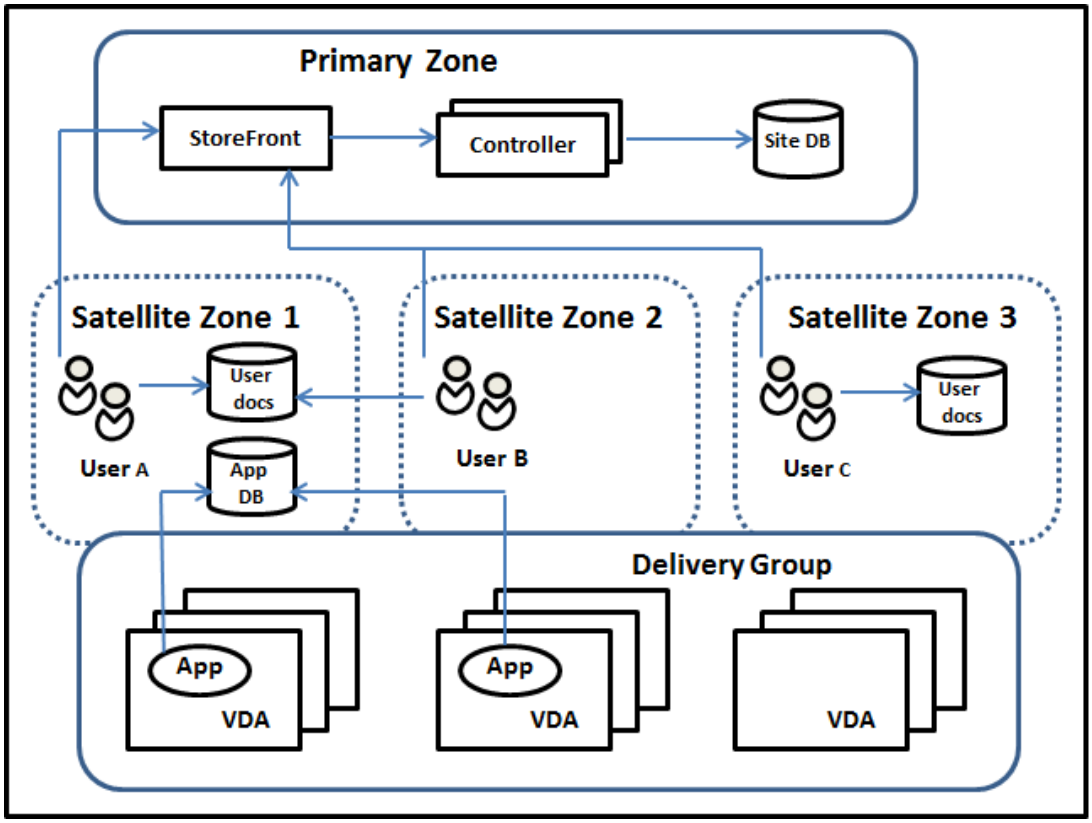
In einer Site mit mehreren Zonen bietet das Zonenpräferenz-Feature Administratoren mehr Flexibilität bei der Steuerung, welcher VDA zum Starten einer Anwendung oder eines Desktops verwendet werden soll.

Funktionsweise der Zonenpräferenz

Es gibt drei Formen der Zonenpräferenz. Die Präferenz einer Zone zur Verwendung eines spezifischen VDAs kann auf folgenden Parametern basieren:

- Speicherort der Anwendungsdaten. Dies wird als "Anwendungshome"bezeichnet.
- Speicherort der Benutzerstammdaten (Profil oder Stammfreigabe). Dies wird als "Benutzerhome"bezeichnet.
- Aktueller Standort des Benutzers (auf dem Citrix Receiver ausgeführt wird). Dies wird als "Benutzerstandort"bezeichnet.

Die folgende Abbildung zeigt ein Beispiel für eine Konfiguration mit mehreren Zonen.



In diesem Beispiel sind die VDAs über drei Satellitenzonen verteilt, gehören jedoch zur gleichen Bereitstellungsgruppe. Daher kann der Broker möglicherweise einen von mehreren VDAs für eine Startanforderung auswählen. Das Beispiel illustriert, dass die Benutzer Citrix Receiver an diversen Standorten ausführen können: Benutzer A verwendet ein Gerät mit Citrix Receiver in der Satellitenzone 1, Benutzer B verwendet ein Gerät in der Satellitenzone 2. Die Dokumente der Benutzer können an verschiedenen Speicherorten gespeichert sein: Bei Benutzer A und B ist es eine Freigabe in Satellitenzone 1, bei Benutzer C eine Freigabe in Satellitenzone C. Für eine der veröffentlichten Anwendungen wird eine Datenbank in Satellitenzone 1 verwendet.

Zum Zuordnen eines Benutzers oder einer Anwendung zu einer Zone konfigurieren Sie eine Home-

zone für den Benutzer bzw. die Anwendung. Der Delivery Controller-Broker wählt dann die Zone zum Start einer Sitzung anhand dieser Zuordnungen, sofern Ressourcen verfügbar sind. Ihre Aufgaben:

- Sie konfigurieren die Homezone für einen Benutzer, indem Sie diesen einer Zone hinzufügen.
- Sie konfigurieren die Homezone für eine Anwendung durch Bearbeiten der Anwendungseigenschaften.

Ein Benutzer bzw. eine Anwendung kann jeweils nur eine Homezone haben. (Ausnahme sind ggf. Benutzer, die zu mehreren Zonen gehören. Informationen hierzu finden Sie im Abschnitt "Weitere Überlegungen". Der Broker verwendet jedoch auch hier nur eine Homezone.)

Es können zwar Zonenpräferenzen für Benutzer und Anwendungen konfiguriert werden, der Broker wählt jedoch für einen Start nur eine bevorzugte Zone. Die Standardpriorität bei der Wahl der bevorzugten Zone ist Anwendungshome > Benutzerhome > Benutzerstandort. (Sie können diese Abfolge wie im nächsten Abschnitt beschrieben einschränken.) Wenn ein Benutzer eine Anwendung startet, passiert Folgendes:

- Wenn für die Anwendung eine Zonenzuordnung konfiguriert ist (= Anwendungshome), wird diese als bevorzugte Zone für die Anwendung verwendet.
- Wenn die Anwendung keine Zonenzuordnung hat, doch für den Benutzer wurde eine konfiguriert (= Benutzerhome), wird diese als bevorzugte Zone verwendet.
- Wenn weder Anwendung noch Benutzer eine Zonenzuordnung haben, wird als bevorzugte Zone diejenige verwendet, in der der Benutzer eine Citrix Receiver-Instanz ausführt (Benutzerstandort). Ist diese Zone nicht definiert, werden VDA und Zone nach dem Zufallsprinzip ausgewählt. Beim Lastausgleich werden alle VDAs in der bevorzugten Zone berücksichtigt. Gibt es keine bevorzugte Zone, werden beim Lastausgleich alle VDAs in der Bereitstellungsgruppe berücksichtigt.

Anpassen der Zonenpräferenz

Wenn Sie eine Homezone für einen Benutzer oder eine Anwendung konfigurieren oder entfernen, können Sie auch die Anwendung der Zonenpräferenz steuern.

- **Obligatorische Verwendung der Homezone des Benutzers:** In Bereitstellungsgruppen können Sie festlegen, dass Sitzungen in der Homezone von Benutzern (sofern eine existiert) gestartet werden und kein Failover auf andere Zonen erfolgt, wenn in der Homezone keine Ressourcen verfügbar sind. Dadurch können Sie verhindern, dass umfangreiche Profile oder große Datendateien von Zone zu Zone kopiert werden. In diesem Fall wird also eine Sitzung lieber gar nicht gestartet als in einer anderen Zone.
- **Obligatorische Verwendung der Homezone der Anwendung:** Wenn Sie eine Homezone für eine Anwendung konfigurieren, können Sie festlegen, dass die Anwendung nur in dieser Zone

gestartet wird und kein Failover auf andere Zonen erfolgt, wenn in der Homezone der Anwendung keine Ressourcen verfügbar sind.

- **Keine Anwendungshomezone und konfigurierte Benutzerhomezone ignorieren:** Wenn Sie keine Homezone für eine Anwendung konfiguriert haben, können Sie auch festlegen, dass jegliche Benutzerhomezonen beim Starten der Anwendung nicht berücksichtigt werden. Damit können Sie beispielsweise dafür sorgen, dass anhand des Benutzerstandorts die Verwendung einer bestimmten Anwendung auf einem VDA erzwungen wird, der sich in der Nähe der Maschine mit der ausgeführten Citrix Receiver-Instanz befindet, selbst wenn ein Benutzer eine andere Homezone hat.

Wie bevorzugte Zonen die Sitzungsverwendung beeinflussen

Wenn ein Benutzer eine Anwendung oder einen Desktop startet, bevorzugt der Broker die bevorzugte Zone anstelle der vorhandenen Sitzung.

Wenn ein Benutzer beim Starten einer Anwendung oder eines Desktops bereits eine Sitzung laufen hat, die sich für die gestartete Ressource eignet (die z. B. die Sitzungsfreigabe für eine von der Ressource bereits ausführte Anwendung oder Sitzung verwenden kann), die Sitzung jedoch auf einem VDA in einer anderen als der bevorzugten Zone des Benutzers bzw. der Anwendung ausgeführt wird, kann eine neue Sitzung erstellt werden. Auf diese Weise erfolgt vorzugsweise der Start in der richtigen Zone (sofern dort Kapazität frei ist), vor der Wiederverbindung mit einer Sitzung in einer für die Sitzungsanforderungen des Benutzers weniger bevorzugten Zone.

Zur Vermeidung verwaister, nicht mehr erreichbarer Sitzungen ist eine Wiederverbindung mit vorhandenen getrennten Sitzungen zulässig, selbst wenn diese in einer nicht bevorzugten Zone sind.

Beim Start gilt für Sitzungen folgende Priorität:

1. Verbindung mit einer vorhandenen Sitzung in der bevorzugten Zone
2. Wiederverbindung mit einer getrennten Sitzung in einer anderen als der bevorzugten Zone
3. Starten einer neuen Sitzung in der bevorzugten Zone
4. Wiederverbindung mit einer verbundenen Sitzung in einer anderen als der bevorzugten Zone
5. Starten einer neuen Sitzung in einer anderen als der bevorzugten Zone

Andere Überlegungen zur Zonenpräferenz

- Wenn Sie eine Homezone für eine Benutzergruppe konfigurieren (z. B. eine Sicherheitsgruppe), werden die (direkten und indirekten) Mitglieder der Gruppe dieser Zone zugeordnet. Da Benutzer jedoch mehreren Sicherheitsgruppen angehören können, können für sie über die Gruppenmitgliedschaft andere Homezonen konfiguriert sein. In solchen Fällen ist die Bestimmung der Homezone nicht eindeutig.

Wenn für einen Benutzer eine Homezone konfiguriert und nicht per Gruppenmitgliedschaft zugewiesen wurde, so erhält diese Zone den Vorzug. Durch Gruppenmitgliedschaft entstandene Zonenzuordnungen werden dann ignoriert.

Gibt es für einen Benutzer mehrere Zonenzuordnungen, die ausschließlich durch Gruppenmitgliedschaften entstanden sind, wählt der Broker die Zone nach dem Zufallsprinzip. Die einmal gewählte Zone wird so lange für nachfolgende Sitzungen verwendet, bis sich die Gruppenmitgliedschaft des Benutzers ändert.

- Für die Zonenpräferenz nach Benutzerstandort ist die Erkennung von Citrix Receiver auf dem Endpunktgerät durch das Citrix NetScaler Gateway erforderlich, über welches das Gerät eine Verbindung herstellt. Hierfür muss NetScaler für die Zuordnung von IP-Adressbereichen zu bestimmten Zonen konfiguriert sein und die ermittelte Zonenidentität muss über StoreFront an den Controller übergeben werden.

Weitere Informationen zur Zonenpräferenz finden Sie unter Zone preference internals.

Überlegungen, Anforderungen und bewährte Methoden

- Sie können Controller, Maschinenkataloge, Hostverbindungen, Benutzer und Anwendungen in einer Zone platzieren. Wenn ein Maschinenkatalog eine Hostverbindung verwendet, müssen Katalog und Verbindung in der gleichen Zone sein, sodass die Verbindung zwischen ihnen eine geringe Latenz und hohe Bandbreite hat.
- Wenn Sie Elemente in einer Satellitenzone platzieren wirkt sich dies auf die Interaktion der Site mit den Elementen und den mit diesen verbundenen Elementen aus.
  - Wenn Controllermaschinen in einer Satellitenzone platziert werden, wird angenommen, dass sie eine gute (lokale) Verbindung mit Hypervisors und VDA-Maschinen in derselben Satellitenzone haben. Controller in dieser Satellitenzone werden dann bevorzugt vor solchen in der primären Zone für das Handling der Hypervisors und VDA-Maschinen eingesetzt.
  - Wenn eine Hypervisorverbindung in einer Satellitenzone platziert wird, wird davon ausgegangen, dass alle über die Hypervisorverbindung verwalteten Hypervisors in derselben Satellitenzone sind. Controller in dieser Satellitenzone werden dann bevorzugt vor solchen in der primären Zone für die Kommunikation mit der Hypervisorverbindung eingesetzt.
  - Wenn ein Maschinenkatalog in einer Satellitenzone platziert wird, wird davon ausgegangen, dass alle VDA-Maschinen des Katalogs in derselben Satellitenzone sind. Lokale Controller werden bei der Registrierung bei der Site bevorzugt gegenüber Controllern in der primären Zone verwendet, nachdem nach der ersten Registrierung jedes VDAs die automatische Aktualisierung der Controllerliste aktiviert wurde.

  - Auch NetScaler Gateway-Instanzen können Zonen zugeordnet werden. Dies geschieht im Rahmen der Konfiguration des optimalen HDX-Routings in StoreFront statt wie bei den anderen hier beschriebenen Elementen über die Konfiguration der XenApp- oder XenDesktop-Site. Wenn ein NetScaler Gateway einer Zone zugeordnet ist, wird es für HDX-Verbindungen mit VDA-Maschinen in dieser Zone bevorzugt eingesetzt.

- Beim Erstellen des ersten Maschinenkatalogs und der ersten Bereitstellungsgruppe einer Produktionssite sind alle Elemente in der primären Zone. Sie können Satellitenzonen erst erstellen, wenn das anfängliche Setup abgeschlossen ist. Wenn Sie eine leere Site erstellen, enthält die primäre Zone zunächst nur einen Controller. Sie können Satellitenzonen vor oder nach dem Erstellen eines Maschinenkatalogs und einer Bereitstellungsgruppe erstellen.
- Beim Erstellen der ersten Satellitenzone mit einem oder mehreren Elementen verbleiben alle anderen Elemente der Site in der primären Zone.
- Die primäre Zone heißt standardmäßig "Primär". Sie können diesen Namen nach Wunsch ändern. Obwohl die primäre Zone in Studio als solche gekennzeichnet ist, empfiehlt sich die Verwendung eines Namens, anhand dessen sie sich leicht identifizieren lässt. Sie können die primäre Zone neu zuweisen, d. h. eine andere Zone als primäre Zone festlegen, die Sitedatenbank und alle hoch verfügbaren Server müssen jedoch immer in der primären Zone sein.
- Die Sitedatenbank muss immer in der primären Zone sein.
- Nach dem Erstellen von Zonen können Sie Elemente zwischen Zonen verschieben. Diese Flexibilität birgt jedoch das Risiko der Trennung von Elementen, die am besten in unmittelbarer Nähe zueinander funktionieren. Das Verschieben eines Maschinenkatalogs in eine andere Zone als die zugehörige Verbindung (Host), durch welche die Maschinen in dem Katalog erstellt werden, kann sich beispielsweise negativ auf die Leistung auswirken. Überlegen Sie daher vor dem Verschieben von Elementen zwischen Zonen, ob dies unerwünschte Auswirkungen haben könnte. Behalten Sie einen Katalog und die verwendete Hostverbindung in derselben Zone oder in Zonen, die gut verbunden sind (z. B. über ein Netzwerk mit niedriger Latenz und hoher Bandbreite).
- Zur Erzielung der optimalen Leistung installieren Sie Studio und Director nur in der primären Zone. Wenn Sie eine zusätzliche Studio-Instanz in einer Satellitenzone installieren möchten, z. B. in einer Satellitenzone mit Controllern, die für ein Failover bei Ausfall der primären Zone verwendet wird, führen Sie Studio als lokal veröffentlichte Anwendung aus. Sie können auch von einer Satellitenzone auf Director zugreifen, da es eine Webanwendung ist.
- Idealerweise sollte NetScaler Gateway in einer Satellitenzone für Benutzerverbindungen aus anderen Zonen oder externen Orten verwendet werden, es kann jedoch auch für zoneninterne Verbindungen verwendet werden.
- **Nicht vergessen:** Zur Verwendung des Zonenpräferenz-Features müssen Sie mindestens StoreFront 3.7 und NetScaler Gateway 11.0-65.x ausführen.

Erforderliche Verbindungsqualität

Die Controller in der Satellitenzone führen SQL-Interaktionen direkt mit der Sitedatenbank aus. Dies erfordert eine bestimmte Qualität der Verbindung zwischen der Satellitenzone und der primären Zone mit der Sitedatenbank. Wie hoch die Verbindungsqualität sein muss, hängt von der Zahl der VDAs und deren Benutzersitzungen in der Satellitenzone ab. Satellitenzonen mit einigen wenigen VDAs und Sitzungen kommen mit einer geringeren Verbindungsqualität aus als solche mit vielen VDAs und Sitzungen.

Weitere Informationen finden Sie unter Latency and SQL Blocking Query Improvements.

Auswirkungen der Latenz auf die Vermittlungsleistung

Sitzungen können in Zonen zwar über Verbindungen mit einer höheren Latenz ausgeführt werden (sofern es einen lokalen Broker gibt), die zusätzliche Latenz wirkt sich jedoch unweigerlich auf die Benutzererfahrung aus. Bei den meisten Arbeiten, die Benutzer in solchen Sitzungen ausführen, machen sich durch Roundtrips zwischen den Controllern in der Satellitenzone und der Sitedatenbank verursachte Verzögerungen bemerkbar.

Beim Starten von Anwendungen treten zusätzliche Verzögerungen auf, während die Sitzungsvermittlung geeignete VDAs zum Senden von Sitzungsstartanfragen sucht.

Erstellen und Verwalten von Zonen

Ein Volladministrator kann alle Aufgaben der Zonenerstellung und -verwaltung ausführen. Sie können jedoch auch eine benutzerdefinierte Rolle zum Erstellen, Bearbeiten oder Löschen einer Zone erstellen. Das Verschieben von Elementen zwischen Zonen erfordert für die Zone selbst lediglich eine Leseberechtigung. Sie benötigen jedoch die Berechtigung zum Bearbeiten der Elemente, die Sie verschieben möchten. Zum Verschieben eines Maschinenkatalogs von einer Zone in eine andere brauchen Sie beispielsweise die Berechtigung zum Bearbeiten des Maschinenkatalogs. Weitere Informationen finden Sie im Artikel Delegierte Administration.

Mit Provisioning Services: Die mit diesem Release bereitgestellte Provisioning Services-Konsole erkennt keine Zonen. Citrix empfiehlt daher, Studio zum Erstellen von Maschinenkatalogen zu verwenden, die Sie in Satellitenzonen platzieren möchten. Verwenden Sie den Assistenten in Studio zum Erstellen des Katalogs und geben Sie die richtige Satellitenzone an. Verwenden Sie dann die Provisioning Services Console zum Bereitstellen von Maschinen in diesem Katalog. Wenn Sie den Katalog mit dem Provisioning Services-Assistenten erstellen, wird er in die primäre Zone platziert und muss anschließend mit Studio in die Satellitenzone verschoben werden.

Erstellen von Zonen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen** aus.
2. Wählen Sie im Aktionsbereich **Zone erstellen**.
3. Geben Sie einen Namen für die Zone und optional eine Beschreibung ein. Der Name muss innerhalb der Site eindeutig sein.
4. Wählen Sie die Elemente, die Sie in der neuen Zone platzieren möchten. Sie können die Liste der verfügbaren Elemente filtern oder durchsuchen. Sie können auch eine leere Zone erstellen. Wählen Sie hierfür einfach keine Elemente aus.
5. Klicken Sie auf **Speichern**.

Alternativ können Sie ein oder mehrere Elemente in Studio auswählen und dann im Aktionsbereich die Option **Zone erstellen** auswählen.

Ändern des Namen oder der Beschreibung einer Zone

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen** aus.
2. Wählen Sie im mittleren Bereich eine Zone und dann im Aktionsbereich **Zone bearbeiten**.
3. Ändern Sie den Zonennamen und/oder die Beschreibung. Wenn Sie den Namen der primären Zone ändern, stellen Sie sicher, dass sie weiterhin eindeutig als primäre Zone identifiziert werden kann.
4. Klicken Sie auf **OK** oder **Übernehmen**.

Verschieben von Elementen zwischen Zonen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen** aus.
2. Wählen Sie im mittleren Bereich eine Zone und dann ein oder mehrere Elemente.
3. Ziehen Sie das Element in die Zielzone oder wählen Sie im Aktionsbereich **Elemente verschieben** und geben Sie dann die gewünschte Zielzone an.

Durch eine Meldung mit einer Liste der ausgewählten Elemente werden Sie aufgefordert, das Verschieben zu bestätigen.

Nicht vergessen: Wenn ein Maschinenkatalog eine Hostverbindung zu einem Hypervisor oder Clouddienst verwendet, müssen Katalog und Verbindung in der gleichen Zone sein. Andernfalls kann die Leistung leiden. Wenn Sie eines dieser Elemente verschieben, verschieben Sie auch das andere.

Löschen von Zonen

Eine Zone muss leer sein, damit sie gelöscht werden kann. Die primäre Zone kann nicht gelöscht werden.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen** aus.
2. Wählen Sie eine Zone im mittleren Bereich.
3. Wählen Sie im Aktionsbereich **Zone löschen**. Wenn die Zone nicht leer ist, werden Sie aufgefordert, die Zone auszuwählen, in die die enthaltenen Elemente verschoben werden sollen.
4. Bestätigen Sie die Löschung.

Hinzufügen einer Homezone für einen Benutzer

Das Konfigurieren einer Homezone für einen Benutzer wird als *Hinzufügen eines Benutzers zu einer Zone bezeichnet*.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen** und dann im mittleren Bereich eine Zone.
2. Wählen Sie im Aktionsbereich **Benutzer zur Zone hinzufügen**.
3. Klicken Sie im Dialogfeld **Benutzer zur Zone hinzufügen** auf **Hinzufügen**, und wählen Sie dann die Benutzer und Gruppen aus, die der Zone hinzugefügt werden sollen. Wenn darunter Benutzer sind, die bereits eine Homezone haben, werden zwei Optionen angezeigt: Mit **Ja** werden nur die Benutzer hinzugefügt, die noch keine Homezone haben, bei Auswahl von **Nein** wird wieder das Dialogfeld zur Auswahl der Benutzer angezeigt.
4. Klicken Sie auf **OK**.

Für Benutzer mit einer Homezone können Sie festlegen, dass Sitzungen nur in der Homezone starten dürfen:

1. Erstellen oder bearbeiten Sie eine Bereitstellungsgruppe.
2. Aktivieren Sie auf der Seite **Benutzer** das Kontrollkästchen **Sitzungen müssen in der Homezone eines Benutzers starten, wenn eine konfiguriert wurde**.

Alle von Benutzern in der Bereitstellungsgruppe gestarteten Sitzungen müssen auf Maschinen in der Homezone des jeweiligen Benutzers gestartet werden. Wenn für einen Benutzer in der Bereitstellungsgruppe keine Homezone konfiguriert ist, hat diese Einstellung keine Auswirkung.

Entfernen einer Homezone für einen Benutzer

Dieses Verfahren wird auch als Entfernen eines Benutzers aus einer Zone bezeichnet.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Zonen** und dann im mittleren Bereich eine Zone.
2. Wählen Sie im Aktionsbereich **Benutzer aus Zone entfernen**.
3. Klicken Sie im Dialogfeld **Benutzer zur Zone hinzufügen** auf **Entfernen**, und wählen Sie dann die Benutzer und Gruppen aus, die aus der Zone entfernt werden sollen. Mit dieser Aktion wer-

den die Benutzer nur aus der Zone entfernt, sie verbleiben in den Bereitstellungsgruppen und Anwendungsgruppen, zu denen sie gehören.

4. Bestätigen Sie das Entfernen, wenn Sie dazu aufgefordert werden.

Verwalten von Homezonen für Anwendungen

Das Konfigurieren einer Homezone für eine Anwendung wird als Hinzufügen einer Anwendung zu einer Zone bezeichnet. Standardmäßig haben Anwendungen in Umgebungen mit mehreren Zonen keine Homezone.

Die Homezone wird in den Anwendungseigenschaften festgelegt. Sie können die Eigenschaften von Anwendungen konfigurieren, wenn Sie die Anwendung einer Gruppe hinzufügen, oder später durch Bearbeitung der Eigenschaften in Studio.

- Wählen Sie beim Erstellen einer Bereitstellungsgruppe, Erstellen einer Anwendungsgruppe oder Hinzufügen von Anwendungen zu vorhandenen Gruppen auf der Seite **Anwendungen** des Assistenten **Eigenschaften**.
- Zum Ändern der Eigenschaften einer Anwendung nach dem Hinzufügen wählen Sie im Studio-Navigationsbereich **Anwendungen**. Wählen Sie die Anwendung und dann im Aktionsbereich **Anwendungseigenschaften bearbeiten**.

Auf der Seite **Zonen** in den Eigenschaften/Einstellungen der Anwendung:

- Wenn Sie eine Homezone für die Anwendung konfigurieren möchten:
  - Aktivieren Sie das Optionsfeld **Durch ausgewählte Zone bestimmen, wo die Anwendung gestartet wird** und wählen Sie dann die Zone aus der Dropdownliste.
  - Wenn die Anwendung ausschließlich in der ausgewählten Zone gestartet werden soll, aktivieren Sie das Kontrollkästchen unter der Zonenauswahl.
- Wenn Sie keine Homezone für die Anwendung konfigurieren möchten:
  - Aktivieren Sie das Optionsfeld **Keine Homezone für diese Anwendung konfigurieren**.
  - Wenn der Broker beim Start dieser Anwendung keine für Benutzer konfigurierten Homezonen berücksichtigen soll, aktivieren Sie das Kontrollkästchen unterhalb des Optionsfelds. In diesem Fall werden weder für die Anwendung noch für Benutzer konfigurierte Homezonen bei der Wahl des Orts, an dem die Anwendung gestartet wird, berücksichtigt.

Andere Aktionen, die eine Angabe von Zonen erfordern

In Sites mit mindestens einer Satellitenzone können Sie beim Hinzufügen einer Hostverbindung und beim Erstellen eines Maschinenkatalogs (nach Erstellen der Site) eine Zone für dieses Element angeben.

In den meisten Fällen ist die primäre Zone die Standardeinstellung. Wenn Sie einen Maschinenkatalog mit den Maschinenerstellungsdiensten erstellen, wird die für die Hostverbindung konfigurierte Zone automatisch ausgewählt.

Enthält die Site keine Satellitenzonen, wird die primäre Zone ausgewählt und die Option zur Auswahl der Zone wird nicht angezeigt.

Verbindungen und Ressourcen

August 18, 2021

Einführung

Sie können die erste Verbindung mit Hosting-Ressourcen erstellen, wenn Sie eine Site erstellen. Später können Sie die Verbindung ändern und weitere Verbindungen erstellen. Beim Konfigurieren einer Verbindung wählen Sie den Typ der Verbindung aus der Liste unterstützter Hypervisors und Clouddienste aus. Der von Ihnen ausgewählte Speicher und das Netzwerk sind die Ressourcen der Verbindung.

Lesezugriffadministratoren können die Verbindung und Ressourcendetails anzeigen. Sie müssen Volladministrator sein, um Verwaltungsaufgaben an Verbindungen und Ressourcen durchzuführen. Weitere Informationen finden Sie im Artikel zur delegierten Administration.

Informationen zu Verbindungstypen

Mit den unterstützten Virtualisierungsplattformen können Sie Maschinen in der XenApp- oder XenDesktop-Umgebung hosten und verwalten. In dem Artikel über die Systemanforderungen werden die unterstützten Typen aufgeführt. Sie können mit den unterstützten Cloudbereitstellungslösungen Produktkomponenten hosten und virtuelle Maschinen bereitstellen. Mit diesen Lösungen werden Computing-Ressourcen gepoolt, um öffentliche oder private Infrastructure-as-a-Service (IaaS)-Clouds sowie Hybrid-IaaS-Clouds zu erstellen.

Weitere Informationen finden Sie in den folgenden Informationsquellen:

Microsoft Hyper-V

- Artikel über Microsoft System Center Virtual Machine Manager-Virtualisierungsumgebungen
- Microsoft-Dokumentation

Microsoft Azure

- Microsoft Azure-Virtualisierungsumgebungen
- Microsoft-Dokumentation

Microsoft Azure Resource Manager

- Artikel über Microsoft Azure-Ressourcen-Manager
- Microsoft-Dokumentation

Amazon Web Services (AWS)

- Citrix und AWS.
- AWS-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und den geheimen Schlüssel angeben. Sie können die Schlüsseldatei mit diesen Werten aus AWS exportieren und anschließend importieren. Sie müssen auch die Werte für Region, Verfügbarkeitszone, VPC-Namen, Subnetzadressen, Domänenname, Namen der Sicherheitsgruppen und Anmeldeinformationen angeben.
- Die für das AWS-Rootkonto von der AWS-Konsole abgerufene Anmeldeinformationsdatei hat nicht das gleiche Format wie die Anmeldeinformationsdateien, die für Standard-AWS-Benutzer heruntergeladen werden. Die Datei kann darum von Studio nicht zum Ausfüllen der Felder API-Schlüssel und "Geheimer Schlüssel"verwendet werden. Verwenden Sie AWS IAM-Anmeldeinformationsdateien.
- Dedizierte Hosts und der PowerShell-Parameter `tenancytype` zum Angeben eines dedizierten Hosts für AWS-Verbindungen werden in dieser Version von XenApp und XenDesktop nicht unterstützt. Dedizierte Hosts werden ab Release 1811 unterstützt. Weitere Informationen finden Sie unter So erstellen Sie Maschinen in MCS über AWS Cloud.

CloudPlatform

- CloudPlatform-Dokumentation
- Beim Erstellen einer Verbindung in Studio müssen Sie den API-Schlüssel und den geheimen Schlüssel angeben. Sie können die Schlüsseldatei mit diesen Werten aus CloudPlatform exportieren und anschließend in Studio importieren.

Citrix XenServer

- Citrix XenServer-Dokumentation
- Beim Erstellen einer Verbindung müssen Sie die Anmeldeinformationen eines VM-Hauptadministrators oder eines höherrangigen Benutzers eingeben.
- Citrix empfiehlt, HTTPS zum Sicheren der Kommunikation mit XenServer zu verwenden. Um HTTPS zu verwenden, müssen Sie das standardmäßig mit XenServer installierte SSL-Zertifikat ersetzen (siehe CTX128656).
- Sie können hohe Verfügbarkeit konfigurieren, wenn dies auf XenServer aktiviert ist. Citrix empfiehlt, dass Sie alle Server im Pool (über "Server mit hoher Verfügbarkeit bearbeiten"

) auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.
- Sie können einen GPU-Typ und eine GPU-Gruppe oder Passthrough auswählen, wenn der XenServer vGPU unterstützt. Es wird angezeigt, ob die Auswahl dedizierte GPU-Ressourcen umfasst.

Nutanix Acropolis

- Artikel über Nutanix-Virtualisierungsumgebungen
- Nutanix-Dokumentation.

VMware

- Artikel über VMware-Virtualisierungsumgebungen
- VMware-Produktdokumentation

Hostspeicher

Beim Provisioning von Maschinen werden die Daten nach Typ klassifiziert:

- Betriebssystemdaten (OS-Daten), einschließlich Masterimages.
- Temporäre Daten, einschließlich aller nicht persistenten Daten, die auf mit MSC bereitgestellten Maschinen geschrieben werden, Windows-Seitendateien, Benutzerprofildaten und alle Daten, die mit ShareFile synchronisiert werden. Diese Daten werden beim Neustart einer Maschine verworfen.
- Persönliche Daten, die auf persönlichen vDisks gespeichert werden.

Durch die Bereitstellung von separatem Speicher für die einzelnen Datentypen können Sie auf Speichergeräten die Last reduzieren und die IOPS-Leistung verbessern und so den größten Nutzen aus den verfügbaren Ressourcen des Hosts ziehen. Außerdem kann so der entsprechende Speicher für die verschiedenen Datentypen verwendet werden, denn Persistenz und Resilienz ist für einige Daten wichtiger als für andere.

Speicher kann freigegeben sein (zentraler Speicher, der separat von den Hosts ist, aber von allen Hosts verwendet wird) oder lokal auf einem Hypervisor bereitgestellt werden. Ein zentraler freigegebener Speicher kann beispielsweise aus einem oder mehreren geclusterten Windows Server 2012-Speichervolumes (mit oder ohne angeschlossenem Speicher) oder dem Gerät eines Speicheranbieters bestehen. Der zentrale Speicher bietet möglicherweise auch eigene Optimierungen, wie Steuerungspfade für Hypervisorspeicher und direkter Zugriff über Partner-Plug-Ins.

Durch das lokale Speichern temporärer Daten muss für den Zugriff auf freigegebenen Speicher nicht das Netzwerk passiert werden. Dadurch wird die Last (IOPS) auf dem freigegebenen Speichergerät reduziert. Freigegebener Speicher kann kostspieliger sein, daher können durch das lokale Speichern

von Daten die Ausgaben gesenkt werden. Diese Vorteile müssen gegen die Verfügbarkeit von genügend Speicher auf den Hypervisorservern abgewogen werden.

Beim Erstellen einer Verbindung müssen Sie eine von zwei Speicherverwaltungsmethoden auswählen: für Hypervisors freigegebener Speicher oder lokaler Speicher auf dem Hypervisor.

> **Hinweis:**
>
> Wenn Sie auf XenServer-Hosts lokalen Speicher für die temporäre Datenspeicherung verwenden, stellen Sie sicher, dass jeder Speicherort im Pool einen eindeutigen Namen hat. (Sie ändern einen Namen in XenCenter, indem Sie mit der rechten Maustaste auf den Speicher klicken und die Nameneigenschaft bearbeiten.)

Für Hypervisors freigegebener Speicher

Bei für Hypervisors freigegebenem Speicher werden Daten, die länger erhalten bleiben sollen, zentral gespeichert und bieten zentrale Backup- und Verwaltungsmöglichkeiten. Dieser Speicher umfasst die Betriebssystemdatenträger und die persönlichen vDisk-Datenträger.

Bei dieser Methode können Sie wählen, ob Sie lokalen Speicher (auf Servern im gleichen Hypervisorpool) für temporäre Daten verwenden, die nicht so viel Persistenz oder Resilienz erfordern wie die Daten im freigegebenen Speicher. Dies ist der *temporäre Datencache*. Die lokale Festplatte reduziert den Datenverkehr zum Hauptbetriebssystemspeicher. Dieser Datenträger wird nach dem Neustart einer Maschine gelöscht. Auf den Datenträger wird über einen Write-through-Speichercache zugegriffen. Wenn Sie lokalen Speicher für temporäre Daten verwenden, ist der bereitgestellte VDA an einen bestimmten Hypervisorhost gebunden. Wenn der Host ausfällt, kann die VM nicht gestartet werden.

Ausnahme: Wenn Sie geclusterte Speichervolumes (CSV) verwenden, gestattet Microsoft System Center Virtual Machine Manager nicht, dass temporäre Datenträgercaches auf dem lokalen Speicher erstellt werden.

Wenn Sie beim Erstellen einer Verbindung die Option für die lokale Speicherung der temporären Daten aktivieren, können Sie benutzerdefinierte Werte für die Größe des Cachedatenträgers und des Speichers jeder VM aktivieren und konfigurieren, wenn Sie einen Maschinenkatalog erstellen, der diese Verbindung verwendet. Die Standardwerte sind jedoch auf den Verbindungstyp zugeschnitten und in den meisten Fällen ausreichend. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Der Hypervisor kann auch Optimierungstechnologien über lokales Lese-Caching der Datenträgerimages bieten; XenServer bietet beispielsweise IntelliCache. Dies kann auch den Netzwerkdatenverkehr zum zentralen Speicher reduzieren.

Lokaler Speicher auf dem Hypervisor

Bei der Methode mit lokalem Speicher auf dem Hypervisor werden Daten lokal auf dem Hypervisor gespeichert. Mit dieser Methode werden Masterimages und andere Betriebssystemdaten an alle Hypervisors in der Site übermittelt, sowohl bei der anfänglichen Maschinenerstellung als auch bei zukünftigen Imageupdates. Dies führt zu intensivem Datenverkehr auf dem Verwaltungsnetzwerk. Imageübertragungen sind zeitaufwändig und die Images werden jedem Host zu einem anderen Zeitpunkt zur Verfügung gestellt.

Bei Auswahl dieser Methode können Sie wählen, ob Sie freigegebenen Speicher für persönliche vDisks verwenden, um Resilienz und Unterstützung für Backup- und Notfallwiederherstellungssysteme bieten.

Erstellen einer Verbindung und von Ressourcen

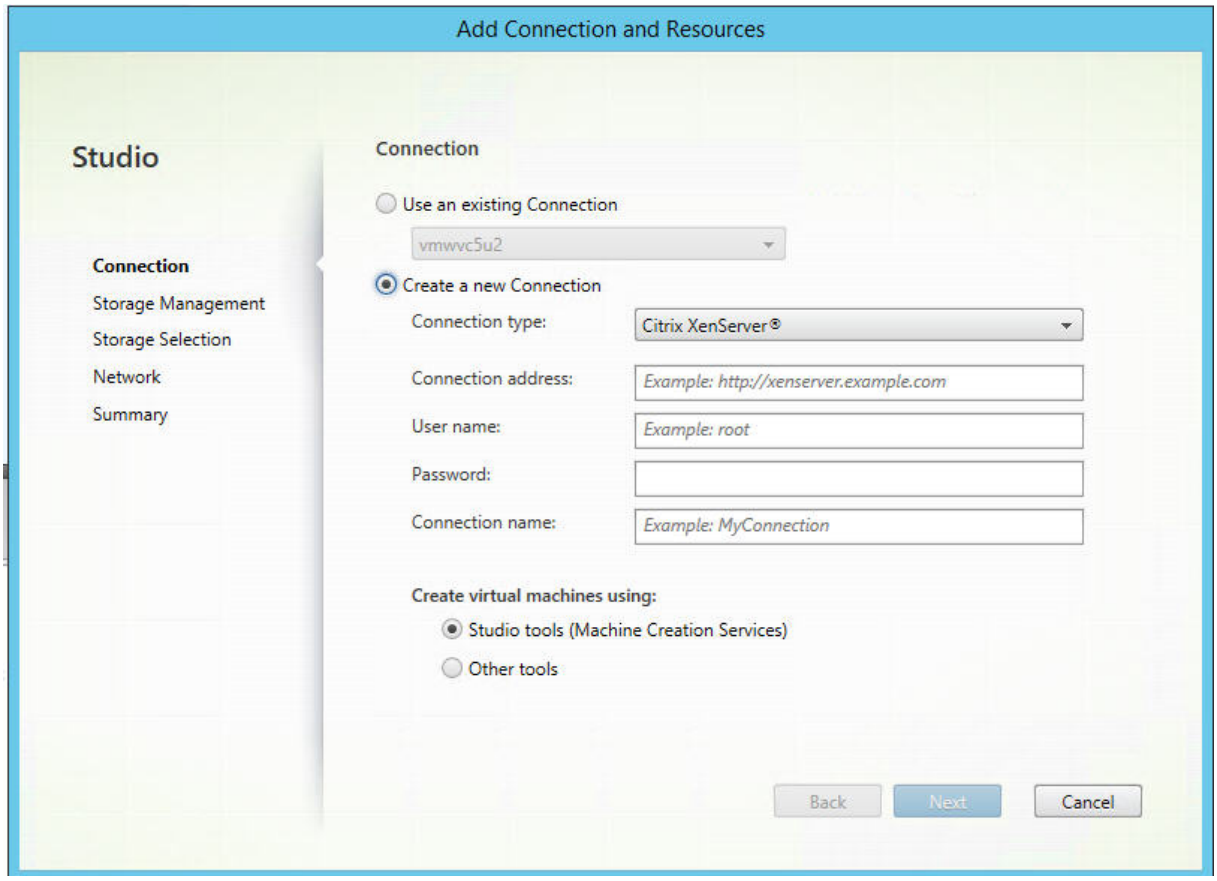
Sie können die erste Verbindung beim Erstellen der Site erstellen. Der Assistent für die Siteerstellung enthält die nachfolgend beschriebenen Seiten für Verbindungen: Verbindung, Speicherverwaltung, Speicherauswahl und Netzwerk.

Wenn Sie eine Verbindung erstellen, nachdem Sie die Site erstellt haben, beginnen Sie mit Schritt 1 (siehe unten).

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

- Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
- Wählen Sie im Bereich “Aktionen”die Option **Verbindung und Ressourcen hinzufügen**.
- Der Assistent führt Sie durch die folgenden Seiten (der Seiteninhalt hängt vom ausgewählten Verbindungstyp ab). Wenn Sie mit einer Seite fertig sind, klicken Sie jeweils auf **Weiter**, bis Sie zur letzten Seite **Zusammenfassung** gelangen.

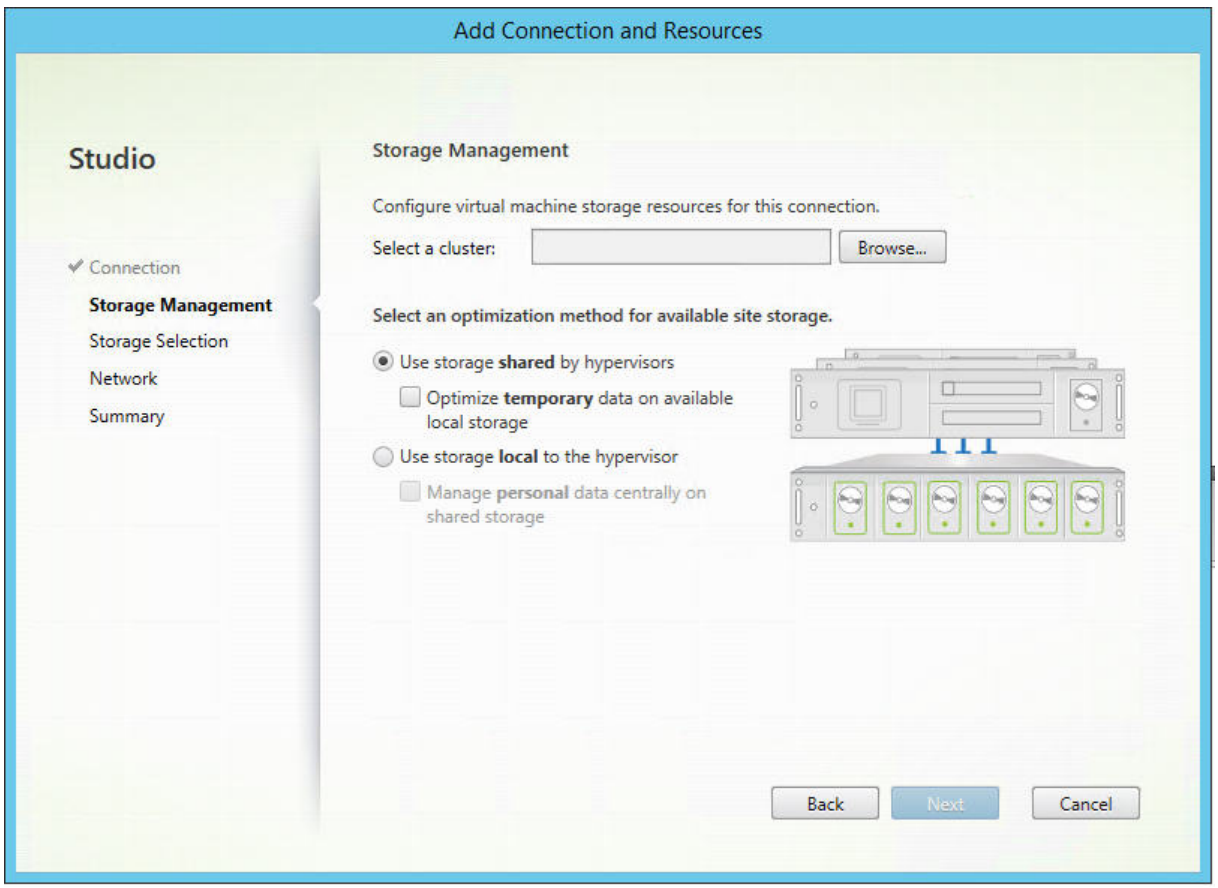
Verbindung



Auf der Seite **Verbindung**:

- Um eine neue Verbindung zu erstellen, wählen Sie **Neue Verbindung erstellen**. Um eine Verbindung zu erstellen, die auf derselben Hostkonfiguration wie eine bestehende Verbindung basiert, klicken Sie **Vorhandene Verbindung verwenden** und wählen dann die entsprechende Verbindung.
- Wählen Sie im Feld **Verbindungstyp** den Hypervisor oder Clouddienst aus, den Sie verwenden.
- Die Felder für Verbindungsadresse und Anmeldeinformationen sind je nach ausgewähltem Verbindungstyp unterschiedlich. Geben Sie die angeforderten Informationen ein.
- Geben Sie einen Verbindungsnamen ein. Dieser Name wird in Studio angezeigt.
- Wählen Sie das Tool, mit dem Sie virtuelle Maschinen erstellen: Studio-Tools (z. B. Maschinenerstellungsdienste (MCS) oder Provisioning Services) oder andere Tools.

Speicherverwaltung



Informationen zur Speicherverwaltungstypen und -methoden finden Sie unter Hostspeicher.

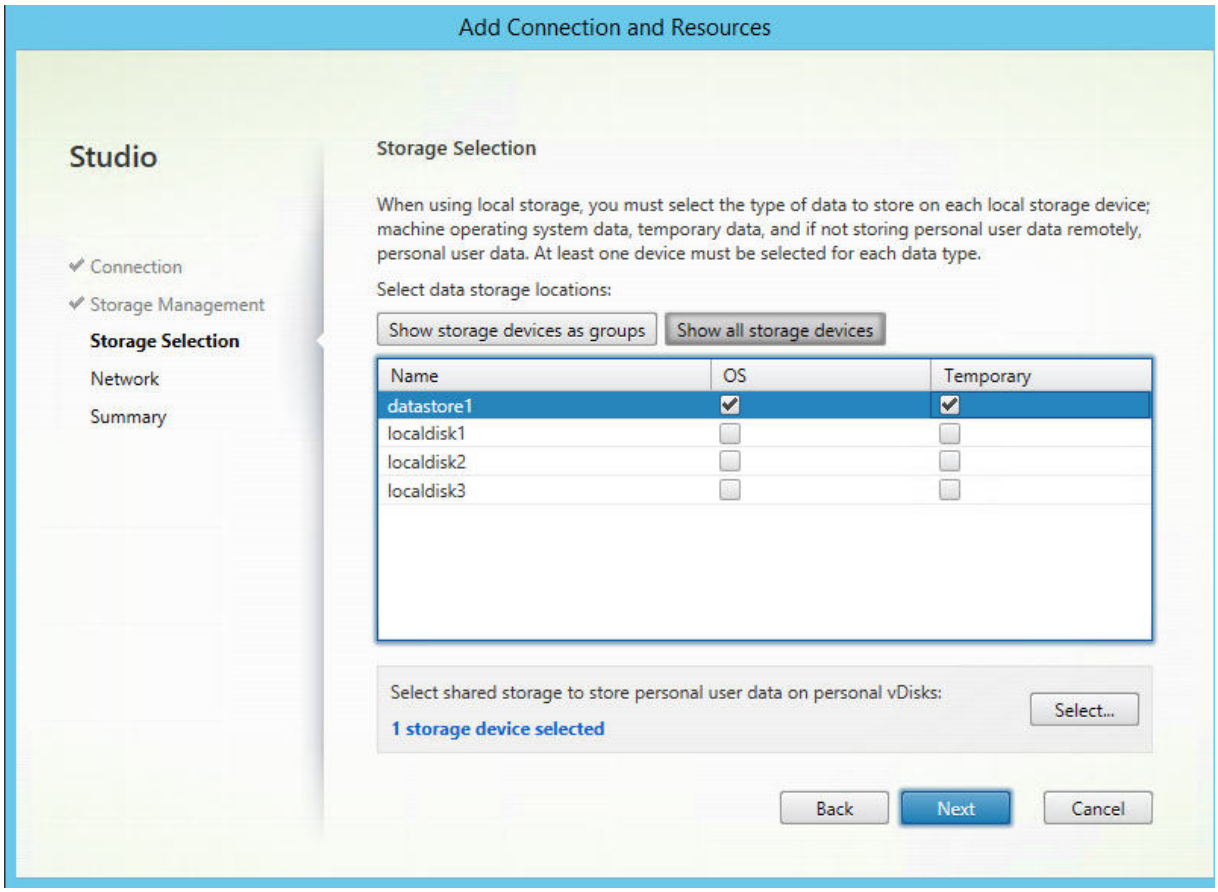
Wenn Sie eine Verbindung zu einem Hyper-V- oder VMware-Host konfigurieren, navigieren Sie zu einem Clusternamen und wählen Sie ihn aus. Andere Verbindungstypen erfordern keine Clusternamen.

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

- Wenn Sie für Hypervisors freigegebenen Speicher wählen, geben Sie an, ob temporäre Daten im verfügbaren lokalen Speicher gespeichert werden sollen. (Sie können nicht standardmäßige temporäre Speichergrößen in den Maschinenkatalogen angeben, die diese Verbindung verwenden.) **Ausnahme:** Wenn Sie geclusterte Speichervolumes (CSV) verwenden, erlaubt Microsoft System Center Virtual Machine Manager nicht, dass temporäre Datenträgercaches auf dem lokalen Speicher erstellt werden, daher schlägt das Konfigurieren des Speicherverwaltungssetups in Studio fehl.
- Wenn Sie lokalen Speicher auf dem Hypervisor wählen, geben Sie an, ob Sie persönliche Daten (persönliche vDisks) im freigegebenen Speicher verwalten möchten.

Wenn Sie freigegebenen Speicher auf einem XenServer-Hypervisor verwenden, geben Sie an, ob Sie IntelliCache zum Reduzieren der Last auf dem freigegebenen Speichergerät verwenden. Weitere Informationen finden Sie unter Verwenden von IntelliCache für XenServer-Verbindungen.

Speicherauswahl



Weitere Informationen zur Speicherauswahl finden Sie unter Hostspeicher.

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

Der untere Teil der Seite **Speicherauswahl** enthält zusätzliche Konfigurationsoptionen, wenn Sie auf der Seite vorher eine der folgenden Optionen ausgewählt haben.

- Wenn Sie von Hypervisors gemeinsam genutzten Speicher wählen und das Kontrollkästchen **Temporäre Daten in verfügbarem lokalem Speicher optimieren** aktivieren, können Sie wählen, welche lokalen Speichergeräte (im selben Hypervisorpool) für temporäre Daten verwendet werden sollen.

- Wenn Sie Speicher wählen, der lokal auf dem Hypervisor ist, und das Kontrollkästchen **Persönliche Daten zentral im freigegebenen Speicher verwalten** aktiviert haben, können Sie wählen, welche freigegebenen Geräte für persönliche Daten (PvD) verwendet werden sollen.

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

1. Klicken Sie auf **Auswählen**, um die zu verwendenden Speichergeräte zu ändern.
2. Aktivieren oder deaktivieren Sie im Dialogfeld **Speicher auswählen** die Kontrollkästchen für Speichergeräte, und klicken Sie dann auf **OK**.

Network

Geben Sie einen Namen für die Ressourcen ein. Dieser Name wird in Studio angezeigt, um das Speichergerät und die der Verbindung zugeordnete Netzwerkkombination zu identifizieren.

Wählen Sie mindestens ein Netzwerk für die VMs aus.

Zusammenfassung

Überprüfen Sie Ihre Auswahl. Wenn Sie Änderungen vornehmen möchten, kehren Sie zu den vorherigen Seiten des Assistenten zurück. Wenn Sie Ihre Bewertung abgeschlossen haben, klicken Sie auf **Fertig stellen**.

Nicht vergessen: Wenn Sie temporäre Daten lokal speichern, können Sie benutzerdefinierte Werte für den temporären Datenspeicher konfigurieren, wenn Sie den Maschinenkatalog mit den Maschinen für diese Verbindung erstellen. Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen.

Bearbeiten von Verbindungseinstellungen

Verwenden Sie diese Vorgehensweise nicht, um eine Verbindung umzubenennen oder eine neue Verbindung zu erstellen. Dafür sind andere Schritte erforderlich. Ändern Sie die Adresse nur, wenn die aktuelle Hostmaschine eine neue Adresse hat. Durch die Eingabe der Adresse einer anderen Maschine werden die Maschinenkataloge der Verbindung unbrauchbar.

Sie können die GPU-Einstellungen für eine Verbindung nicht ändern, da Maschinenkataloge, die auf diese Ressource zugreifen, ein entsprechendes GPU-spezifisches Masterimage verwenden müssen. Erstellen Sie eine neue Verbindung.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.

2. Wählen Sie die Verbindung und dann im Bereich "Aktionen"die Option **Verbindung bearbeiten**.
3. Folgen Sie den Anweisungen unten bei der Auswahl der Einstellungen zum Bearbeiten einer Verbindung.
4. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, damit die Änderungen angewendet werden und das Fenster geöffnet bleibt, oder klicken Sie auf **OK**, damit die Änderungen angewendet werden und das Fenster geschlossen wird.

Seite **Verbindungseigenschaften**:

- Zum Ändern der Verbindungsadresse und Anmeldeinformationen wählen Sie **Einstellungen bearbeiten** und geben die neuen Informationen ein.
- Zum Angeben der Server mit hoher Verfügbarkeit für eine XenServer-Verbindung wählen Sie **Server mit hoher Verfügbarkeit bearbeiten**. Citrix empfiehlt, dass Sie alle Server im Pool auswählen, um die Kommunikation mit XenServer zu ermöglichen, wenn der Poolmaster ausfällt.

Seite **Erweitert**:

Für eine Wake-On-LAN-Verbindung unter Microsoft System Center Configuration Manager, die mit Remote-PC-Zugriff verwendet wird, geben Sie ConfigMgr Wake Proxy, Magic Packets und Paketübertragungsinformationen an.

Über die Einstellungen für den Einschränkungsschwellenwert können Sie eine maximale Anzahl von Energieaktionen für eine Verbindung festlegen. Diese Einstellungen können nützlich sein, wenn durch die Energieverwaltungseinstellungen der gleichzeitige Start zu vieler oder zu weniger Maschinen zugelassen wird. Für jeden Verbindungstyp gibt es bestimmte Standardwerte, die in den meisten Fällen geeignet sind und in der Regel nicht geändert werden sollten.

Über **Gleichzeitige Aktionen (alle Typen)** und **Gleichzeitige Updates für Personal vDisk-Inventar** wird Folgendes festgelegt: die maximale absolute Zahl Aktionen/Updates, die gleichzeitig an dieser Verbindung auftreten dürfen, und den maximalen Prozentsatz aller Maschinen, die diese Verbindung verwenden. Sie müssen beide Werte angeben, angewendet wird der geringere der Werte.

Beispiel: Wird in einer Bereitstellung mit 34 Maschinen die Einstellung **Gleichzeitige Aktionen (alle Typen)** auf einen absoluten Wert von 10 und einen Prozentsatz von 10 festgelegt, wird als tatsächliches Limit 3 angewendet (d. h. 10 Prozent von 34 auf die nächste Ganzzahl gerundet –ein kleinerer Wert als die absolute Zahl von 10 Maschinen).

Die **Höchstanzahl neue Aktionen pro Minute** ist eine absolute Zahl. Es gibt keinen Prozentwert.

Hinweis: Geben Sie die Informationen im Feld **Verbindungsoptionen** nur unter der Anleitung eines Supportmitarbeiters von Citrix ein.

Aktivieren und Deaktivieren des Wartungsmodus für eine Verbindung

Wenn Sie den Wartungsmodus für eine Verbindung aktivieren, können keine neuen Energieaktionen auf in dieser Verbindung gespeicherten Maschinen stattfinden. Benutzer können keine Verbindung mit einer Maschine herstellen, wenn sie im Wartungsmodus ist. Wenn Benutzer bereits verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung aus. Zum Aktivieren des Wartungsmodus wählen Sie im Bereich "Aktionen"die Option **Wartungsmodus einschalten**. Zum Deaktivieren des Wartungsmodus wählen Sie **Wartungsmodus ausschalten**.

Sie können den Wartungsmodus auch für einzelne Maschinen ein- und ausschalten. Darüber hinaus können Sie den Wartungsmodus auch für Maschinen in Maschinenkatalogen und Bereitstellungsgruppen aktivieren oder deaktivieren.

Löschen einer Verbindung

> **Achtung:**
>
> Das Löschen einer Verbindung kann zur Folge haben, dass eine große Zahl von Maschinen gelöscht wird, Datenverlust eingeschlossen. Stellen Sie sicher, dass die Benutzerdaten auf den betroffenen Maschinen gesichert wurden oder nicht mehr benötigt werden.

Vor dem Löschen einer Verbindung müssen Sie Folgendes sicherstellen:

- Alle Benutzer sind von den in dieser Verbindung gespeicherten Maschinen abgemeldet.
- Es werden keine getrennten Benutzersitzungen ausgeführt.
- Der Wartungsmodus wird für gepoolte und dedizierte Maschinen aktiviert.
- Alle Maschinen in den von der Verbindung verwendeten Maschinenkatalogen sind ausgeschaltet.

Ein Maschinenkatalog kann nicht mehr verwendet werden, wenn Sie eine Verbindung löschen, auf die dieser Katalog verweist. Verweist ein Katalog auf diese Verbindung, haben Sie die Option zum Löschen des Katalogs. Stellen Sie vor dem Löschen eines Katalogs sicher, dass er nicht von anderen Verbindungen verwendet wird.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Bereich "Aktionen"die Option **Verbindung löschen**.
3. Wenn für die Verbindung Maschinen gespeichert sind, werden Sie gefragt, ob die Maschinen gelöscht werden sollen. Wenn dies der Fall ist, geben Sie an, was mit dem zugewiesenen Active Directory-Computerkonten passieren soll.

Umbenennen oder Testen einer Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Bereich "Aktionen"die Option **Verbindung umbenennen** oder **Verbindung testen**.

Anzeigen von Maschinendetails für eine Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Verbindung und dann im Bereich "Aktionen"die Option **Maschinen anzeigen**.

Im oberen Bereich werden die Maschinen angezeigt, auf die über die Verbindung zugegriffen wird. Wählen Sie eine Maschine aus, um die Details im unteren Bereich anzuzeigen. Für geöffnete Sitzungen werden auch Sitzungsdetails angezeigt.

Sie können das Suchfeature verwenden, um Maschinen schnell aufzufinden. Wählen Sie entweder eine gespeicherte Suche aus der Liste im oberen Bereich des Bildschirms aus oder erstellen Sie eine neue Suche. Sie können nach dem Maschinennamen suchen, indem Sie den ganzen Namen oder einen Teil des Namens eingeben. Alternativ können Sie auch einen Ausdruck für eine erweiterte Suche erstellen. Klicken Sie auf die **Erweiterungsschaltfläche**, um einen Ausdruck zu erstellen, und wählen Sie dann aus den angezeigten Listen Eigenschaften und Operatoren aus.

Verwalten von Maschinen einer Verbindung

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie eine Verbindung und dann im Bereich "Aktionen"die Option **Maschinen anzeigen**.
3. Wählen Sie im Bereich Aktionen eine der folgenden Optionen. Abhängig vom Maschinenzustand und dem Verbindungshosttyp sind einige Aktionen möglicherweise nicht verfügbar.

- **Starten:** Die Maschine wird gestartet, wenn sie ausgeschaltet oder angehalten ist.
- **Anhalten:** Die Maschine wird ohne Herunterfahren angehalten die Liste der Maschinen wird aktualisiert.
- **Herunterfahren:** Das Betriebssystem wird aufgefordert, herunterzufahren.
- **Herunterfahren erzwingen:** Die Maschine wird zwingend abgeschaltet und die Liste der Maschinen wird aktualisiert.
- **Neu starten:** Das Betriebssystem wird heruntergefahren und die Maschine wird neu gestartet. Wenn das Betriebssystem diese Aufgaben nicht ausführen kann, bleibt der Desktop im aktuellen Zustand.
- **Wartungsmodus aktivieren:** Stoppt vorübergehend Verbindungen mit einer Maschine. Benutzer können keine Verbindung mit einer Maschine in diesem Zustand herstellen. Wenn Benutzer verbunden sind, wird der Wartungsmodus wirksam, sobald sich die Benutzer abmelden.

Sie können den Wartungsmodus auch für alle Maschinen aktivieren bzw. deaktivieren, auf die über eine Verbindung zugegriffen wird (siehe oben).

- **Aus Bereitstellungsgruppe entfernen:** Beim Entfernen einer Maschine aus einer Bereitstellungsgruppe wird sie nicht aus dem von der Bereitstellungsgruppe verwendeten Maschinenkatalog gelöscht. Sie können eine Maschine nur entfernen, wenn keine Benutzer mit ihr verbunden sind; aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie die Maschine entfernen.
- **Löschen:** Wenn Sie eine Maschine löschen, können Benutzer nicht mehr darauf zugreifen und die Maschine wird aus dem Maschinenkatalog gelöscht. Stellen Sie vor dem Löschen einer Maschine sicher, dass alle Benutzerdaten gesichert wurden oder nicht mehr benötigt werden. Sie können eine Maschine nur löschen, wenn keine Benutzer mit ihr verbunden sind; aktivieren Sie den Wartungsmodus, um zu verhindern, dass Benutzer eine Verbindung herstellen, während Sie die Maschine löschen.

Bei Aktionen, bei denen eine Maschine heruntergefahren wird, wird diese ausgeschaltet, wenn das Herunterfahren nicht innerhalb von 10 Minuten erfolgt. Wenn Windows versucht, während des Herunterfahrens Updates zu installieren, besteht die Gefahr, dass die Maschine ausgeschaltet wird, bevor die Updates abgeschlossen sind.

Bearbeiten des Speichers

Sie können den Status der Server anzeigen, auf denen das Betriebssystem sowie temporäre und persönliche Daten (PvD) für VMs gespeichert werden, die eine Verbindung verwenden. Sie können auch festlegen, welche Server für die Speicherung der jeweiligen Datentypen verwendet werden.

1. Wählen Sie im Studio-Navigationsbereich Konfiguration > Hosting.
2. Wählen Sie eine Verbindung und dann im Bereich Aktionen den Befehl Speicher bearbeiten.
3. Wählen Sie im linken Bereich den Datentyp: Betriebssystem, persönliche vDisk oder temporär.
4. Aktivieren oder deaktivieren Sie für den ausgewählten Datentyp das Kontrollkästchen für mindestens ein Speichergerät.
5. Klicken Sie auf OK.

Jedes Speichergerät in der Liste enthält den Namen und Speicherstatus. Gültige Speicherstatuswerte sind Folgende:

- **Wird verwendet:** Der Speicher wird zum Erstellen neuer Maschinen verwendet.
- **Abgelöst**: Der Speicher wird nur für vorhandene Maschinen verwendet. Diesem Speicher werden keine neuen Maschinen hinzugefügt.
- **Nicht verwendet:** Der Speicher wird nicht zum Erstellen von Maschinen verwendet.

Wenn Sie das Kontrollkästchen für ein Gerät deaktivieren, das den Status **Wird verwendet** hat, ändert sich der Status in **Abgelöst**. Vorhandene Maschinen verwenden das Speichergerät weiterhin (und

können Daten darauf schreiben), daher kann der Speicher voll werden, selbst wenn er nicht mehr zum Erstellen neuer Maschinen verwendet wird.

Löschen, Umbenennen oder Testen von Ressourcen

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Hosting**.
2. Wählen Sie die Ressource aus und wählen Sie dann den entsprechenden Eintrag im Bereich "Aktionen"die Option: **Ressourcen löschen**, **Ressourcen umbenennen** oder **Ressourcen testen**.

Verwenden von IntelliCache für XenServer-Verbindungen

Durch den Einsatz von IntelliCache werden gehostete VDI-Bereitstellungen kostengünstiger, da eine Kombination aus freigegebenem und lokalem Speicher verwendet werden kann. Dies verbessert die Leistung und reduziert den Datenverkehr im Netzwerk. Das Masterimage aus dem freigegebenen Speicher wird im lokalen Speicher zwischengespeichert, wodurch die Anzahl der Lesevorgänge im freigegebenen Speicher reduziert wird. Bei gemeinsam genutzten Desktops werden Schreibvorgänge auf den differenzierenden Festplatten in den lokalen Speicher auf dem Host und nicht in den gemeinsam genutzten Speicher geschrieben.

- Der freigegebene Speicher muss NFS sein, wenn Sie IntelliCache verwenden.
- Citrix empfiehlt die Verwendung eines lokalen Speichergeräts mit hoher Leistung, um eine schnellstmögliche Datenübertragung zu gewährleisten.

Um IntelliCache zu verwenden, müssen Sie es in diesem Produkt und XenServer aktivieren.

- Bei der Installation von XenServer wählen Sie **Enable thin provisioning (Optimized storage for XenDesktop)**. Citrix bietet keine Unterstützung für gemischte Serverpools, auf denen IntelliCache auf manchen Servern aktiviert ist und auf anderen nicht. Weitere Informationen finden Sie in der Dokumentation für XenServer.
- In XenApp und XenDesktop ist IntelliCache standardmäßig deaktiviert. Sie können die Einstellung nur beim Erstellen einer XenServer-Verbindung ändern, IntelliCache kann später nicht deaktiviert werden. Gehen Sie folgendermaßen vor, wenn Sie eine XenServer-Verbindung von Studio aus hinzufügen:
  - Wählen Sie als Speichertyp **Freigegeben** aus.
  - Aktivieren Sie das Kontrollkästchen **IntelliCache verwenden**.

Verbindungstimer

Sie können mit Richtlinieneinstellungen drei Verbindungstimer konfigurieren:

- Timer für längste Verbindung: Diese Einstellung legt die Höchstdauer einer ununterbrochenen Verbindung zwischen einem Benutzergerät und einem Desktop fest. Verwenden Sie die Richtlinieneinstellungen **Sitzungsleerlauftimer** und **Sitzungsleerlauf - Timerintervall**.
- Timer für längste Verbindung: Legt fest, wie lange eine ununterbrochene Verbindung zwischen einem Benutzergerät und einem virtuellen Desktop erhalten wird, wenn keine Eingabe vom Benutzer erfolgt. Verwenden Sie die Richtlinieneinstellungen **Sitzungsleerlauftimer** und **Sitzungsleerlauf - Timerintervall**.
- Timer für getrennte Verbindungen: Legt fest, wie lange ein getrennter, gesperrter virtueller Desktop gesperrt bleibt, bis die Sitzung abgemeldet wird. Verwenden Sie die Richtlinieneinstellungen **Timer für getrennte Sitzung** und **Getrennte Sitzungen - Timerintervall**.

Wenn Sie eine dieser Einstellungen aktualisieren, achten Sie darauf, dass sie in der ganzen Bereitstellung konsistent sind.

Weitere Informationen finden Sie in der Dokumentation für die Richtlinieneinstellungen.

Lokaler Hostcache

August 18, 2021

Um sicherzustellen, dass die XenApp und XenDesktop-Sitedatenbank immer verfügbar ist, empfiehlt Citrix, unter Befolgung der bewährten Methoden zur hohen Verfügbarkeit von Microsoft mit einer fehlertoleranten SQL Server-Bereitstellung zu beginnen. (Der Abschnitt "Datenbanken"des Artikels Systemanforderungen enthält eine Liste der in XenApp und XenDesktop unterstützten SQL Server-Features für hohe Verfügbarkeit.) Aufgrund von Netzwerkproblemen und Unterbrechungen können Benutzer jedoch evtl. keine Verbindung mit ihren Anwendungen oder Desktops herstellen.

Der lokale Hostcache (LHC) ermöglicht bei einem Systemausfall das fortgesetzte Verbindungsbrokering in einer XenApp- oder XenDesktop-Site. Es kommt zu einem Ausfall, wenn ein Fehler bei der Verbindung zwischen einem Delivery Controller und der Sitedatenbank auftritt. Der lokale Hostcache wird aktiviert, wenn die Sitekonfigurationsdatenbank für 90 Sekunden nicht verfügbar ist.

Der lokale Hostcache ist das umfassendste Feature für hohe Verfügbarkeit in XenApp und XenDesktop. Er ist eine leistungsfähigere Alternative zum Verbindungsleasing, das in XenApp 7.6 eingeführt wurde.

Die neue Implementierung des lokalen Hostcache hat zwar denselben Namen wie ein Feature in XenApp-Releases bis 6.x, weist jedoch einige wichtige Verbesserungen auf. Diese Implementierung ist robuster und beschädigungsresistent. Die Wartungsanforderungen wurden auf ein Minimum begrenzt (z. B. sind keine regelmäßigen dsmaint-Befehle mehr erforderlich). Der neue lokale Hostcache ist technisch völlig anders implementiert. Nachfolgend erfahren Sie, wie er funktioniert.

> **Hinweis:**
>
> Das Verbindungsleasing wird in Version 7.15 LTSR zwar unterstützt, aus dem nachfolgenden Release wird es jedoch entfernt.

Dateninhalt

Der lokale Hostcache enthält folgende Informationen (die eine Teilmenge der Informationen in der Hauptdatenbank sind):

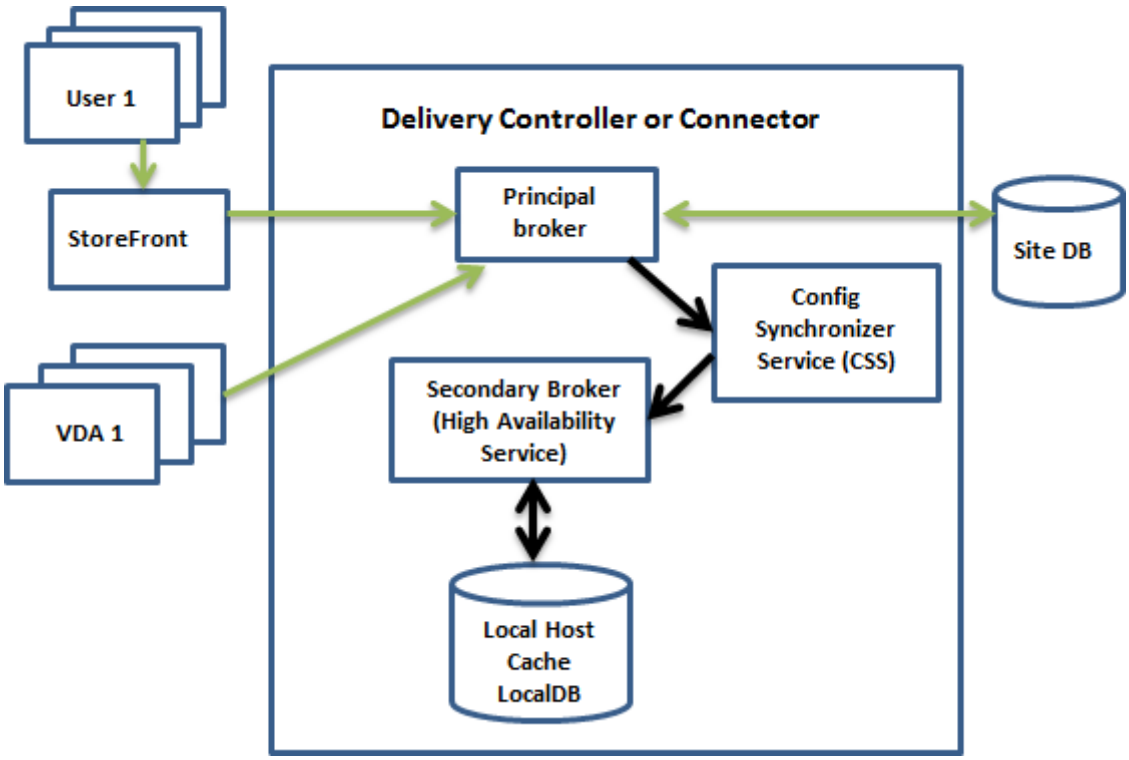
- Identität der Benutzer und Gruppen, denen Rechte für die in der Site veröffentlichte Ressourcen zugewiesen wurden.
- Identität der Benutzer, die Ressourcen der Site gerade verwenden oder kürzlich verwendet haben.
- Identität von VDA-Maschinen (einschließlich Remote-PC-Zugriffsmaschinen), die in der Site konfiguriert sind.
- Identität (Name und IP-Adresse) von Citrix Receiver-Clientmaschinen, die aktiv für die Verbindung mit veröffentlichten Ressourcen verwendet werden.

Er enthält außerdem Informationen zu aktiven Verbindungen, die eingerichtet wurden, während die Hauptdatenbank nicht verfügbar war:

- Ergebnisse jeglicher von Citrix Receiver durchgeführten Clientmaschinen-Endpunktanalyse.
- Identität von Infrastrukturmaschinen (z. B. NetScaler Gateway- und StoreFront-Server), die mit der Site zu tun haben.
- Datum und Uhrzeit und Art kürzlich erfolgter Aktivitäten von Benutzern.

Funktionsweise

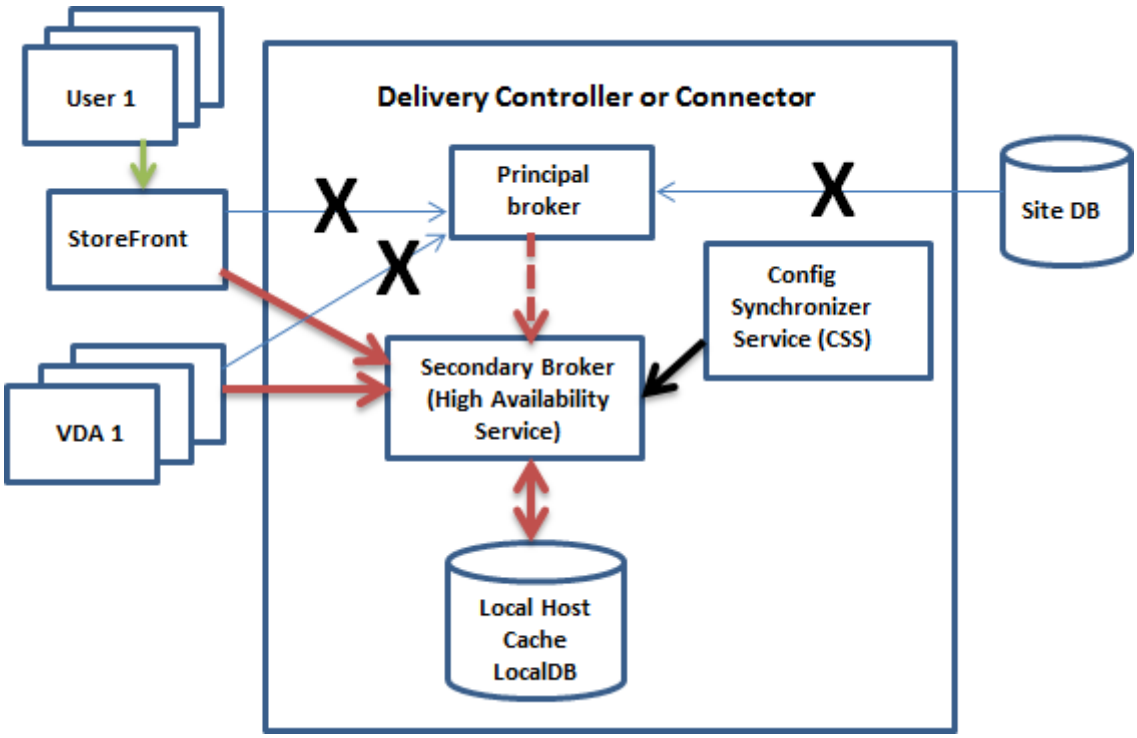
Die folgende Abbildung zeigt die Komponenten des lokalen Hostcaches und die im Normalbetrieb verwendeten Kommunikationspfade:



Normalbetrieb:

- Der *Hauptbroker* (Citrix Brokerdienst) auf einem Controller akzeptiert Verbindungsanfragen von StoreFront und kommuniziert zur Verbindung zwischen beim Controller registrierten Benutzern und VDAs mit der Sitedatenbank.
- Alle zwei Minuten wird die Konfiguration des Hauptbrokers auf Änderungen geprüft. Änderungen können von PowerShell-/Studio-Aktionen (z. B. Ändern der Eigenschaft einer Bereitstellungsgruppe) oder Systemaktionen (z. B. Maschinenzuweisungen) hervorgerufen werden.
- Wenn seit der letzten Prüfung eine Änderung gemacht wurde, verwendet der Hauptbroker CSS (Citrix Config Sync-Dienst), um die Informationen mit dem *sekundären Broker* (Citrix Dienst für hohe Verfügbarkeit) auf dem Controller zu synchronisieren (Kopie). Dabei werden nicht nur die seit der letzten Prüfung geänderten Elemente, sondern alle Brokerkonfigurationsdaten kopiert. Der sekundäre Broker importiert die Daten in eine Microsoft SQL Server Express-LocalDB-Datenbank auf dem Controller. Der CSS stellt sicher, dass die Informationen in der LocalDB-Datenbank des sekundären Brokers mit den Informationen in der Sitedatenbank übereinstimmen. Die LocalDB-Datenbank wird bei jeder Synchronisierung neu erstellt.
- Wenn seit der letzten Prüfung keine Änderungen erfolgt sind, werden keine Daten kopiert.

Die folgende Abbildung zeigt die Änderungen an den Kommunikationspfaden, wenn der Hauptbroker die Verbindung mit der Sitedatenbank verliert (d. h. zu Beginn eines Ausfalls):



Wenn ein Ausfall beginnt:

- Der Hauptbroker kann nicht mehr mit der Sitedatenbank kommunizieren und beendet das Lauschen auf StoreFront- und VDA-Informationen (X in der Abbildung). Der Hauptbroker weist dann den sekundären Broker (High Availability Service) an, auf Verbindungsanforderungen zu lauschen und diese zu verarbeiten (rote gestrichelte Linie in der Abbildung).
- Bei Ausfallbeginn hat der sekundäre Broker keine aktuellen VDA-Registrierungsdaten, aber sobald der VDA mit ihm kommuniziert, wird eine Neuregistrierung ausgelöst. Während dieses Vorgangs erhält der sekundäre Broker auch aktuelle Sitzungsinformationen zu dem betreffenden VDA.
- Während der sekundäre Broker Verbindungen verarbeitet, überwacht der Hauptbroker weiterhin die Verbindung mit der Sitedatenbank. Wenn die Verbindung wiederhergestellt ist, weist der Hauptbroker den sekundären Broker an, das Lauschen auf Verbindungsinformationen einzustellen, und nimmt das Verbindungsbrokering wieder auf. Wenn ein VDA das nächste Mal mit dem Hauptbroker kommuniziert, wird eine Neuregistrierung ausgelöst. Der sekundäre Broker entfernt alle verbleibenden VDA-Registrierungen aus dem vorherigen Ausfall und aktualisiert wieder die LocalDB-Datenbank mit den vom CSS empfangenen Konfigurationsänderungen.

Im dem unwahrscheinlichen Fall, dass ein Ausfall während einer Synchronisierung beginnt, wird der aktuelle Import verworfen und die letzte bekannte Konfiguration verwendet.

Das Ereignisprotokoll enthält Informationen über Synchronisierungen und Ausfälle. Weitere Informationen finden Sie unter “Überwachen”weiter unten.

Sie können einen Ausfall auch absichtlich auslösen. Informationen dazu, wozu dies dient und wie Sie dabei vorgehen finden Sie im Abschnitt "Erzwingen eines Ausfalls"weiter unten.

Sites mit mehreren Controllern

Unter anderem hat der CSS die Aufgabe, den sekundären Broker regelmäßig mit Informationen zu allen Controllern in der Zone zu versorgen. (Enthält Ihre Bereitstellung nicht mehrere Zonen, wirkt sich diese Aktion auf alle Controller in der Site aus.) Anhand dieser Informationen ist jeder sekundäre Broker über sekundäre Peerbroker informiert.

Die sekundären Broker kommunizieren miteinander über einen anderen Kanal. Anhand einer alphabetischen Liste der FQDNs der Maschinen, auf denen sie ausgeführt werden, ermitteln (wählen) sie, welcher sekundäre Broker bei einem Ausfall das Brokering in der Zone übernimmt. Bei einem Ausfall registrieren sich alle VDAs bei dem gewählten sekundären Broker neu. Die nicht gewählten sekundären Broker in der Zone weisen eingehende Verbindungs- und VDA-Registrierungsanfragen aktiv ab.

Wenn ein gewählter sekundärer Broker während eines Ausfalls selbst ausfällt, wird stattdessen ein anderer sekundärer Broker gewählt und die VDAs registrieren sich bei diesem.

Wird bei einem Ausfall ein Controller neu gestartet, passiert Folgendes:

- Handelt es sich bei dem Controller nicht um den gewählten primären Broker, hat der Neustart keine Auswirkungen.
- Handelt es sich um den gewählten primären Broker, wird ein anderer Controller gewählt und somit werden die VDAs neu registriert. Wenn der Neustart des Controllers beendet ist, übernimmt er automatisch das Brokering und somit werden die VDAs erneut neu registriert. In diesem Szenario kann es während der erneuten Registrierung zu Leistungseinbußen kommen.

Wenn Sie einen Controller während des normalen Betriebs ausschalten und dann während eines Ausfalls einschalten, kann der lokale Hostcache auf diesem Controller nicht verwendet werden, wenn dieser als primärer Broker ausgewählt wurde.

Das Ereignisprotokoll enthält Informationen zu diesen Wahlen. Weitere Informationen finden Sie unter "Überwachen"weiter unten.

Designüberlegungen und -anforderungen

Der lokale Hostcache wird für servergehostete Anwendungen und Desktops und statische (zugewiesene) Desktops unterstützt, nicht aber für gepoolte VDI-Desktops (die mit MCS oder PVS erstellt wurden).

Es gibt keine zeitliche Begrenzung für den Betrieb in Ausfallmodus. Allerdings sollten Sie den Normalbetrieb so schnell wie möglich wiederherstellen.

Auswirkungen eines Ausfalls:

- Sie können Studio nicht verwenden und keine PowerShell-Cmdlets ausführen.
- Hypervisor-Anmeldeinformationen können nicht vom Hostdienst abgerufen werden. Bei allen Maschinen ist der Energiezustand unbekannt, es können keine Energievorgänge ausgelöst werden. Auf dem Host eingeschaltete VMs können jedoch für Verbindungsanfragen verwendet werden.
- Zugewiesene Maschinen können nur verwendet werden, wenn die Zuweisung während des normalen Betriebs erfolgte. Neue Zuweisungen sind bei einem Ausfall nicht möglich.
- Die automatische Registrierung und Konfiguration von Remote-PC-Zugriff-Maschinen ist nicht möglich. Im normalen Betrieb registrierte und konfigurierte Maschinen können dagegen verwendet werden.
- Benutzer servergehosteter Anwendungen und Desktops können möglicherweise mehr Sitzungen verwenden als das für sie konfigurierte Sitzungslimit zulässt, wenn die Ressourcen in verschiedenen Zonen sind.
- Benutzer können Anwendungen und Desktops nur von registrierten VDAs in der Zone starten, die den aktuell aktiven/gewählten (sekundären) Broker enthält. Startvorgänge über Zonen hinweg (von einem Broker in einer Zone zu einem VDA in einer anderen Zone) werden während eines Ausfalls nicht unterstützt.

Energieverwaltete Desktop-VDAs in gepoolten Bereitstellungsgruppen, für die die Eigenschaft `ShutdownDesktopsAfterUse` aktiviert ist, werden standardmäßig bei einem Ausfall in den Wartungsmodus versetzt. Sie können diese Standardeinstellung ändern, damit solche Desktops während eines Ausfalls verwendet werden können. Während des Ausfalls können Sie sich jedoch nicht auf die Energieverwaltung verlassen. (Die Energieverwaltung wird bei Wiederaufnahme des Normalbetriebs wieder aufgenommen.) Solche Desktops können außerdem Daten des vorherigen Benutzers enthalten, weil sie nicht neu gestartet wurden.

Um das Standardverhalten außer Kraft zu setzen, müssen Sie es Site-übergreifend für jede betroffene Bereitstellungsgruppe aktivieren.

Führen Sie für die Site das folgende PowerShell Cmdlet aus:

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

Führen Sie das folgende PowerShell-Cmdlet für jede betroffene Bereitstellungsgruppe aus:

```
Set-BrokerDesktopGroup -Name "\<*name*\>"-ReuseMachinesWithoutShutdownInOutage
 $true
```

Das Aktivieren dieses Features für die Site und Bereitstellungsgruppen wirkt sich nicht auf die Funktionsweise der Eigenschaft `ShutdownDesktopsAfterUse` während des normalen Betriebs aus.

RAM-Größe:

Der LocalDB-Dienst kann ca. 1,2 GB RAM belegen (bis zu 1 GB für den Datenbankcache plus 200 MB für das Ausführen von SQL Server Express LocalDB). Der Dienst für hohe Verfügbarkeit kann bis zu 1 GB RAM belegen, wenn ein Ausfall länger andauert und viele Anmeldungen erfolgen (z. B. 12 Stunden mit 10.000 Benutzern). Diese Speicheranforderungen verstehen sich zusätzlich zu den normalen RAM-Anforderungen des Controllers, d. h. Sie müssen möglicherweise die RAM-Kapazität erhöhen.

Wenn Sie SQL Server Express für die Sitedatenbank verwenden, gibt es zwei sqlserver.exe-Prozesse.

CPU-Kern- und Socketkonfiguration:

Die CPU-Konfiguration eines Controllers, insbesondere die Zahl der für die SQL Server Express-LocalDB verfügbaren Kerne, wirkt sich direkt und in einem noch höheren Maß als die Speicherbelegung auf die Leistung des lokalen Hostcaches aus. Der CPU-Mehraufwand tritt nur während eines Ausfalls auf, wenn die Datenbank nicht erreichbar und der Dienst für hohe Verfügbarkeit aktiv ist.

Die LocalDB kann zwar bis zu 4 Kerne verwenden, ist aber auf ein einziges Socket beschränkt. Durch Hinzufügen weiterer Sockets (z. B. mit 4 Sockets mit je 1 Kern) lässt sich die Leistung nicht verbessern. Stattdessen empfiehlt Citrix die Verwendung von mehreren Sockets mit mehreren Kernen. Bei von Citrix durchgeführten Tests lieferte eine 2x3-Konfiguration (2 Sockets, 3 Kerne) eine bessere Leistung als eine 4x1- oder 6x1-Konfiguration.

Speicher:

Wenn Benutzer bei einem Ausfall auf Ressourcen zugreifen, wächst die LocalDB. Bei einem An-/Abmeldetest mit 10 Anmeldungen pro Sekunde vergrößerte sich die Datenbank beispielsweise alle 2 bis 3 Minuten um ein MB. Bei Wiederaufnahme des Normalbetriebs wird die lokale Datenbank neu erstellt und der Speicherplatz wieder zurückgegeben. Der Broker benötigt jedoch auf dem Laufwerk, auf dem die LocalDB installiert ist, ausreichend Speicherplatz für das Wachstum der Datenbank. Beim lokalen Hostcache erfolgen während eines Ausfalls außerdem zusätzliche E/A-Vorgänge: ca. 3 MB Schreibvorgänge pro Sekunde bei mehreren Hunderttausend Lesevorgängen.

Leistung:

Bei einem Ausfall verarbeitet ein einziger Broker alle Verbindungen. In Sites (oder Zonen) mit Lastausgleich zwischen mehreren Controllern muss der gewählte Broker daher möglicherweise viel mehr Anfragen verarbeiten als im Normalbetrieb. Die CPU-Anforderungen sind somit höher. Jeder einzelne Broker in der Site (Zone) muss in der Lage sein, die zusätzliche, von der LocalDB und allen betroffenen VDAs verursachte Last zu verarbeiten, da der gewählte Broker bei einem Ausfall wechseln kann.

VDI-Grenzwerte:

- In einer einzonigen VDI-Bereitstellung können während eines Ausfalls bis zu 10.000 VDAS effektiv bewältigt werden.
- In einer VDI-Bereitstellung mit mehreren Zonen können bis zu 10.000 VDAs pro Zone und insgesamt bis zu 40.000 VDAs pro Site gehandhabt werden. Beispielsweise ist ein effektives Handling der folgenden Sites während eines Ausfalls möglich:

  - Eine Site mit vier Zonen mit je 10.000 VDAs
  - Eine Site mit sieben Zonen, von denen eine 10.000 VDAs enthält und die restlichen sechs je 5.000 VDAs

Bei einem Ausfall kann die Lastverwaltung der Site beeinträchtigt werden. Lastauswertungsprogramme (und insbesondere Sitzungszahlregeln) werden möglicherweise überschritten.

Während der Zeit, die für die Neuregistrierung aller VDAs bei einem Broker benötigt wird, hat der Broker evtl. nicht alle Informationen über die aktuellen Sitzungen. Die Verbindungsanfrage eines Benutzers kann während dieses Zeitraums daher zum Start einer neuen Sitzung führen, obwohl eine Wiederverbindung mit einer vorhandenen Sitzung möglich wäre. Dieses Intervall (des Abrufs von Sitzungsinformationen bei allen VDAs durch den "neuen"Broker) ist unvermeidlich. Auf Sitzungen, die bei Ausfallbeginn verbunden waren, hat das Übergangsintervall keine Auswirkungen, doch bei neuen Sitzungen und erneuten Sitzungsverbindungen ist eine Beeinträchtigung möglich.

Das Intervall tritt immer dann auf, wenn die VDAs sich bei einem anderen Broker neu registrieren müssen:

- Ausfallbeginn: bei der Migration von einem Hauptbroker zu einem sekundären Broker
- Brokerfehler während eines Ausfalls: bei der Migration von dem fehlerhaften sekundären Broker zu dem neu gewählten sekundären Broker
- Wiederherstellung nach Ausfall: bei Wiederaufnahme des Normalbetriebs und der erneuten Übernahme der Steuerung durch den Hauptbroker

Sie können das Intervall verringern, indem Sie den Registrierungswert "HeartbeatPeriodMs"für Citrix Broker Protocol (Standardwert = 600000 ms, d. h. 10 Minuten) verringern. Dieser Taktwert ist doppelt so lang wie das Intervall, das der VDA für Pings verwendet. Der Standardwert führt zu einem Ping alle 5 Minuten.

Mit dem folgenden Befehl ändern Sie beispielsweise den Heartbeat auf fünf Minuten (300.000 Millisekunden), was alle 2,5 Minuten zu einem Ping führt:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs
-PropertyType DWORD –Value 300000
```

Das Intervall kann nicht vollständig eliminiert werden, egal wie schnell die VDAs registrieren.

Die Dauer der Synchronisierung zwischen den Brokern erhöht sich mit steigender Anzahl der Objekte (VDAs, Anwendungen, Gruppen usw.). Die Synchronisierung von 5000 VDAs kann beispielsweise 10 Minuten oder länger dauern. Informationen zu Synchronisierungseinträgen im Ereignisprotokoll finden Sie unter "Überwachen"weiter unten.

Verwalten des lokalen Hostcache

Damit der lokale Hostcache ordnungsgemäß funktioniert, muss die PowerShell-Ausführungsrichtlinie für jeden Controller auf "RemoteSigned", "Unrestricted"oder "Bypass"festgelegt sein.

SQL Server Express-LocalDB

Die vom lokalen Hostcache verwendete Microsoft SQL Server Express-LocalDB wird automatisch installiert, wenn Sie einen Controller installieren oder von einer Version vor 7.9 aktualisieren. Die LocalDB erfordert keine Wartung durch den Administrator. Nur der sekundäre Broker kommuniziert mit dieser Datenbank, sie kann nicht mit PowerShell-Cmdlets geändert werden. Die LocalDB kann nicht für mehrere Controller freigegeben werden.

Die Datenbanksoftware der SQL Server Express-LocalDB wird unabhängig davon installiert, ob der lokale Hostcache aktiviert wird.

Um die Installation zu verhindern, installieren bzw. aktualisieren Sie den Controller mit dem Befehl "XenDesktopServerSetup.exe"und verwenden Sie die Option /exclude "Local Host Cache Storage (LocalDB)". Der lokale Hostcache funktioniert allerdings nicht ohne die Datenbank und Sie können keine andere Datenbank für den sekundären Broker verwenden.

Die Installation der LocalDB-Datenbank ist irrelevant für die Entscheidung, ob Sie SQL Server Express zur Verwendung als Sitedatenbank installieren.

Standardeinstellungen nach Installation bzw. Upgrade von XenApp- oder XenDesktop

Bei einer Neuinstallation von XenApp und XenDesktop ist der lokale Hostcache standardmäßig aktiviert. (Das Verbindungsleasing ist standardmäßig deaktiviert.)

Nach einem Upgrade bleibt die Einstellung für den lokalen Hostcache erhalten. War der lokale Hostcache beispielsweise in der Vorgängerversion aktiviert, ist er auch in der aktualisierten Version aktiviert. Wenn der lokale Hostcache in der früheren Version nicht aktiviert war (oder nicht unterstützt wurde), bleibt er in der aktualisierten Version deaktiviert.

Aktivieren und Deaktivieren des lokalen Hostcaches

Zum Aktivieren des lokalen Hostcache geben Sie Folgendes ein:

```
Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled
 $false
```

Dieses Cmdlet deaktiviert außerdem das Verbindungsleasing. Aktivieren Sie den lokalen Hostcache und das Verbindungsleasing nicht gleichzeitig.

Um zu ermitteln, ob der lokale Hostcache aktiviert ist, geben Sie Folgendes ein:

```
Get-BrokerSite
```

Vergewissern Sie sich, dass die Eigenschaft “LocalHostCacheEnabled”auf “True”und die Eigenschaft “ConnectionLeasingEnabled”auf “False”eingestellt ist.

Zum Deaktivieren des lokalen Hostcache und Aktivieren des Verbindungsleasings geben Sie Folgendes ein:

```
Set-BrokerSite -LocalHostCacheEnabled $false -ConnectionLeasingEnabled
 $true
```

Funktionsprüfung des lokalen Hostcache

Überprüfung des lokalen Hostcache auf korrekte Einrichtung und fehlerfreien Betrieb:

- Stellen Sie sicher, dass Synchronisierungsimporte erfolgreich abgeschlossen werden. Überprüfen Sie die Ereignisprotokolle.
- Stellen Sie sicher, dass die LocalDB von SQL Server Express auf jedem Delivery Controller erstellt wurde. Dadurch wird bestätigt, dass der Dienst für hohe Verfügbarkeit bei Bedarf übernehmen kann.
- Navigieren Sie auf dem Delivery Controller-Server zu C:\Windows\ServiceProfiles\NetworkService.
- Überprüfen Sie, ob HaDatabaseName.mdf und HaDatabaseName_log.ldf erstellt wurde.
- Erzwingen Sie einen Ausfall bei den Delivery Controllern. Vergessen Sie nicht, nach der Funktionsprüfung des lokalen Hostcache alle Controller wieder in den normalen Modus zu versetzen. Dies kann ca. 15 Minuten dauern, um eine VDA-Registrierungsflut zu vermeiden.

Erzwingen eines Ausfalls

In folgenden Situationen kann das Erzwingen eines Datenbankausfalls erforderlich sein:

- Die Netzwerkverbindung wird wiederholt unterbrochen. Durch das Erzwingen eines Ausfalls bis zum Beheben des Netzwerkproblems werden fortlaufende Übergänge zwischen normalem Modus und Ausfallmodus vermieden.
- Zum Testen eines Notfallwiederherstellungsplans
- Beim Ersetzen oder Warten des Sitedatenbankservers

Zum Erzwingen eines Ausfalls bearbeiten Sie die Registrierung aller Server, die einen Delivery Controller enthalten.

- Legen Sie unter HKLM\Software\Citrix\DesktopServer\LHC OutageModeForced auf 1 fest. Dadurch wird der Broker angewiesen, unabhängig vom Zustand der Datenbank in den Aus-

fallmodus zu wechseln. (Wenn Sie den Wert auf 0 festlegen, wird der Ausfallmodus auf dem Server beendet.)
- In einer Citrix Cloud wechselt der Connector unabhängig vom Zustand der Verbindung mit der Steuerungsebene oder der primären Zone in den Ausfallmodus.

Überwachung

Ereignisprotokolle enthalten Informationen zu Synchronisierungen und Ausfällen.

Config Synchronizer Service:

Im Normalbetrieb können beim Kopieren und Exportieren der Brokerkonfiguration durch den Config Service und beim Importieren in die LocalDB unter Einsatz des Diensts für hohe Verfügbarkeit (sekundärer Broker) die folgenden Ereignisse auftreten.

- 503: Es wurde eine Änderung an der Konfiguration des Hauptbrokers erkannt und ein Import wird gestartet.
- 504: Die Brokerkonfiguration wurde erfolgreich kopiert, exportiert und in die LocalDB importiert.
- 505: Der Import in die LocalDB ist fehlgeschlagen (siehe weiter unten).
- 510: Es wurden keine Konfigurationsdienst-Konfigurationsdaten vom primären Konfigurationsdienst empfangen.
- 517: Ein Problem ist bei der Kommunikation mit dem primären Broker aufgetreten.
- 518: Das Config Sync-Skript wurde abgebrochen, weil der sekundäre Broker (Hohe Verfügbarkeit) nicht ausgeführt wird.

Dienst für hohe Verfügbarkeit:

- 3502: Ein Ausfall ist aufgetreten und der sekundäre Broker (Dienst für hohe Verfügbarkeit) hat das Brokering übernommen.
- 3503: Ein Ausfall wurde behandelt und der Normalbetrieb wieder aufgenommen.
- 3504: Gibt an, welcher sekundäre Broker gewählt wurde und welche anderen Broker bei der Wahl beteiligt waren.

Problembehandlung

Mehrere Problembehandlungstools sind verfügbar, wenn ein Synchronisierungsimport in die LocalDB fehlschlägt und ein 505-Ereignis verzeichnet wird.

Ablaufverfolgung mit CDF: Enthält Optionen für die Module ConfigSyncServer und BrokerLHC. In Kombination mit anderen Brokermodulen kann mit diesen Optionen das Problem in der Regel identifiziert werden.

Bericht: Wenn ein Synchronisierungsimport fehlschlägt, können Sie einen Bericht erstellen. Der Bericht endet mit dem Objekt, das den Fehler verursacht hat. Das Berichtsfeature wirkt sich auf die Synchronisierungsgeschwindigkeit aus. Deshalb empfiehlt Citrix, es zu deaktivieren, wenn es nicht verwendet wird.

Zum Aktivieren von CSS und Erstellen eines Ablaufverfolgungsberichts geben Sie folgenden Befehl ein:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

Der HTML-Bericht wird unter `C:\\Windows\\ServiceProfiles\\NetworkService\\AppData\\Local\\Temp\\CitrixBrokerConfigSyncReport.html` veröffentlicht.

Wenn der Bericht generiert wurde, deaktivieren Sie das Berichtsfeature durch Eingabe des folgenden Befehls:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

Exportieren der Brokerkonfiguration: stellt die exakte Konfiguration zum Debuggen zur Verfügung.

```
Export-BrokerConfiguration | Out-File file-pathname
```

Beispiel: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

Verwalten von Sicherheitsschlüsseln

May 9, 2022

> **Hinweis:**
>
> Sie müssen dieses Feature in Kombination mit StoreFront 1912 LTSR CU2 oder höher verwenden.

Mit diesem Feature können nur genehmigte StoreFront- und Citrix Gateway-Maschinen mit Citrix Delivery Controllern kommunizieren. Nachdem Sie das Feature aktiviert haben, werden alle Anforderungen ohne Schlüssel blockiert. Verwenden Sie diese Funktion, um eine zusätzliche Sicherheitsebene zum Schutz vor Angriffen aus dem internen Netzwerk hinzuzufügen.

Ein allgemeiner Workflow zur Verwendung des Features ist folgender:

1. Aktivieren Sie das Feature in Studio per PowerShell-SDK.
2. Konfigurieren Sie die Einstellungen in Studio. (Verwenden Sie die Studio-Konsole oder PowerShell.)
3. Konfigurieren Sie die Einstellungen in StoreFront. (Verwenden Sie PowerShell.)

Aktivieren Sie das Sicherheitsschlüsselfeature

Standardmäßig ist das Feature deaktiviert. Verwenden Sie das Remote PowerShell SDK, um das Feature zu aktivieren. Weitere Informationen zum Remote PowerShell SDK finden Sie unter SDKs und APIs.

Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Führen Sie das XenApp and XenDesktop Remote PowerShell SDK aus.
2. Führen Sie in einem Befehlsfenster die folgenden Befehle aus:
    - `Add-PSSnapIn Citrix*`. Mit diesem Befehl werden die Citrix Snap-Ins hinzugefügt.
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

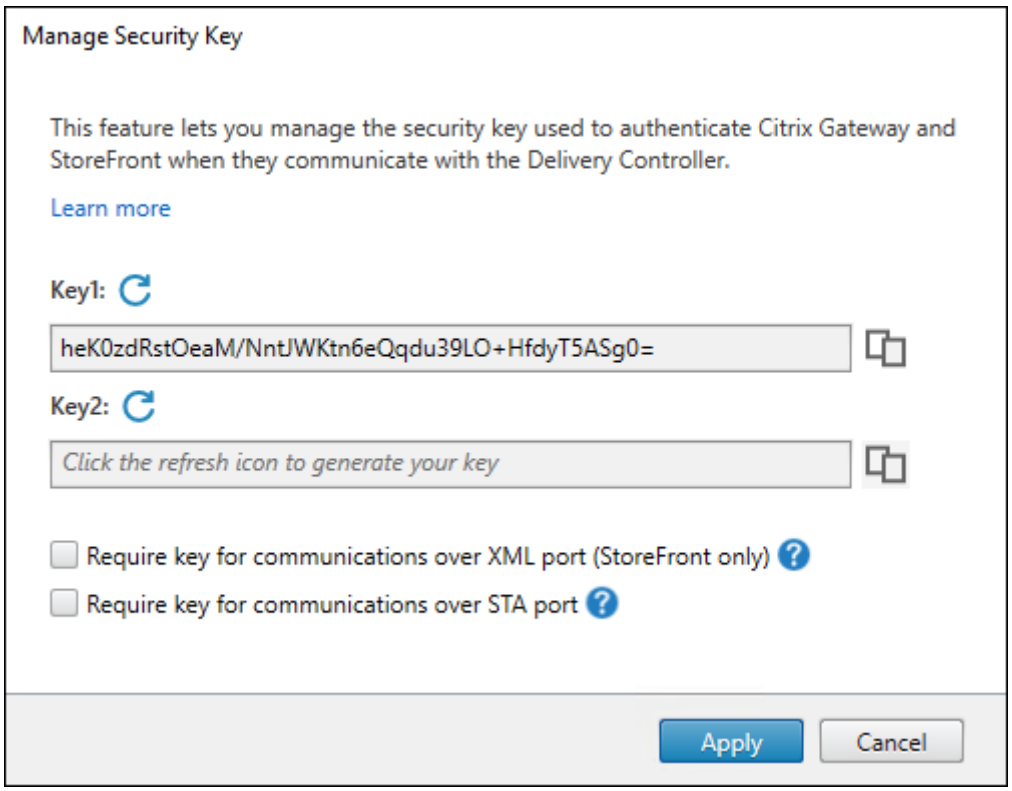
Konfigurieren von Einstellungen in Studio

Sie können Einstellungen in Studio über die Studio-Konsole oder PowerShell konfigurieren.

Verwenden der Studio-Konsole

Wenn Sie das Feature aktiviert haben, navigieren Sie zu **Studio > Konfiguration > Sicherheitsschlüssel verwalten**. Möglicherweise müssen Sie auf **Aktualisieren** klicken, damit die Option **Sicherheitsschlüssel verwalten** angezeigt wird.

Nachdem Sie auf **Sicherheitsschlüssel verwalten**geklickt haben, wird das Fenster **Sicherheitsschlüssel verwalten** angezeigt.



Wichtig:

- Es stehen zwei Schlüssel zur Verfügung. Sie können für die Kommunikation über den XML- und den STA-Port denselben oder verschiedene Schlüssel verwenden. Wir empfehlen, dass Sie jeweils nur einen Schlüssel verwenden. Der nicht verwendete Schlüssel dient nur zur Schlüsselrotation.
- Klicken Sie nicht auf das Aktualisierungssymbol, um den bereits verwendeten Schlüssel zu aktualisieren. Dies führt zu einer Dienstunterbrechung.

Klicken Sie auf das Aktualisierungssymbol, um neue Schlüssel zu generieren

Schlüssel für Kommunikation über XML-Port erforderlich (nur StoreFront). Ist diese Option aktiviert, dann ist ein Schlüssel erforderlich, um die Kommunikation über den XML-Port zu authentifizieren. StoreFront kommuniziert über diesen Port mit Citrix Cloud. Informationen zum Ändern des XML-Ports finden Sie im Knowledge Center-Artikel CTX127945.

Schlüssel für die Kommunikation über den STA-Port erforderlich. Ist diese Option aktiviert, dann ist ein Schlüssel erforderlich, um die Kommunikation über den STA-Port zu authentifizieren. Citrix Gateway und StoreFront kommunizieren über diesen Port mit Citrix Cloud. Informationen zum Ändern des STA-Ports finden Sie im Knowledge Center-Artikel CTX101988.

Nachdem Sie die Änderungen übernommen haben, klicken Sie auf **Schließen**, um das Fenster **Sicherheitsschlüssel verwalten** zu schließen.

Verwenden von PowerShell

Nachfolgend sind die den Studio-Vorgängen entsprechenden PowerShell-Schritte aufgeführt.

1. Führen Sie das XenApp und XenDesktop Remote PowerShell SDK aus.
2. Führen Sie in einem Befehlsfenster folgenden Befehl aus:
   - `Add-PSSnapIn Citrix*`
3. Führen Sie die folgenden Befehle aus, um einen Schlüssel zu generieren und Key1 einzurichten:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Führen Sie die folgenden Befehle aus, um einen Schlüssel zu generieren und Key2 einzurichten:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Führen Sie einen oder beide der folgenden Befehle aus, um die Verwendung eines Schlüssels bei der Authentifizierung der Kommunikationen zu aktivieren:
   - Zum Authentifizieren der Kommunikation über den XML-Port:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Zum Authentifizieren der Kommunikation über den STA-Port:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Befehlen.

Konfigurieren von Einstellungen in StoreFront

Nach Abschluss der Konfiguration in Studio müssen Sie relevante Einstellungen in StoreFront mit PowerShell konfigurieren.

Führen Sie auf dem StoreFront-Server die folgenden PowerShell-Befehle aus:

- Um den Schlüssel für die Kommunikation über den XML-Port zu konfigurieren, verwenden Sie die Befehle `Get-STFStoreServie` und `Set-STFStoreService`. Beispiel:
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>`
- Um den Schlüssel für die Kommunikation über den STA-Port zu konfigurieren, verwenden Sie den Befehl `New-STFSecureTicketAuthority`. Beispiel:

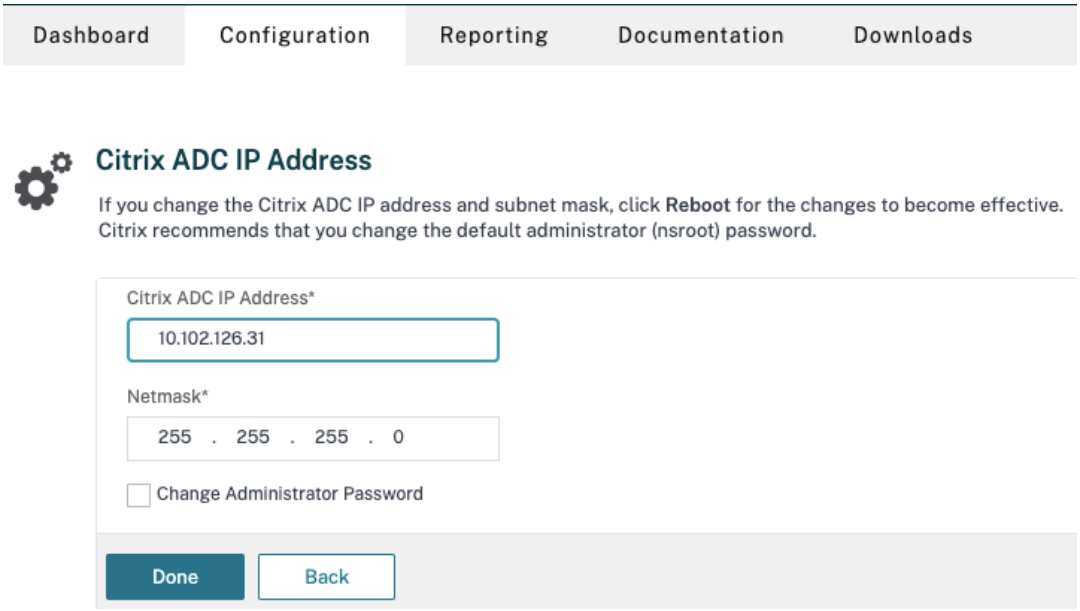

```
- PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL
  > -StaValidationEnabled $true -StavalidationSecret <the key
  you generated in Studio>
```

Anleitungen und Informationen zur Syntax finden Sie in der Hilfe zu PowerShell-Befehlen.

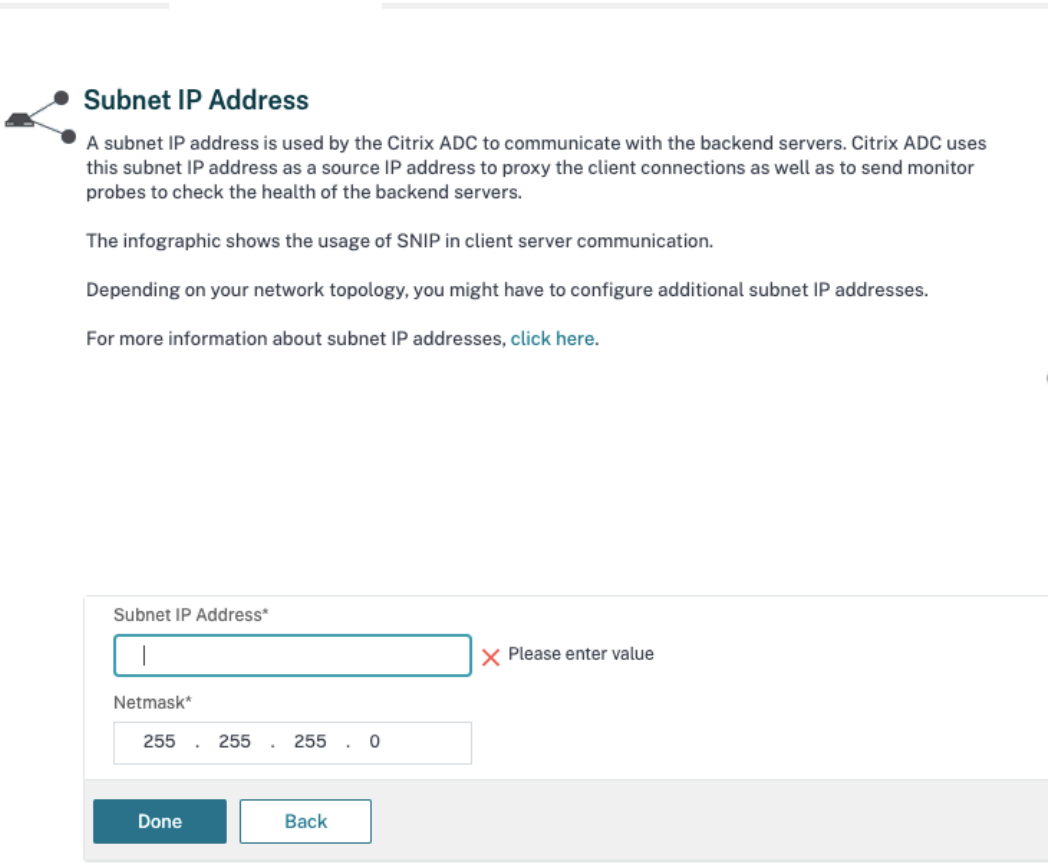
Konfigurieren der Einstellungen in Citrix ADC

> **Hinweis:**
>
> Die Konfiguration dieses Features in Citrix ADC ist nur erforderlich, wenn Sie Citrix ADC als Gateway verwenden. Wenn Sie Citrix ADC verwenden, führen Sie die folgenden Schritte aus.

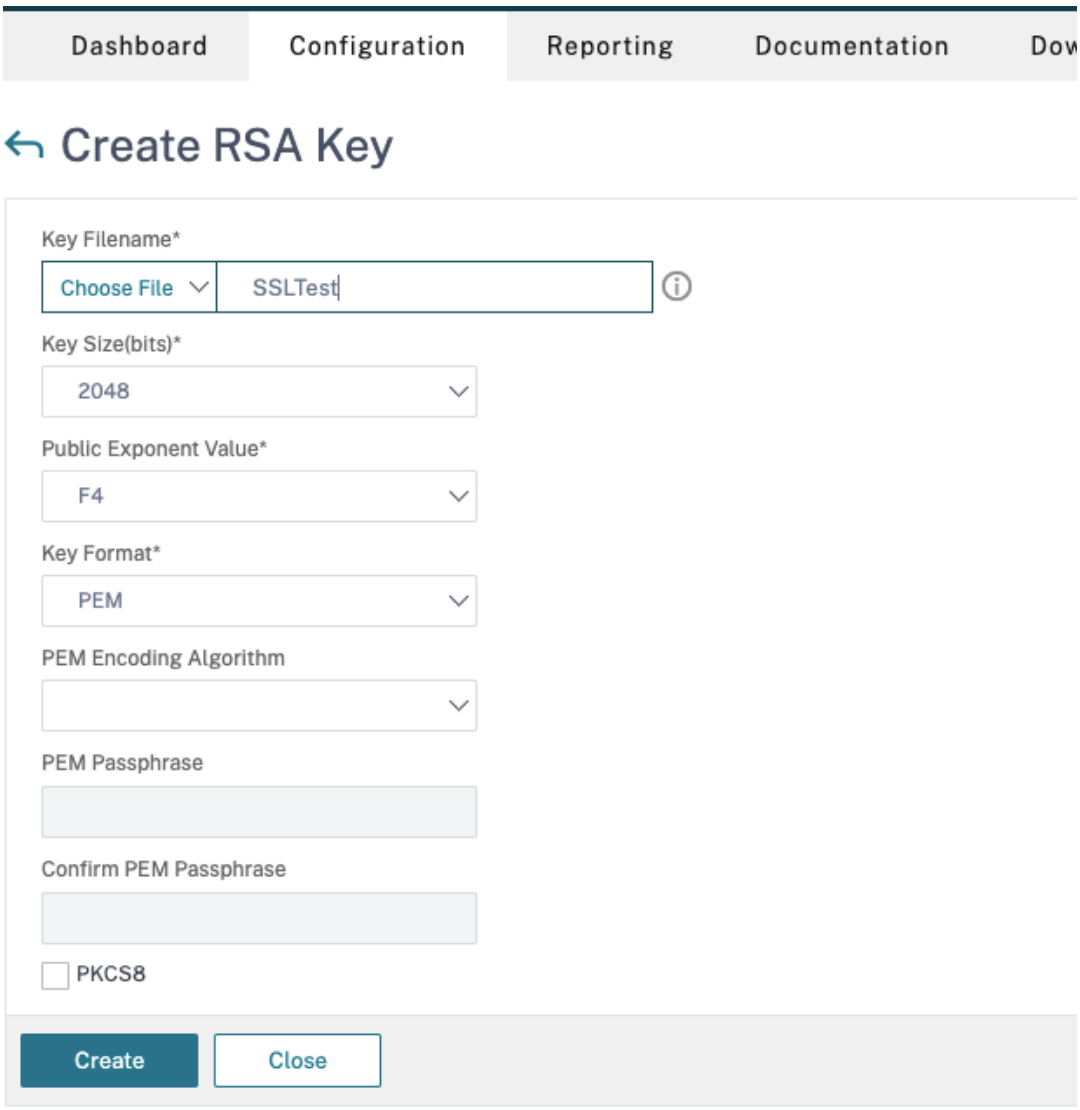
1. Vergewissern Sie sich, dass die erforderliche Konfiguration ausgeführt wurde:
   - Die folgenden IP-Adressen im Zusammenhang mit Citrix ADC wurden konfiguriert.
     - Citrix ADC Management-IP-Adresse (NSIP) für den Zugriff auf die Citrix ADC-Konsole. Weitere Informationen finden Sie unter Konfigurieren der NSIP-Adresse.



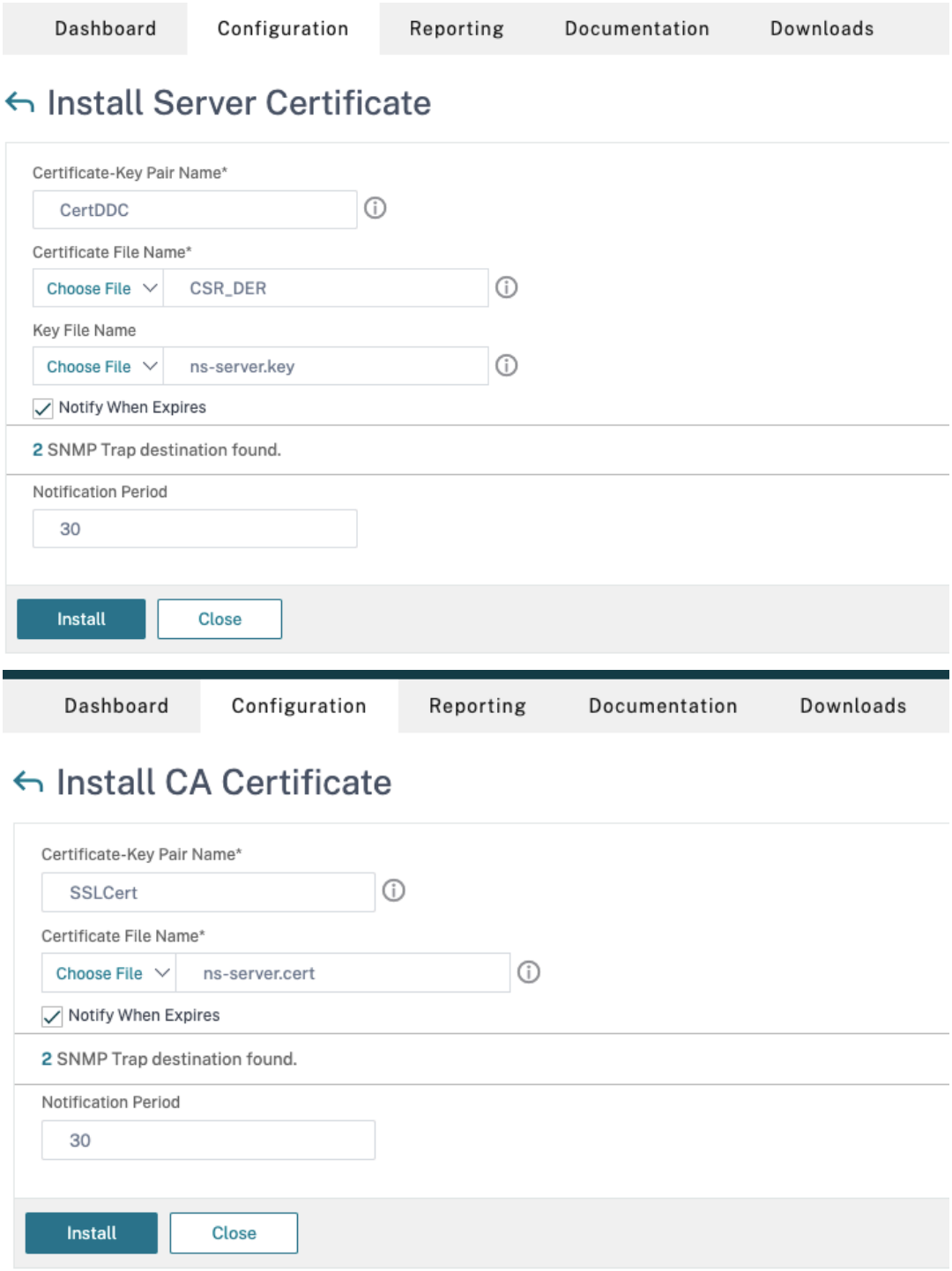
     - Subnetz-IP-Adresse (SNIP) zur Kommunikation zwischen der Citrix ADC Appliance und den Back-End-Servern. Weitere Informationen finden Sie unter Konfigurieren von Subnetz-IP-Adressen.
     - Virtuelle IP-Adresse von Citrix Gateway und des Load Balancers zur Anmeldung bei der ADC Appliance für den Sitzungsstart. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.



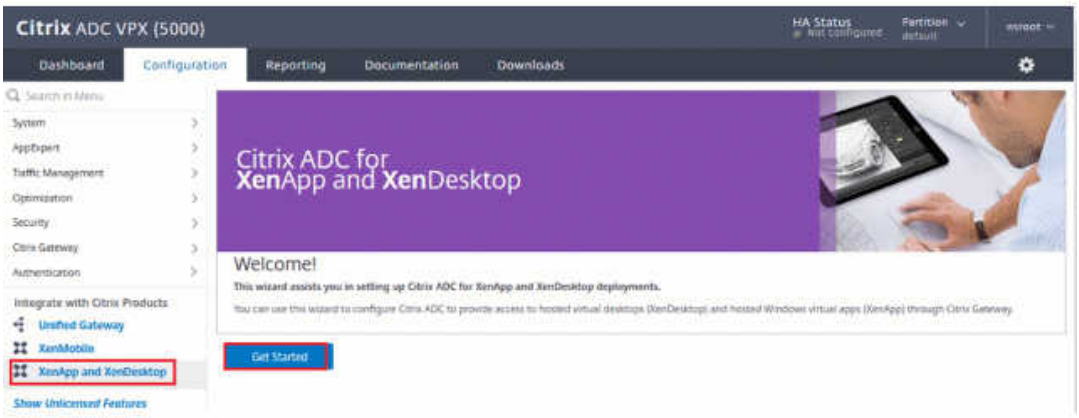
- Die erforderlichen Modi und Features in der Citrix ADC Appliance sind aktiviert.
  - Um die Modi zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Mode**.
  - Um die Features zu aktivieren, gehen Sie in Citrix ADC zu **System > Settings > Configure Basic Features**.
- Die Konfiguration für Zertifikate wurde ausgeführt.
  - Die Zertifikatsignieranforderung (CSR) wurde erstellt. Weitere Informationen finden Sie unter Erstellen eines Zertifikats.



- Das Serverzertifikat, das ZS-Zertifikat und das Stammzertifikat wurden installiert. Weitere Informationen finden Sie unter Installieren, Links und Updates.

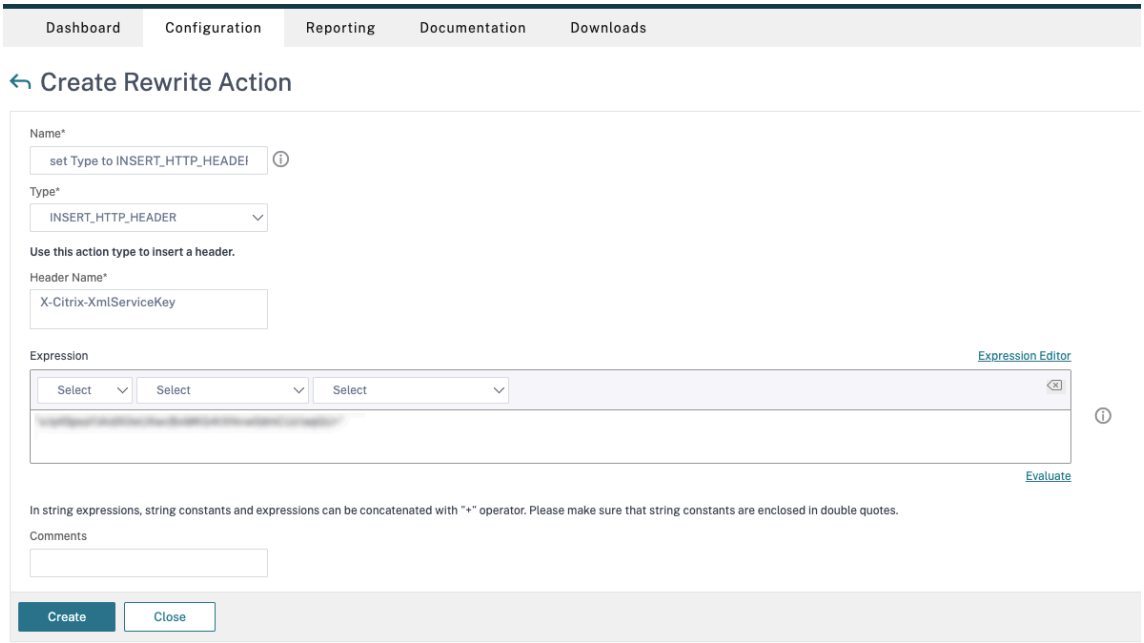


- Für Citrix Virtual Desktops wurde ein Citrix Gateway erstellt. Testen Sie die Verbindung durch Klicken auf die Schaltfläche **Test STA Connectivity**, um sicherzustellen, dass die virtuellen Server online sind. Weitere Informationen finden Sie unter Einrichten von Citrix ADC für Citrix Virtual Apps and Desktops.



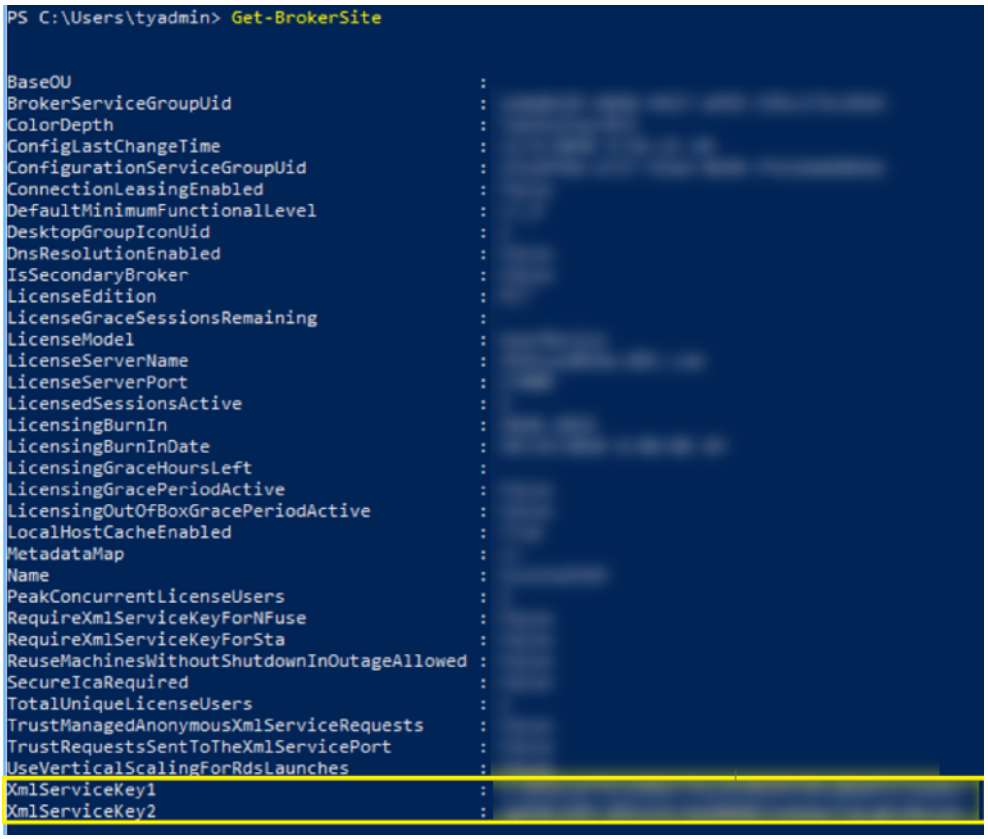
2. Fügen Sie eine Rewrite-Aktion hinzu. Weitere Informationen finden Sie unter Konfigurieren einer Rewrite-Aktion.

   a) Gehen Sie zu **AppExpert > Rewrite > Actions**.
   b) Klicken Sie auf **Hinzufügen**, um eine neue Rewrite-Aktion hinzuzufügen. Sie können die Aktion "set Type to INSERT_HTTP_HEADER"nennen.



   a) Wählen Sie unter **Type** die Option **INSERT_HTTP_HEADER**.
   b) Geben Sie im Feld **Header Name** "X-Citrix-XmlServiceKey"ein.
   c) Fügen Sie unter **Ausdruck** <`XmlServiceKey1 value`> mit Anführungszeichen hinzu.

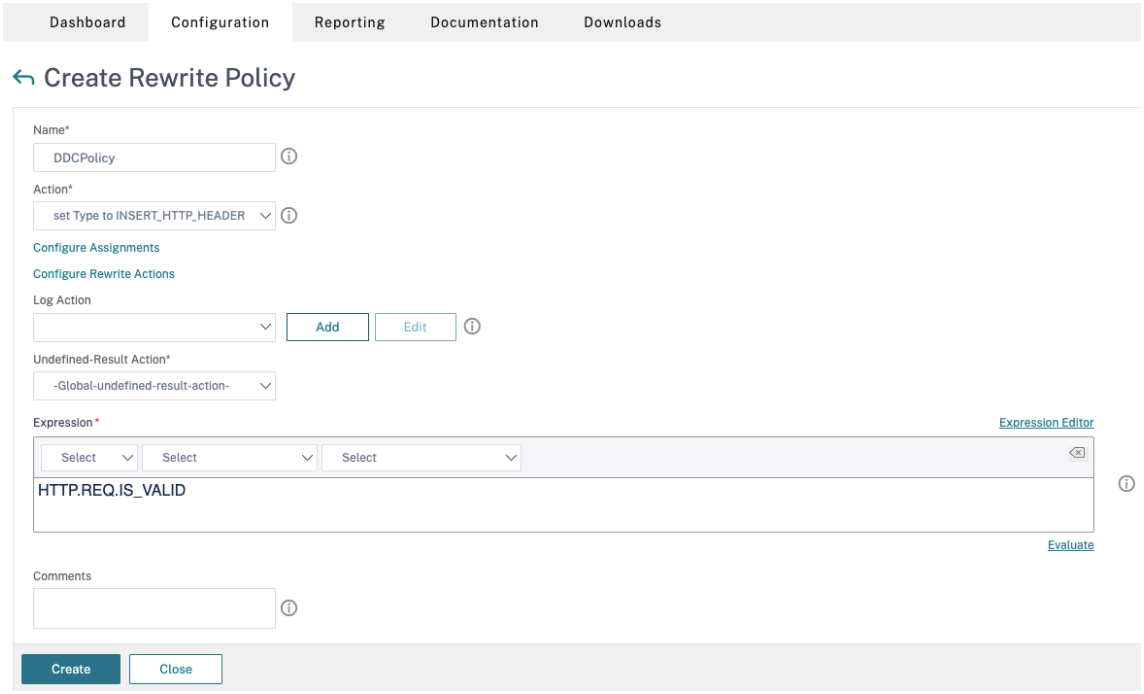
Sie können den XmlServiceKey1-Wert aus der Desktop Delivery Controller-Konfiguration kopieren.



3. Fügen Sie eine Rewrite-Richtlinie hinzu. Weitere Informationen finden Sie unter Konfigurieren einer Rewrite-Richtlinie.

   a) Gehen Sie zu **AppExpert > Rewrite > Policies**.

   b) Klicken Sie auf **Add**, um eine neue Richtlinie hinzuzufügen.



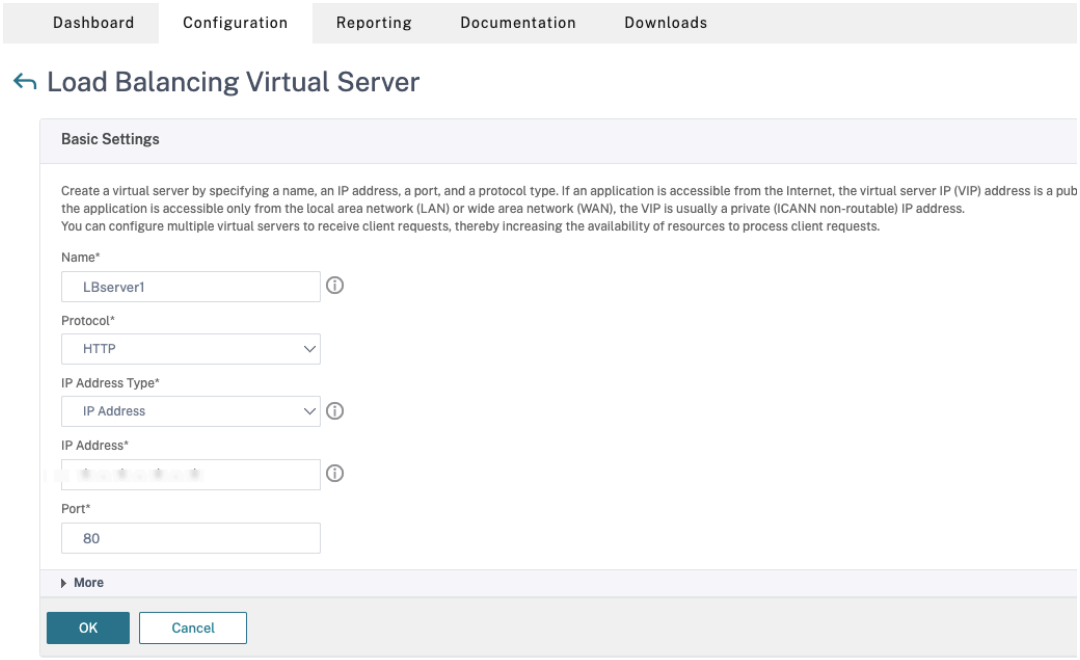
a) Wählen Sie unter **Action** die im vorherigen Schritt erstellte Aktion aus.
b) Fügen Sie unter **Expression** “HTTP.REQ.IS_VALID”hinzu.
c) Klicken Sie auf **OK**.

4. Richten Sie den Lastenausgleich ein. Sie müssen einen virtuellen Lastausgleichsserver pro STA-Server konfigurieren. Ansonsten können die Sitzungen nicht gestartet werden.

   Weitere Informationen finden Sie unter Einrichten des einfachen Lastenausgleichs.

   a) Erstellen Sie einen virtuellen Lastausgleichsserver.

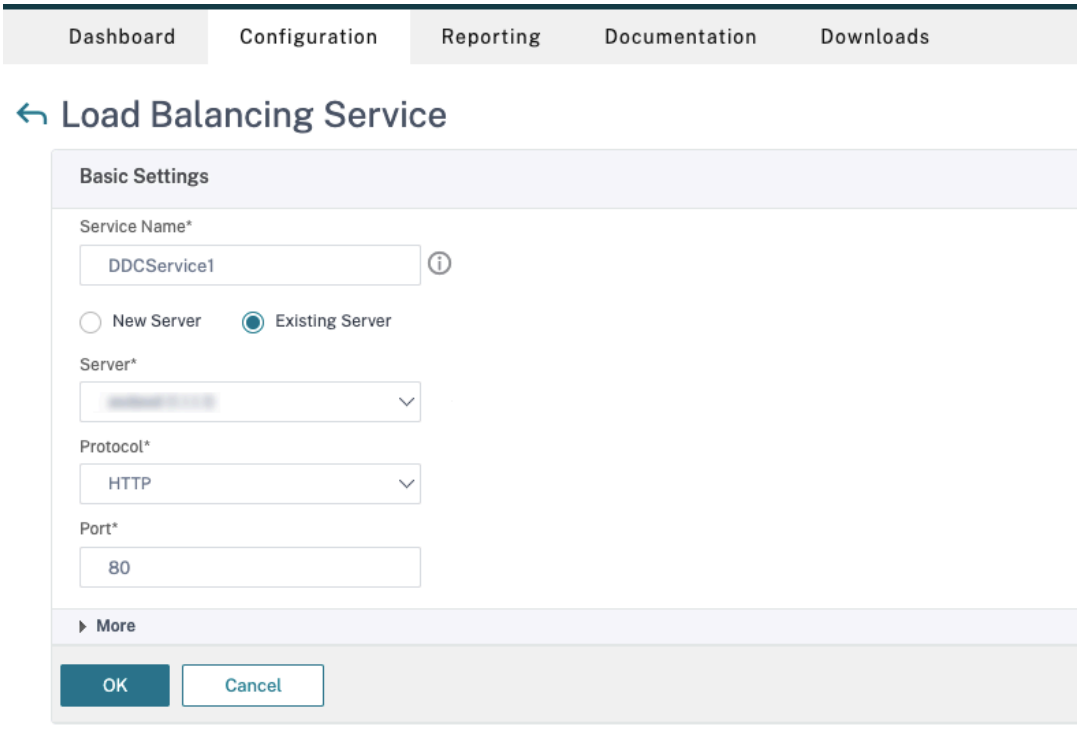
      - Navigieren Sie zu **Traffic Management > Load Balancing > Servers**.
      - Klicken Sie auf der Seite **Virtual Servers** auf **Add**.



- Wählen Sie unter **Protocol** die Option **HTTP**.
- Geben Sie die IP-Adresse des virtuellen Lastausgleichsserver ein und wählen Sie für **Port** die Option **80**.
- Klicken Sie auf **OK**.

b) Erstellen Sie einen Lastausgleichsdienst.

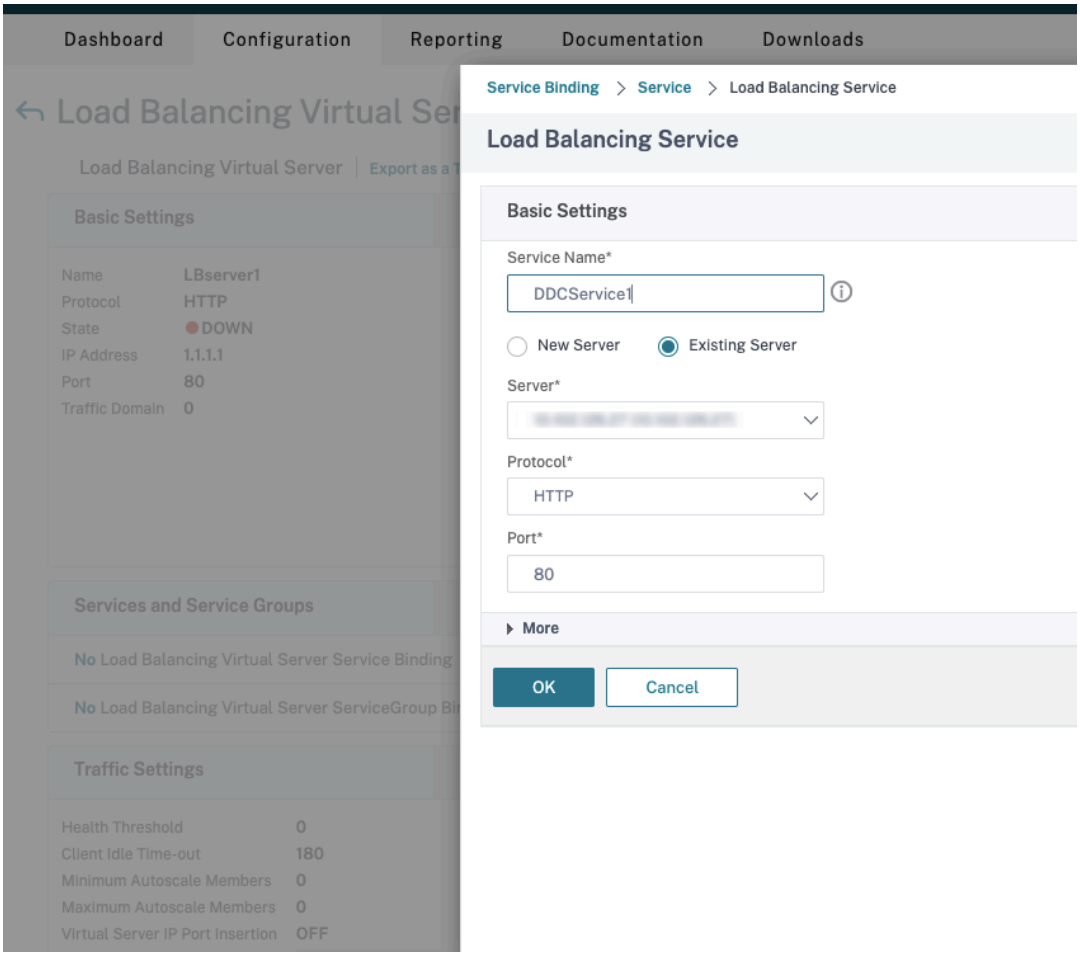
- Navigieren Sie zu **Traffic Management > Load Balancing > Services**.



- Wählen Sie unter **Existing Server** den im vorherigen Schritt erstellten virtuellen Server aus.
- Wählen Sie für **Protocol** die Option **HTTP** und für **Port** die Option **80**.
- Klicken Sie auf **OK** und dann auf **Done**.

c) Binden Sie den Dienst an den virtuellen Server.

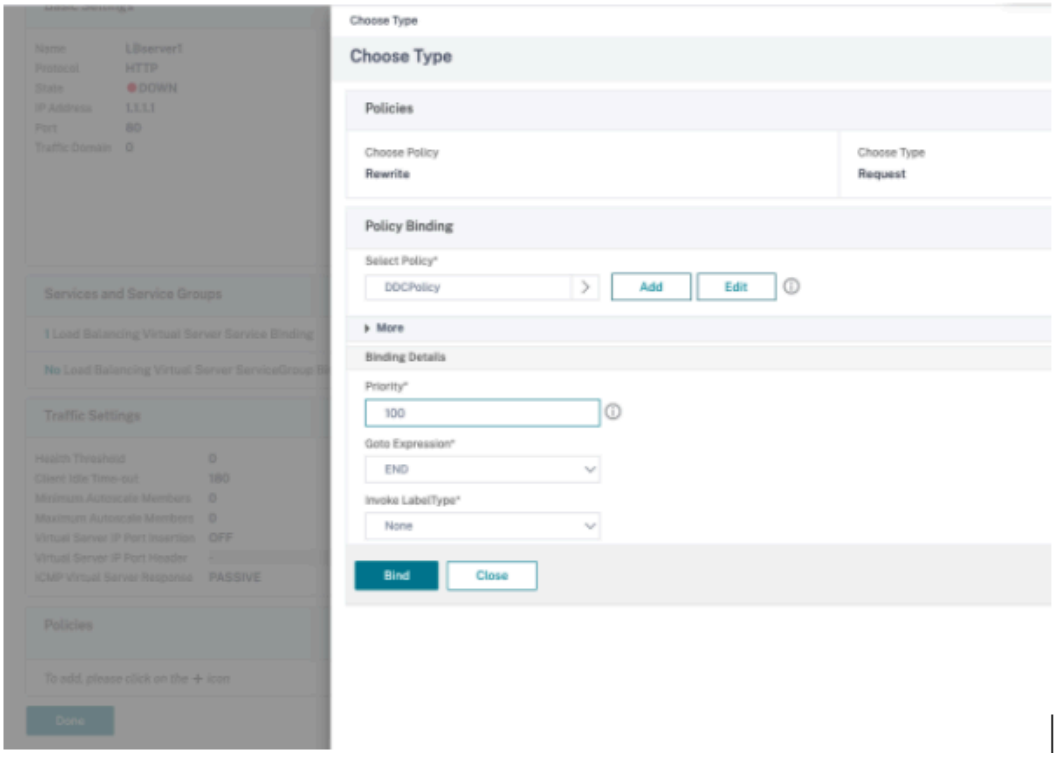
- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie in **Services and Service Groups** auf **No Load Balancing Virtual Server Service Group Binding**.



- Wählen Sie unter **Service Binding** den zuvor erstellten Dienst aus.
- Klicken Sie auf **Bind**.

d) Binden Sie die zuvor erstellte Rewrite-Richtlinie an den virtuellen Server.

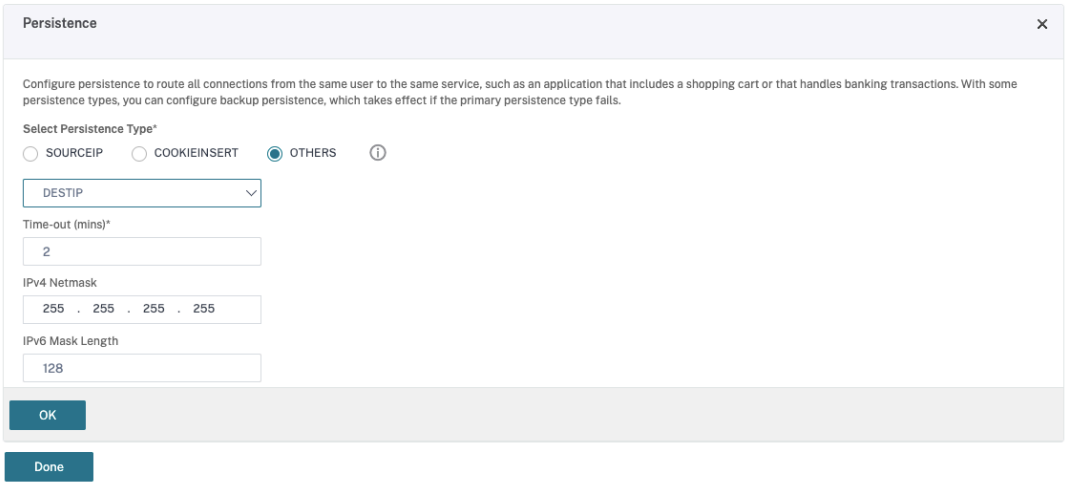
- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie unter **Advanced Settings** auf **Policies** und im Bereich **Policies** auf **+**.



- Wählen Sie unter **Choose Policy** die Option **Rewrite** und für **Choose Type**, die Option **Request**.
- Klicken Sie auf **Weiter**.
- Wählen Sie unter **Select Policy** die zuvor erstellte Rewrite-Richtlinie aus.
- Klicken Sie auf **Bind**.
- Klicken Sie auf **Fertig**.

e) Legen Sie ggf. die Persistenz für den virtuellen Server fest.

- Wählen Sie den zuvor erstellten virtuellen Server aus und klicken Sie auf **Edit**.
- Klicken Sie unter **Advanced Settings** auf **Persistence**.



- Wählen Sie als Persistenztyp **Others**.
- Wählen Sie **DESTIP**, um Persistenzsitzungen basierend auf der IP-Adresse des vom virtuellen Server ausgewählten Diensts (Ziel-IP-Adresse) zu erstellen
- Fügen Sie in **IPv4 Netmask** die Netzwerkmaske des DDC hinzu.
- Klicken Sie auf **OK**.

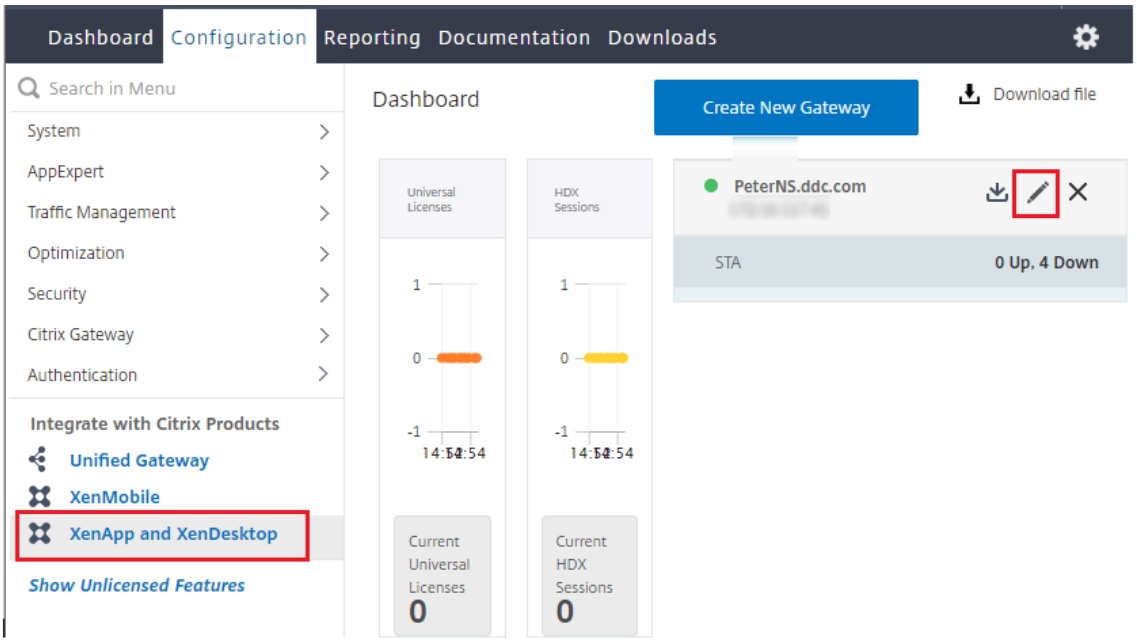
f) Wiederholen Sie diese Schritte für den anderen virtuellen Server.

Konfigurationsänderungen bei bereits mit Citrix Virtual Desktops konfigurierter Citrix ADC Appliance

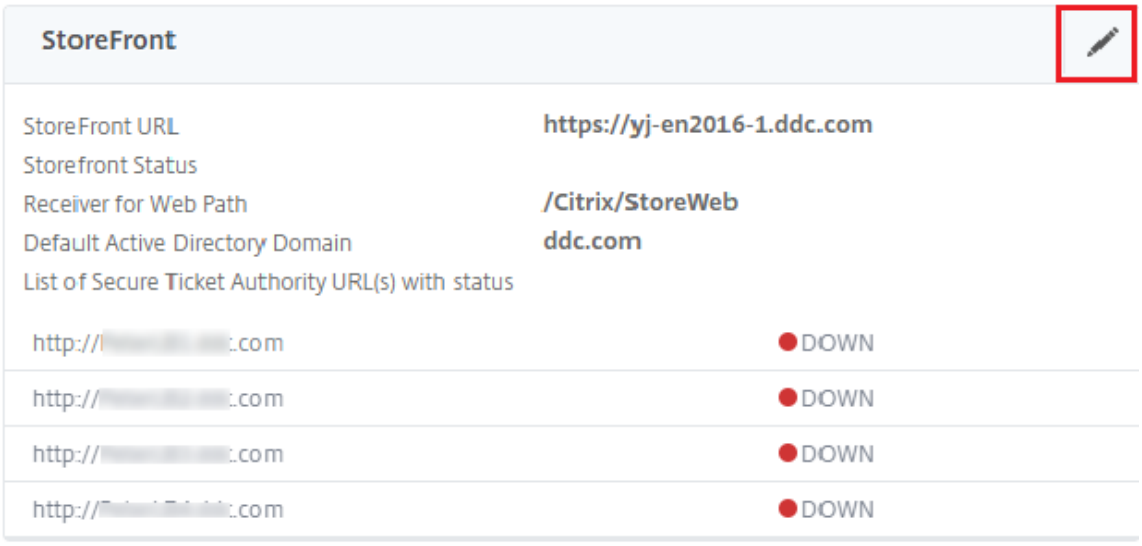
Wenn die Citrix ADC Appliance bereits mit Citrix Virtual Desktops konfiguriert ist, müssen Sie zur Verwendung von Secure XML die folgenden Konfigurationsänderungen vornehmen.

- Ändern Sie vor dem Start der Sitzung die **Secure Ticket Authority-URL** des Gateways, um die FQDNs der virtuellen Lastausgleichsserver zu verwenden.
- Stellen Sie sicher, dass der Parameter `TrustRequestsSentToTheXmlServicePort` auf "False"festgelegt ist. Standardmäßig ist der Parameter `TrustRequestsSentToTheXmlServicePort` auf "False"festgelegt. Wenn der Kunde Citrix ADC jedoch bereits für Citrix Virtual Desktops konfiguriert hat, ist `TrustRequestsSentToTheXmlServicePort` auf "True"festgelegt.

1. Gehen Sie in Citrix ADC zu **Configuration > Integrate with Citrix Products** und klicken Sie auf **XenApp and XenDesktop**.
2. Wählen Sie die Gateway-Instanz aus und klicken Sie auf das Bearbeitungssymbol

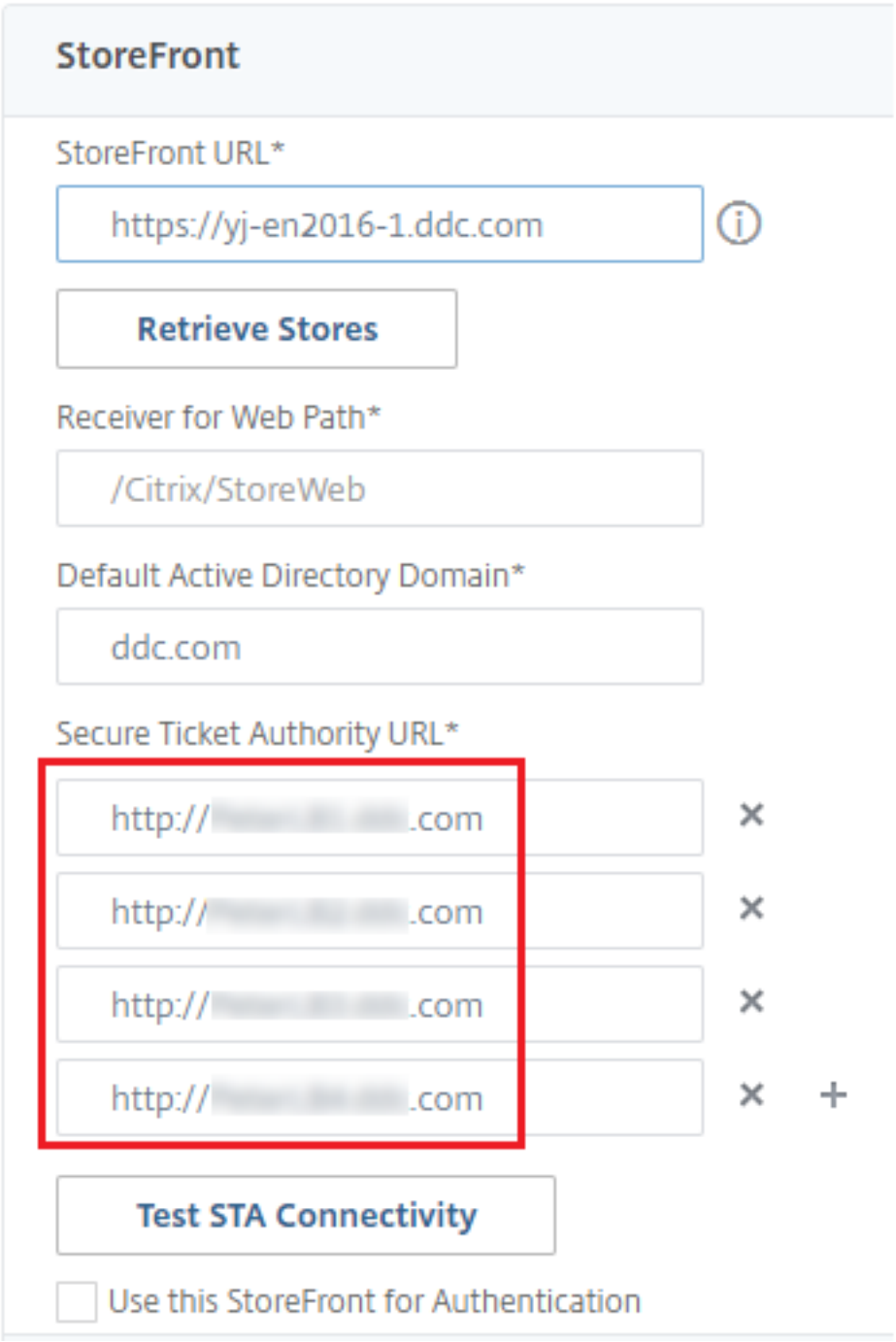


3. Klicken Sie im StoreFront-Bereich auf das Bearbeitungssymbol.



4. Fügen Sie die **Secure Ticket Authority-URL**hinzu.

   - Wenn Secure XML aktiviert ist, muss die STA-URL die URL des Lastausgleichsdiensts sein.
   - Wenn Secure XML deaktiviert ist, muss die STA-URL die URL der STA (Adresse des DDC) sein und der Parameter "TrustRequestsSentToTheXmlServicePort"des DDC muss auf "True"festgelegt sein.



Verbindungsleasing

August 18, 2021

> **Wichtig:**
>
> Der lokale Hostcache (LHC) wird bei XenApp und XenDesktop als Lösung für hohe Verfügbarkeit dem Verbindungsleasing gegenüber bevorzugt. Weitere Informationen finden Sie unter Lokaler Hostcache.

- Bei einer Neuinstallation dieser Version von XenApp und XenDesktop ist das Verbindungsleasing standardmäßig deaktiviert.
- Verbindungsleasing wird ab dem aktuellen Release nach XenApp- und XenDesktop 7.15 Long Term Service Release nicht mehr bereitgestellt.

Um sicherzustellen, dass die Sitedatenbank immer verfügbar ist, empfiehlt Citrix, unter Befolgung der bewährten Methoden zur hohen Verfügbarkeit von Microsoft mit einer fehlertoleranten SQL Server-Bereitstellung zu beginnen. Delivery Controller können jedoch aufgrund von Netzwerkproblemen und Unterbrechungen möglicherweise nicht auf die Datenbank zugreifen, was dazu führt, dass Benutzer keine Verbindung mit ihren Anwendungen oder Desktops herstellen können.

Das Feature für Verbindungsleasing ergänzt die bewährten Methoden zur hohen Verfügbarkeit bei SQL Server, da es Benutzern die Wiederverbindung mit den zuletzt verwendeten Anwendungen und Desktops ermöglicht, selbst wenn die Sitedatenbank nicht verfügbar ist.

Benutzer verfügen zwar über eine große Anzahl veröffentlichter Ressourcen, verwenden jedoch oft nur wenige davon regelmäßig. Wenn Sie das Verbindungsleasing aktivieren, werden die Benutzerverbindungen mit den zuletzt verwendeten Anwendungen und Desktops im Normalbetrieb (wenn die Datenbank verfügbar ist) von jedem Controller zwischengespeichert.

Die auf jedem Controller generierten Leases werden in die Sitedatenbank für eine regelmäßige Synchronisierung mit den anderen Controllern der Site hochgeladen. Neben den Leases werden in jedem Controllercache Informationen zu Anwendung, Desktop, Symbol und Worker gespeichert. Lease und zugehörige Informationen werden auf dem lokalen Datenträger eines jeden Controllers gespeichert. Wenn die Datenbank nicht mehr verfügbar ist, wechselt der Controller in den Leasingverbindungsmodus und beim Versuch der Herstellung oder des Neuaufbaus einer Verbindung mit einer kürzlich verwendeten Anwendung oder einem kürzlich verwendeten Desktop von StoreFront aus werden die zwischengespeicherten Vorgänge "abgespielt".

Die Verbindungen werden für eine Leasedauer von zwei Wochen zwischengespeichert. Wenn die Datenbank nicht verfügbar ist, besteht daher über StoreFront Zugriff auf die Desktops und Anwendungen, die in den vorherigen zwei Wochen gestartet wurden. Auf Desktops und Anwendungen, die nicht während der zweiwöchigen Leasedauer gestartet wurden, kann jedoch nicht zugegriffen werden, wenn die Datenbank nicht verfügbar ist. Wenn eine Anwendung z. B. vor drei Wochen gestartet wurde, ist ihre Lease abgelaufen und sie kann bei Nichtverfügbarkeit der Datenbank nicht gestartet werden. Leases für langwährende aktive oder getrennte Anwendungs- oder Desktopsitzungen werden verlängert und somit nicht als abgelaufen behandelt.

Standardmäßig gilt das Verbindungsleasing für die komplette Site. Sie können jedoch alle Leases für bestimmte Benutzer widerrufen, wodurch verhindert wird, dass diese auf Anwendungen oder Desktops zugreifen können, wenn der Controller im Leasingverbindungsmodus ausgeführt wird. Mehrere weitere Registrierungseinstellungen gelten pro Controller.

Überlegungen und Einschränkungen

Das Verbindungsleasing kann zwar die Verbindungsresilienz und die Produktivität der Benutzer verbessern, es sind jedoch Überlegungen im Hinblick auf Verfügbarkeit, Betrieb und Leistung anderer Funktionen anzustellen.

Das Verbindungsleasing wird für servergehostete Anwendungen und Desktops und statische (zugewiesene) Desktops unterstützt. Es wird nicht unterstützt für gepoolte VDI-Desktops oder Benutzer, denen kein Desktop zugewiesen wurde, wenn die Datenbank betriebsunfähig wird.

Wenn der Controller im Leasingverbindungsmodus ist, gilt Folgendes:

- Administratoren können Studio, Director und die PowerShell-Konsole nicht verwenden.
- Workspace Control ist nicht verfügbar. Wenn sich ein Benutzer bei Citrix Receiver anmeldet, werden Sitzungen nicht automatisch wieder verbunden. Der Benutzer muss die Anwendung neu starten.
- Wenn eine neue Lease unmittelbar vor dem Nichtverfügbarwerden der Datenbank erstellt wurde, die Leaseinformationen jedoch noch nicht auf allen Controllern synchronisiert wurden, können Benutzer möglicherweise eine betroffene Ressource nicht starten.
- Benutzer servergehosteter Anwendungen und Desktops können möglicherweise mehr Sitzungen verwenden als das für sie konfigurierte Sitzungslimit zulässt. Beispiel:
  - Ein Benutzer stellt eine Verbindung von einem Gerät (extern über NetScaler Gateway) her, während der Controller im normalen Verbindungsmodus ist. Später stellt der Benutzer von einem anderen Gerät im LAN eine Verbindung her, während Controller im Leasingverbindungsmodus ist. In diesem Fall findet möglicherweise kein Roaming der Sitzung statt.
  - Die Wiederverbindung einer Sitzung kann fehlschlagen, wenn eine Anwendung startet, kurz bevor die Datenbank betriebsunfähig wird. In diesem Fall werden eine neue Sitzung und Anwendungsinstanz gestartet.
- Bei statischen (zugewiesenen) Desktops findet keine Energieverwaltung statt. VDAs, die beim Umschalten des Controllers in den Leasingverbindungsmodus ausgeschaltet werden, stehen erst wieder zur Verfügung, wenn die Datenbankverbindung wiederhergestellt ist, es sei denn, der Administrator schaltet sie manuell ein.

- Sind Sitzungsvorabstart und Sitzungsfortbestehen aktiviert, werden neue Vorabstartsitzungen nicht gestartet. Vorab gestartete und fortbestehende Sitzungen werden während der Nichtverfügbarkeit der Datenbank nicht entsprechend den konfigurierten Schwellenwerten beendet.
- Die Lastverwaltung der Site kann beeinträchtigt werden. Serverbasierte Verbindungen werden an den zuletzt verwendeten VDA geleitet. Lastauswertungsprogramme (und insbesondere Sitzungszahlregeln) werden möglicherweise überschritten.
- Der Controller wechselt nicht in den Leasingverbindungsmodus, wenn Sie die Datenbank mit SQL Server Management Studio offline nehmen. Verwenden Sie stattdessen eine der folgenden Transact-SQL-Anweisungen:
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK AFTER <seconds>

  Beide Anweisungen beenden ausstehende Transaktionen und trennen die Verbindung des Controllers mit der Datenbank. Der Controller wechselt dann in den Leasingverbindungsmodus.

Beim Verbindungsleasing gibt es zwei kurze Intervalle, während derer Benutzer keine Verbindung (wieder)herstellen können: (1) zwischen dem Zeitpunkt, zu dem die Datenbank betriebsunfähig wird bis zum Umschalten des Controllers in den Leasingverbindungsmodus und (2) vom Zeitpunkt des Umschaltens des Controllers vom Leasingverbindungsmodus bis der Datenbankzugriff vollständig wiederhergestellt ist und die VDAs erneut registriert sind.

Wenn Sie einen nicht standardmäßigen Wert für das Sitzungsroaming festlegen und ein Controller auf eine geleaste Verbindung schaltet, tritt bei Sitzungswiederverbindung wieder der Standardwert in Kraft. Weitere Informationen finden Sie unter Verbindungsleasing und Sitzungsroaming.

Informationen zum Speicherort der Verbindungsleasingdaten finden Sie in dem Artikel Zonen.

Konfigurieren und Bereitstellen

Beim Konfigurieren der Bereitstellung zum Ermöglichen des Verbindungsleasings ist Folgendes zu beachten:

- VDAs müssen mindestens in Version 7.6 und die Maschinenkataloge und Bereitstellungsgruppen, die diese Maschinen verwenden, müssen in der entsprechenden Mindestversion vorliegen.
- Die Speicherplatzanforderungen der Sitedatenbank sind größer.
- Jeder Controller erfordert zusätzlichen Speicherplatz für die zwischengespeicherten Leasedateien.

Sie können das Verbindungsleasing im PowerShell-SDK oder in der Windows-Registrierung deaktivieren und aktivieren. Im PowerShell-SDK können Sie auch aktuelle Leases entfernen. Die folgenden PowerShell-Cmdlets wirken sich auf das Verbindungsleasing aus. Informationen hierzu finden Sie in der Cmdlet-Hilfe.

- Set-BrokerSite -ConnectionLeasingEnabled $true|$false:| aktiviert bzw. deaktiviert das Verbindungsleasing. Standard = $true
- Get-BrokerServiceAddedCapability: Gibt "ConnectionLeasing"für den lokalen Controller aus.
- Get-BrokerLease: Ruft alle Leases oder einen gefilterten Satz aktueller Leases auf.
- Remove-BrokerLease: Markiert alle Leases oder einen gefilterten Satz Leases zum Löschen.
- Update-BrokerLocalLeaseCache: aktualisiert den Cache für das Verbindungsleasing auf dem lokalen Controller. Bei der nächsten Synchronisierung werden die Daten neu synchronisiert.

Virtuelle IP und virtuelles Loopback

August 18, 2021

Hinweis: Diese Features gelten nur für Windows-Serverbetriebssystemmaschinen. Sie gelten nicht für Windows-Desktopbetriebssystemmaschinen.

Die Microsoft virtuelle IP-Adresse stellt einer veröffentlichten Anwendung eine eindeutige dynamisch zugeordnete IP-Adresse für jede Sitzung bereit. Mit dem Citrix Feature des virtuellen Loopbacks können Sie Anwendungen, die mit dem lokalen Host (localhost) kommunizieren (normalerweise 127.0.0.1), so konfigurieren, dass sie eine eindeutige virtuelle Loopbackadresse im Bereich des lokalen Hosts verwenden (127.*).

Einige Anwendungen, z. B. CRM oder CTI, verwenden eine IP-Adresse für die Adressierung, Lizenzierung, Identifizierung und andere Zwecke und erfordern daher eine eindeutige IP-Adresse oder eine Loopbackadresse in Sitzungen. Andere Anwendungen binden sich möglicherweise an einen statischen Port an, sodass das Starten weitere Instanzen einer Anwendung in Mehrbenutzerumgebungen fehlschlägt, da der Port bereits verwendet wird. Damit solche Anwendungen in einer XenApp-Umgebung richtig ausgeführt werden können, benötigen Sie für jedes Gerät eine eindeutige IP-Adresse.

Virtuelle IP-Adressen und virtuelles Loopback sind unabhängige Features. Sie können ein Feature oder beide wählen.

Zusammenfassung der Administratoraktion:

- Zur Verwendung von Microsoft virtuellen IPs aktivieren und konfigurieren Sie die Funktion auf dem Windows-Server. (Citrix-Richtlinieneinstellungen sind nicht erforderlich.)
- Für die Verwendung von virtuellem Loopback von Citrix konfigurieren Sie zwei Einstellungen in einer Citrix Richtlinie.

Virtuelle IP

Wenn die virtuelle IP aktiviert und auf dem Windows-Server konfiguriert ist, scheint jede konfigurierte Anwendung, die in einer Sitzung ausgeführt wird, eine eindeutige Adresse zu haben. Benutzer greifen auf diese Anwendungen auf einem XenApp-Server genauso wie auf andere veröffentlichte Anwendungen zu. Ein Prozess erfordert die virtuelle IP in den folgenden Fällen:

- Der Prozess verwendet eine hartcodierte TCP-Portnummer
- Der Prozess verwendet Windows Sockets und benötigt eine eindeutige IP-Adresse oder eine angegebene TCP-Portnummer

Ermitteln, ob eine Anwendung virtuelle IP-Adressen verwenden muss

1. Beziehen Sie das TCPView-Tool von Microsoft. Das Programm zeigt alle Anwendungen an, die an spezifische IP-Adressen und Ports binden.
2. Deaktivieren Sie das Auflösen von IP-Adressen, sodass statt der Adressen die Hostnamen angezeigt werden.
3. Starten Sie die Anwendung und ermitteln Sie mit TCPView, welche IP-Adressen und Ports von der Anwendung geöffnet werden und welche Prozesse diese Ports öffnen.
4. Konfigurieren Sie alle Prozesse, die die IP-Adresse des Servers, 0.0.0.0 oder 127.0.0.1, öffnen.
5. Starten Sie eine zusätzliche Instanz der Anwendung, um sicherzustellen, dass sie nicht dieselbe IP-Adresse auf einem anderen Port öffnet.

Funktionsweise der IP-Virtualisierung von Microsoft-Remotedesktop

- Die virtuelle IP-Adressierung muss auf dem Microsoft Server aktiviert sein.

  Beispiel: In einer Umgebung mit Windows Server 2008 R2 erweitern Sie im Server-Manager "Remotedesktopdienste > Remotedesktop-Sitzungshostverbindungen", um das Remotedesktop-IP-Virtualisierungsfeature zu aktivieren, und konfigurieren Sie die Einstellungen so, dass IP-Adressen dynamisch mit dem DHCP-Server pro Sitzung oder pro Programm zugewiesen werden. Weitere Informationen finden Sie in der Microsoft Dokumentation.

- Nach der Aktivierung des Features fordert der Server beim Sitzungsstart dynamisch zugewiesene IP-Adressen vom DHCP-Server an.
- Das Remotedesktop-IP-Virtualisierungsfeature weist den Remotedesktopverbindungen die IP-Adressen pro Sitzung oder pro Programm zu. Wenn Sie IP-Adressen für mehrere Programme zuweisen, verwenden sie eine gemeine IP-Adresse pro Sitzung.
- Wenn einer Sitzung eine Adresse zugewiesen wurde, verwendet die Sitzung die virtuelle Adresse statt der primären IP-Adresse des Systems bei den folgenden Aufrufen: Bind, Closesocket, Connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

Wenn das IP-Virtualisierungsfeature von Microsoft in der Hostingkonfiguration der Remotedesktopsitzung verwendet wird, sind Anwendungen an bestimmte IP-Adressen gebunden, indem eine Filterkomponente zwischen die Anwendung und den Winsock-Funktionsaufrufen eingefügt wird. Die Anwendung erkennt dann nur die IP-Adresse, die sie verwenden soll. Sollte die Anwendung versuchen, TCP- oder UDP-Kommunikation abzuhören, wird sie automatisch an die zugewiesene virtuelle IP-Adresse (oder Loopbackadresse) gebunden und alle von der Anwendung geöffneten Ausgangsverbindungen gehen von der an die Anwendung gebundene IP-Adresse aus.

In Funktionen, die eine Adresse ausgeben, wie z. B. GetAddrInfo() (über eine Windows–Richtlinie gesteuert), untersucht die virtuelle IP beim Abrufen der IP-Adresse des lokalen Hosts die zurückgegebene IP-Adresse und ändert sie in die virtuelle IP-Adresse der Sitzung. Anwendungen, die mit solchen Namensfunktionen versuchen, die IP-Adresse des lokalen Servers zu ermitteln, erhalten nur die eindeutige virtuelle IP-Adresse, die der Sitzung zugeordnet wurde. Diese IP-Adresse wird oft in späteren Socket-Aufrufen, wie “Bind”oder “Connect”, verwendet.

Oft fordern Anwendungen eine Bindung an einen Port zum Abhören der Adresse 0.0.0.0. Wenn eine Anwendung dies versucht und einen statischen Port verwendet, können Sie höchstens eine Instanz der Anwendung starten. Das virtuelle IP-Adressfeature sucht in diesen Aufrufen nach 0.0.0.0 und ändert den Abruf so, dass die angegebene virtuelle IP-Adresse abgehört wird. Dies ermöglicht, dass mehrere Anwendungen denselben Port auf demselben Computer abhören, da sie auf verschiedenen Adressen abhören. Der Aufruf wird nur geändert, wenn er in einer ICA-Sitzungen erfolgt und virtuelle IP-Adressen aktiviert sind. Beispiel: Wenn zwei Instanzen einer Anwendung, die in unterschiedlichen Sitzungen ausgeführt werden, eine Bindung mit allen Schnittstellen (0.0.0.0) und einen bestimmten Port (z. B. 9000) versuchen, werden sie an VIPAddress1:9000 und VIPAddress2:9000 gebunden und es gibt keinen Konflikt.

Virtuelles Loopback

Bei Aktivierung der Citrix Richtlinieneinstellungen für virtuelles Loopback kann jede Sitzung eine eigene Loopbackadresse für die Kommunikation haben. Wenn eine Anwendung die localhost-Adresse (Standard = 127.0.0.1) in einem Winsock-Aufruf verwendet, ersetzt das virtuelle Loopback einfach 127.0.0.1 durch 127.X.X.X, wobei X.X.X für die Sitzungs-ID + 1 steht. Wenn die Sitzungs-ID zum Beispiel 7 ist, ist die Adresse 127.0.0.8. Im unwahrscheinlichen Fall, dass die Sitzungs-ID größer ist, als im vierten Oktett zulässig (mehr als 255), wird beim nächsten Oktett weitergemacht (127.0.1.0) bis zum Maximum von 127.255.255.255.

Ein Prozess erfordert das virtuelle Loopback in den folgenden Fällen:

- Der Prozess verwendet die Windows- Sockets-Loopbackadresse (localhost) (127.0.0.1)
- Der Prozess verwendet eine hartcodierte TCP-Portnummer

Verwenden Sie die Richtlinieneinstellungen für virtuelles Loopback für Anwendungen, die eine Loopbackadresse für prozessübergreifende Kommunikation verwenden. Eine zusätzliche Konfiguration

ist nicht erforderlich. Virtuelles Loopback ist nicht von virtueller IP abhängig, sodass der Microsoft-Server nicht konfiguriert werden muss.

- Virtuelle IP - Loopbackunterstützung: Wenn diese Richtlinieneinstellung aktiviert ist, kann jede Sitzung eine eigene virtuelle Loopbackadresse haben. Diese Einstellung ist standardmäßig aktiviert. Das Feature gilt nur für Anwendungen, die mit der Richtlinieneinstellung Virtuelle IP - Programme für virtuelles Loopback angegeben wurden.
- Virtuelle IP - Programme für virtuelles Loopback: Mit dieser Richtlinieneinstellung geben Sie die Anwendung an, die das Feature "Virtuelles IP-Loopback"verwenden. Diese Einstellung gilt nur, wenn die Richtlinieneinstellung Virtuelle IP - Loopbackunterstützung aktiviert ist.

Verwandtes Feature

Mit den folgenden Registrierungseinstellungen stellen Sie sicher, dass virtuelles Loopback den Vorrang vor virtuelle IP erhält; dies wird als bevorzugtes Loopback bezeichnet. Achten Sie jedoch auf Folgendes:

- Bevorzugtes Loopback wird nur unter Windows 2008 R2 and Windows Server 2012 R2 unterstützt.
- Verwenden Sie bevorzugtes Loopback nur, wenn virtuellen IP-Adressen und das virtuelle Loopback aktiviert sind, sonst erhalten Sie u. U. unerwartete Ergebnisse.
- Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Führen Sie regedit auf den Servern aus, auf dem die Anwendungen installiert sind.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\V
für 32-Bit-Maschinen)
- Name: PreferLoopback, Typ: REG_DWORD, Wert: 1
- Name: PreferLoopbackProcesses, Type: REG_MULTI_SZ, Data: <Liste der Prozesse>

Delivery Controller

July 11, 2022

Der Delivery Controller ist die serverseitige Komponente, die für die Verwaltung des Benutzerzugriffs sowie das Brokering und Optimieren von Verbindungen zuständig ist. Controller stellen auch die Maschinenerstellungsdienste zur Erstellung von Desktop- und Serverimages bereit.

Eine Site muss mindestens über einen Controller verfügen. Nach der Installation des ersten Controllers können Sie im Rahmen der Siteerstellung oder auch später weitere Controller hinzufügen. Es gibt zwei Hauptvorteile, mehr als einen Controller in einer Site zu haben.

- Redundanz: Als bewährte Methode sollte eine Produktionssite immer mindestens zwei Controller auf unterschiedlichen physischen Servern haben. Wenn ein Controller ausfällt, können die anderen die Verwaltung der Verbindungen und der Site übernehmen.
- Skalierbarkeit: Je intensiver die Aktivität einer Site, umso mehr nehmen CPU-Auslastung auf dem Controller und die Datenbankaktivität zu. Zusätzliche Controller bieten die Möglichkeit, mehr Benutzer, Anwendungen und Desktopanforderungen zu verarbeiten und die Reaktionszeit insgesamt zu verbessern.

Jeder Controller kommuniziert direkt mit der Sitedatenbank. In einer Site mit mehreren Zonen kommunizieren die Controller in jeder Zone mit der Datenbank in der primären Zone.

> **Wichtig:**
>
> Ändern Sie weder den Computernamen noch die Domänenmitgliedschaft eines Controllers, nachdem Sie die Site konfiguriert haben.

Verfahren der Registrierung von VDAs bei Controllern

VDAs können erst verwendet werden, wenn sie bei einem Delivery Controller in der Site registriert wurden (Herstellen der Kommunikation). Weitere Informationen zur VDA-Registrierung finden Sie unter VDA-Registrierung bei Controllern.

(In der Dokumentation zu älteren Releases von XenApp und XenDesktop 7.x waren die Informationen zur VDA-Registrierung im vorliegenden Artikel enthalten. Diese Informationen wurden erweitert und befinden sich nun in dem oben verlinkten Artikel.)

Hinzufügen, Entfernen oder Verschieben von Controllern

Um einen Controller hinzuzufügen, zu entfernen oder zu verschieben, benötigen Sie die unter Datenbanken aufgeführten Serverrollen- und Datenbankrollenberechtigungen.

> **Hinweis:**
>
> Die Installation eines Controllers auf einem Knoten in einer SQL-Clustering- oder SQL-Spiegelungsinstallation wird nicht unterstützt.

Wenn in der Bereitstellung Datenbankspiegelung verwendet wird, gilt Folgendes:

- Vor dem Hinzufügen, Entfernen oder Verschieben von Controllern müssen Sie sicherstellen, dass sowohl die gespiegelte als auch die Hauptdatenbank ausgeführt werden. Wenn Sie mit Skripts für SQL Server Management Studio arbeiten, müssen Sie den SQLCMD-Modus vor dem Ausführen des Skripts aktivieren.
- Zum Prüfen der Spiegelung nach dem Hinzufügen, Entfernen oder Verschieben des Controllers führen Sie das PowerShell-Cmdlet **get-configdbconnection** aus, um sicherzustellen, dass der Failoverpartner in der Verbindungszeichenfolge für die Spiegelung eingerichtet wurde.

Gehen Sie nach dem Hinzufügen, Entfernen oder Verschieben eines Controllers wie folgt vor:

- Wenn das automatische Update aktiviert ist, erhalten die VDAs eine aktualisierte Liste der Controller innerhalb von 90 Minuten.
- Ist das automatische Update nicht aktiviert, müssen Sie sicherstellen, dass die Controllerrichtlinieneinstellung oder der Registrierungsschlüssel "ListOfDDCs"für alle VDAs aktualisiert wird. Nachdem Sie einen Controller in eine andere Site verschoben haben, müssen Sie die Richtlinieneinstellung oder den Registrierungsschlüssel in beiden Sites aktualisieren.

Hinzufügen eines Controllers

Sie können Controller bei der Siteerstellung oder zu einem späteren Zeitpunkt hinzufügen. Sie können einer Site, die mit dieser Softwareversion erstellt wurde, keine Controller hinzufügen, die mit einer früheren Version installiert wurden.

1. Führen Sie das Installationsprogramm auf einem Server mit einem unterstützten Betriebssystem aus. Installieren Sie den Delivery Controller und alle anderen gewünschten Kernkomponenten. Führen Sie die Schritte des Installationsassistenten durch.
2. Wenn Sie noch keine Site erstellt haben, starten Sie Studio; Sie werden aufgefordert, eine Site zu erstellen. Klicken Sie auf der Seite "Datenbanken"im Assistenten für die Siteerstellung auf die Schaltfläche "Auswählen"und geben Sie die Adresse des Servers ein, auf dem Sie den zusätzlichen Controller installiert haben. **Wichtig:** Wenn Sie Skripts für die Initialisierung der Datenbanken generieren möchten, fügen Sie die Controller vor dem Generieren der Skripts hinzu.
3. Wenn Sie bereits eine Site erstellt haben, verweisen Sie Studio auf den Server, auf dem Sie den zusätzlichen Controller installiert haben. Klicken Sie auf **Bereitstellung erweitern** und geben Sie die Siteadresse ein.

Entfernen eines Controllers

Beim Entfernen eines Controllers aus einer Site werden die Citrix Software und andere Komponenten nicht deinstalliert. Es wird lediglich der Controller aus der Datenbank entfernt, der damit für das

Brokering von Verbindungen oder sonstige Aufgaben nicht mehr verfügbar ist. Wenn Sie einen Controller entfernen, können Sie diesen zu einem späteren Zeitpunkt der gleichen oder einer anderen Site wieder hinzufügen. Eine Site benötigt mindestens einen Controller. Aus diesem Grund können Sie den letzten in Studio aufgelisteten Controller nicht entfernen.

Wenn Sie einen Controller von einer Site entfernen, wird die Controller-Anmeldung für den Datenbankserver nicht entfernt. Auf diese Weise wird vermieden, dass eine Anmeldung entfernt wird, die von den Diensten anderer Produkte auf demselben Computer verwendet wird. Die Anmeldung muss manuell entfernt werden, wenn sie nicht mehr erforderlich ist. Dazu benötigen Sie die Berechtigungen der securityadmin-Serverrolle.

> **Wichtig:**
>
> Entfernen Sie den Controller erst dann aus Active Directory, wenn Sie ihn aus der Site entfernt haben.

1. Stellen Sie sicher, dass der Controller eingeschaltet ist, sodass Studio in weniger als einer Stunde geladen wird. Wenn Studio den Controller lädt, den Sie entfernen möchten, schalten Sie den Controller aus, wenn Sie dazu aufgefordert werden.
2. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Controller** und anschließend den Controller, den Sie entfernen möchten.
3. Wählen Sie im Aktionsbereich **Controller entfernen**. Wenn Sie nicht über die erforderlichen Datenbankrollen und Berechtigungen verfügen, können Sie ein Skript erstellen, mit dem der Datenbankadministrator den Controller für Sie entfernen kann.
4. Möglicherweise müssen Sie das Maschinenkonto des Controllers auf dem Datenbankserver entfernen. Bevor Sie dies durchführen, überprüfen Sie, ob das Konto von einem anderen Dienst verwendet wird.

Nachdem Sie mit Studio einen Controller entfernt haben, besteht ggf. kurze Zeit weiter Datenverkehr zu diesem Controller, um sicherzustellen, dass die aktuellen Tasks einwandfrei abgeschlossen werden. Wenn Sie das Entfernen eines Controllers in sehr kurzer Zeit erzwingen möchten, empfiehlt Citrix, den Server, auf dem er installiert war, herunterzufahren oder aus Active Directory zu entfernen. Starten Sie dann die anderen Controller in der Site neu, um sicherzustellen, dass keine weitere Kommunikation mit dem entfernten Controller stattfindet.

Verschieben eines Controllers in eine andere Zone

Wenn die Site mehrere Zonen enthält, können Sie Controller in eine andere Zone verschieben. Unter *Zonen* finden Sie Informationen darüber, wie sich dies auf die VDA-Registrierung und andere Vorgänge auswirken kann.

1. Wählen Sie im Studio-Navigationsbereich **Konfiguration > Controller** und anschließend den Controller, den Sie verschieben möchten.

2. Wählen Sie im Aktionsbereich **Verschieben**.
3. Geben Sie die Zone an, in die Sie den Controller verschieben möchten.

Verschieben eines Controllers in eine andere Site

Controller können nicht in eine Site verschoben werden, die mit einer früheren Version dieser Software erstellt wurde.

1. Wählen Sie in der derzeitigen Site des Controllers (der alten Site) im Studio-Navigationsbereich **Konfiguration > Controller** und wählen Sie anschließend den Controller, den Sie verschieben möchten.
2. Wählen Sie im Aktionsbereich **Controller entfernen**. Wenn Sie nicht über die erforderlichen Datenbankrollen und Berechtigungen verfügen, können Sie ein Skript erstellen, mit dem eine Person mit den entsprechenden Berechtigungen, (z. B. der Datenbankadministrator) den Controller für Sie entfernen kann. Eine Site benötigt mindestens einen Controller. Aus diesem Grund können Sie den letzten in Studio aufgelisteten Controller nicht entfernen.
3. Öffnen Sie Studio auf dem zu verschiebenden Controller, setzen Sie bei entsprechender Aufforderung die Dienste zurück, wählen Sie **Vorhandener Site beitreten** und geben Sie die Adresse der neuen Site ein.

Verschieben eines VDAs in eine andere Site

Wenn ein VDA mit Provisioning Services bereitgestellt wurde oder wenn er ein vorhandenes Image ist, können Sie einen VDA in eine andere Site (von Site 1 nach Site 2) verschieben, wenn Sie ein Upgrade vornehmen oder wenn Sie ein in einer Testsite erstelltes VDA-Image in eine Produktionssite verschieben. Mit Maschinenerstellungsdienste (MCS) bereitgestellte VDAs können nicht zwischen Sites verschoben werden, da MCS das Ändern der ListOfDDCs nicht unterstützt, die ein VDA zum Registrieren mit einem Controller prüft. Mit Maschinenerstellungsdienste bereitgestellte VDAs prüfen immer die ListOfDDCs, die der Site zugeordnet ist, in der sie erstellt wurden.

Es gibt zwei Möglichkeiten, einen VDA in eine andere Site zu verschieben: mit dem Installationsprogramm oder mit Citrix Richtlinien.

Installationsprogramm: Führen Sie das Installationsprogramm aus und fügen Sie einen Controller hinzu, wobei Sie in Site 2 einen vollqualifizierten Domänennamen (DNS-Eintrag) eines Controllers angeben. **Wichtig:** Geben Sie Controller im Installationsprogramm nur dann an, wenn die Richtlinieneinstellung "Controller"nicht verwendet wird.

Gruppenrichtlinienobjekt-Editor: Im folgenden Beispiel werden mehrere VDAs verschoben.

1. Erstellen Sie eine Richtlinie in Site 1 mit den nachfolgenden Einstellungen und filtern Sie die Richtlinie auf Bereitstellungsgruppenebene, um eine mehrstufige VDA-Migration zwischen den

Sites zu erzielen.
Controller: mit vollqualifizierten Domänennamen (DNS-Einträgen) von einem oder mehreren Controllern der Site 2.
Automatische Controllerupdates aktivieren: auf "Deaktiviert"gesetzt.

2. Jeder VDA in der Bereitstellungsgruppe wird innerhalb von 90 Minuten auf die neue Richtlinie hingewiesen. Der VDA ignoriert die eingegangene Liste der Controller (da automatische Updates deaktiviert sind) und wählt einen der in der Richtlinie angegebenen Controller, d. h. einen der Controller in Site 2.
3. Wenn der VDA erfolgreich bei einem Controller der Site 2 registriert wurde, empfängt er die Liste "ListOfDDCs"und die Richtlinieninformationen von Site 2, für die automatische Updates standardmäßig aktiviert sind. Da der Controller, bei dem der VDA in Site 1 registriert war, nicht in der vom Controller in Site 2 gesendeten Liste ist, erfolgt eine erneute Registrierung des VDAs unter Auswahl eines Controllers der Liste von Site 2. Ab sofort wird der VDA automatisch mit Informationen von Site 2 aktualisiert.

Informationen zum Verwenden des Gruppenrichtlinien-Editors finden Sie unter Citrix Richtlinien.

VDA-Registrierung

August 18, 2021

Einführung

VDAs können erst verwendet werden, wenn sie bei mindestens einem Controller oder einem Cloud Connector der Site registriert wurden (Herstellen der Kommunikation). (In on-premises XenApp und XenDesktop-Bereitstellungen werden VDAs bei einem Controller registriert. In XenApp und XenDesktop Service-Bereitstellungen werden VDAs bei Cloud Connectors registriert.) Der VDA findet den Controller bzw. Connector anhand der Liste "ListofDDCs". Die Liste "ListOfDDCs"auf einem VDA enthält DNS-Einträge, die den VDA an die Controller bzw. Cloud Connectors der Site verweisen. Um einen Lastausgleich zu erzielen, verteilt der VDA die Verbindungen automatisch über alle Controller bzw. Cloud Connectors in der Liste.

Warum ist die VDA-Registrierung so wichtig?

- Bei der Registrierung spielt die Sicherheit eine große Rolle, denn es wird eine Verbindung zwischen Controller bzw. Cloud Connector und VDA hergestellt. Bei einem solchen Vorgang wird eine Abweisung erwartet, wenn bei der Anforderungen nicht alles einwandfrei ist. Es werden zwei separate Kommunikationskanäle eingerichtet: VDA an Controller bzw. Cloud Connector und Controller bzw. Cloud Connector an VDA. Bei der Verbindung wird Kerberos verwendet.

Daher darf es keine Probleme bei der Zeitsynchronisation und Domänenmitgliedschaft geben. Kerberos verwendet Dienstprinzipalnamen (SPN), d. h. Sie können keine per Lastausgleich gewählten IP-\Hostnamen verwenden.

- Wenn Sie Controller bzw. Cloud Connectors zur Site hinzufügen und entfernen und ein VDA keine präzisen und aktuellen Controller-/Connectorinformationen hat, kann er Sitzungsstarts ablehnen, die von einem nicht aufgelisteten Controller bzw. Cloud Connector vermittelt wurden. Ungültige Einträge in der Liste können den Start der Systemsoftware des virtuellen Desktops verzögern. VDAs akzeptieren keine Verbindung von einem unbekannten, nicht vertrauenswürdigen Controller bzw. Cloud Connector.

Die Liste ListOfSIDs (Sicherheits-IDs) enthält die Maschinen auf der Liste ListOfDDCs, denen vertraut wird. Die Liste "ListOfSIDs"kann verwendet werden, um die Last auf Active Directory zu verringern oder um Sicherheitsbedrohungen durch einen nicht sicheren DNS-Server zu vermeiden. Weitere Informationen finden Sie unter ListOfSIDs.

Wenn in ListOfDDCs mehrere Controller bzw. Cloud Connectors angegeben sind, erfolgt die Verbindung mit ihnen durch den VDA in einer zufälligen Reihenfolge. Die Liste "ListOfDDCs"kann auch Controller-/Connectorgruppen enthalten. Der VDA versucht, eine Verbindung mit jedem Controller in einer Gruppe herzustellen, bevor er weitere Einträge in der Liste "ListOfDDCs"versucht.

In XenApp und XenDesktop wird bei der VDA-Installation automatisch die Verbindung mit konfigurierten Controllern bzw. Cloud Connectors überprüft. Wenn ein Controller bzw. Cloud Connector nicht erreicht werden kann, wird ein Fehler angezeigt. Wenn Sie eine Warnung über einen nicht erreichbaren Controller oder Cloud Connector ignorieren (oder wenn Sie während der VDA-Installation keine Adressen angeben), werden Sie durch Meldungen erinnert.

Methoden zum Konfigurieren von Controller-/Cloud Connector-Adressen

Der Administrator wählt die gewünschte Konfigurationsmethode bei der ersten Registrierung des VDAs. Bei dieser Erstregistrierung wird ein persistenter Cache auf dem VDA erstellt. Bei anschließenden Registrierungen ruft der VDA die Liste der Controller bzw. Cloud Connectors aus diesem lokalen Cache ab, es sei denn, es wird eine Konfigurationsänderung erkannt.

Die einfachste Methode des Abrufs dieser Liste bei späteren Registrierungen ist die Verwendung des Features zur automatischen Aktualisierung. Die automatische Aktualisierung ist standardmäßig aktiviert. Weitere Informationen finden Sie unter "Automatische Aktualisierung".

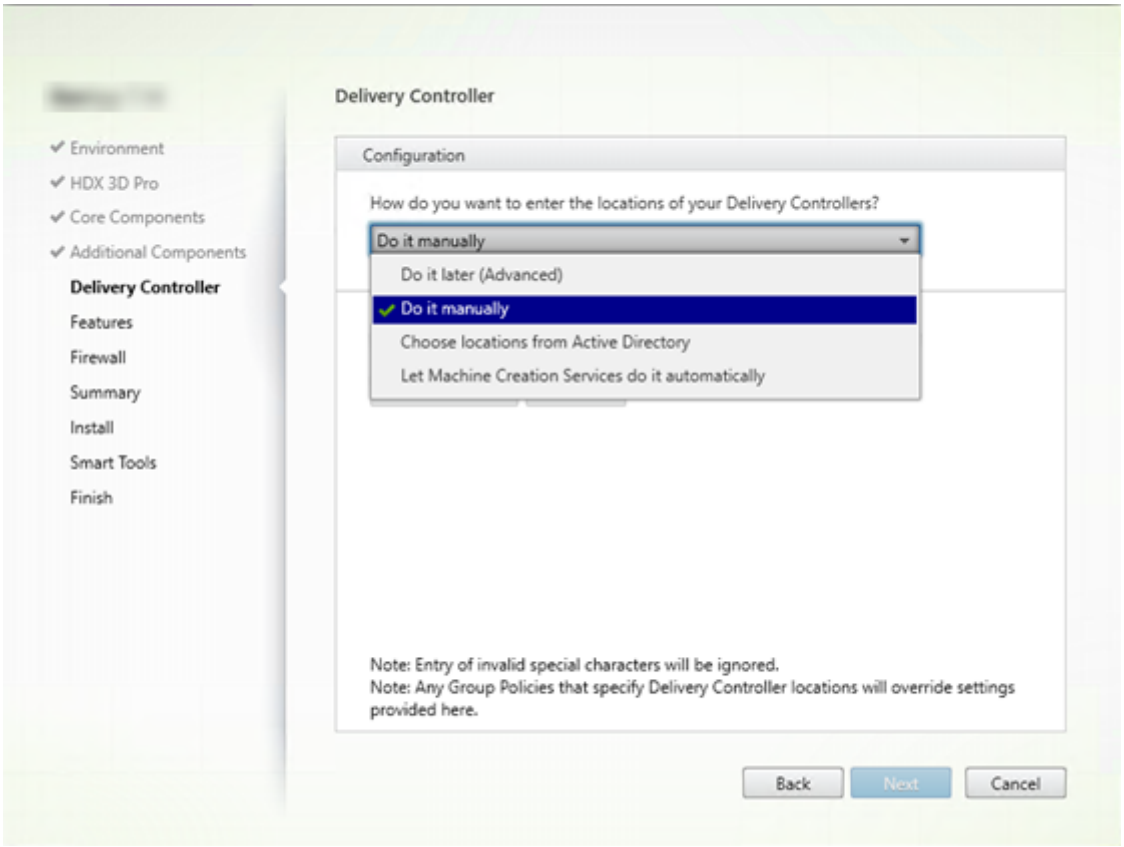
Es gibt verschiedene Methoden zum Konfigurieren von Controller-/Cloud Connector-Adressen auf einem VDA.

- Über Richtlinien (LGPO oder GPO)
- Über die Registrierung (Gruppenrichtlinieneinstellungen, manuell während der VDA-Installation)

- Über Active Directory (Legacy-OU-Discovery)
- Über MCS (personality.ini)

Sie geben die anfängliche Registrierungsmethode an, wenn Sie einen VDA installieren. (Wenn Sie die automatische Aktualisierung deaktivieren, wird die bei der VDA-Installation gewählte Methode auch für nachfolgende Registrierungen verwendet.)

Die nachfolgende Abbildung zeigt die Seite **Delivery Controller** des VDA-Installationsassistenten.



Konfiguration über Richtlinien (LGPO, GPO)

Citrix empfiehlt die Verwendung des Gruppenrichtlinienobjekts für die VDA-Erstregistrierung. Es hat die höchste Priorität. (Obwohl die automatische Aktualisierung vorher mit höchster Priorität aufgelistet wurde, wird automatische Aktualisierung nur nach der Erstregistrierung verwendet.) Die richtlinienbasierte Registrierung bietet den Vorteil der Zentralisierung der Konfiguration über die Gruppenrichtlinie.

Zum Angeben dieser Methode führen Sie die folgenden Schritte aus:

- Wählen Sie auf der Seite **Delivery Controller** des VDA-Installationsassistenten **Später (erweitert)**. Aufgrund der hohen Bedeutung der VDA-Registrierung werden Sie von dem Assistenten

mehrmals an das Angeben von Controlleradressen erinnert, obwohl Sie sie während der VDA-Installation nicht angeben. (Die VDA-Registrierung ist wirklich wichtig!)

- Aktivieren oder deaktivieren Sie die richtlinienbasierte VDA-Registrierung durch die Citrix Richtlinie über die Einstellung `Virtual Delivery Agent Settings > Controllers`. (Wenn Sicherheit höchste Priorität hat, verwenden Sie die Einstellung `Virtual Delivery Agent Settings > Controller SIDs`.)

Diese Einstellung wird unter `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)` gespeichert.

Konfiguration über die Registrierung

Zum Angeben dieser Methode führen Sie einen der folgenden Schritte aus:

- Wählen Sie auf der Seite **Delivery Controller** des VDA-Installationsassistenten **Manuell**. Geben Sie dann den FQDN eines installierten Controllers ein und klicken Sie auf **Hinzufügen**. Wenn Sie weitere Controller installiert haben, fügen Sie deren Adressen hinzu.
- Bei einer VDA-Installation über die Befehlszeile verwenden Sie die Option "/controller"und geben Sie die FQDNs der installierten Controller bzw. Cloud Connectors an.

Diese Informationen werden in der Regel im Registrierungswert ListOfDDCs unter dem Registrierungsschlüssel `HKLM\Software\Citrix\VirtualDesktopAgent` oder `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent` gespeichert.

Sie können diesen Registrierungsschlüssel auch manuell oder über Gruppenrichtlinieneinstellungen (GPP) konfigurieren. Diese Methode ist eventuell der richtlinienbasierten vorzuziehen, z. B. wenn Sie eine bedingungsbasierte Verarbeitung verschiedener Controller bzw. Cloud Connectors wünschen, etwa "'XDC-001'für Computernamen verwenden, die mit 'XDW-001-'beginnen".

Aktualisieren Sie den Registrierungsschlüssel "ListOfDDCs", der die vollqualifizierten Domänennamen aller Controller bzw. Cloud Connectors in der Site enthält. (Dieser Schlüssel entspricht der Active Directory-Site-Organisationseinheit.)

`HKEY_LOCAL_MACHINE\Software\Citrix\\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

Wenn die Registrierungsstruktur `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` sowohl die Registrierungsschlüssel ListOfDDCs und FarmGUID enthält, wird ListOfDDCs für die Controller- oder Cloud Connector-Discovery verwendet. FarmGUID ist vorhanden, wenn die Organisationseinheit der Site bei der Installation des VDAs angegeben wurde. (Dies kann für Legacy-Bereitstellungen verwendet werden.)

Aktualisieren Sie optional den Registrierungsschlüssel "ListOfSIDs"(weitere Informationen unter ListOfSIDs):

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs` (`REG_SZ`)

> **Nicht vergessen:**
>
> Wenn Sie außerdem die richtlinienbasierte VDA-Registrierung über die Citrix Richtlinie aktivieren, hat diese Konfiguration Vorrang vor den bei der VDA-Installation angegebenen Konfigurationseinstellungen, da sie eine höhere Methodenpriorität hat.

Konfiguration über Active Directory-Organisationseinheit

Diese Methode wird hauptsächlich zum Zweck der Abwärtskompatibilität unterstützt und wird nicht empfohlen. Wenn Sie sie noch immer verwenden, empfiehlt Citrix den Wechsel zu einer anderen Methode.

Zum Angeben dieser Methode führen Sie die folgenden Schritte aus:

- Wählen Sie auf der Seite **Delivery Controller** des VDA-Installationsassistenten **Standorte aus Active Directory auswählen**.
- Verwenden Sie das Skript `Set-ADControllerDiscovery.ps1` (steht auf jedem Controller zur Verfügung). Konfigurieren Sie außerdem den Registrierungseintrag "FarmGuid"auf jedem VDA mit der korrekten Organisationseinheit. Diese Einstellung kann mit der Gruppenrichtlinie konfiguriert werden.

Informationen finden Sie unter Auf Organisationseinheiten von Active Directory basierende Controller-Discovery.

Konfiguration über MCS

Wenn Sie virtuelle Maschinen mit MCS bereitstellen, können Sie MCS zur Einrichtung der Liste der Controller bzw. Cloud Connectors konfigurieren. Dieses Feature ist kompatibel mit der automatischen Aktualisierung: MCS fügt die Controller-/Connectorliste bei der ersten Bereitstellung (beim Erstellen des Maschinenkatalogs) in die Datei `Personality.ini` ein. Die automatische Aktualisierung sorgt dafür, dass die Liste immer aktuell bleibt.

Diese Methode wird für große Umgebungen nicht empfohlen. Sie eignet sich in folgenden Fällen:

- Die Umgebung ist klein.
- Es werden keine VDAs zwischen Sites verschoben.
- Sie stellen virtuelle Maschinen ausschließlich mit MCS bereit.
- Sie möchten die Gruppenrichtlinie nicht verwenden.

Gehen Sie zum Angeben dieser Methode folgendermaßen vor:

- Wählen Sie auf der Seite **Delivery Controller** des VDA-Installationsassistenten **Automatische Erstellung durch Maschinenerstellungsdienste**.

Empfehlungen

Bewährte Methoden:

- Verwenden Sie die Gruppenrichtlinie für die Erstregistrierung.
- Verwenden Sie die automatische Aktualisierung (standardmäßig aktiviert), um die Controllerliste auf dem neuesten Stand zu halten.
- Verwenden Sie in einer Multizonenbereitstellung die Gruppenrichtlinie für die anfängliche Konfiguration (mit mindestens zwei Controllern bzw. Cloud Connectors). Verweisen Sie die VDAs auf lokale Controller bzw. Cloud Connectors in ihrer Zone. Verwenden Sie die automatische Aktualisierung um die Einrichtung auf dem letzten Stand zu halten. Durch die automatische Aktualisierung wird die Liste "ListOfDDCs"für VDAs in Satellitenzonen automatisch optimiert.

Automatische Updates

Die automatische Aktualisierung wurde in XenApp und XenDesktop 7.6 eingeführt und ist standardmäßig aktiviert. Sie stellt die effizienteste Methode dar, um VDA-Registrierungen auf dem neuesten Stand zu halten. Bei der Erstregistrierung eines VDAs erfolgt zwar keine automatische Aktualisierung, die zugehörige Software lädt jedoch die Liste "ListOfDDCs"herunter und speichert sie in einem persistenten Cache auf dem VDA. Dies geschieht bei jedem VDA. (In dem Cache werden auch Maschinenrichtlinieninformationen gespeichert, sodass Richtlinieneinstellungen bei Neustarts beibehalten werden.)

Die automatische Aktualisierung wird unterstützt, wenn das Provisioning über MCS oder PVS erfolgt, außer bei Verwendung eines PVS-Server-Cache. Dies ist jedoch kein übliches Verfahren, da es keinen persistenten Cache zur Speicherung automatischer Aktualisierungen gibt.

Gehen Sie zum Angeben dieser Methode folgendermaßen vor:

- Aktivieren oder deaktivieren Sie die automatische Aktualisierung über eine Citrix Richtlinie, die die Einstellung `Virtual Delivery Agent Settings` > `Enable auto update of Controllers` enthält. Diese Einstellung ist standardmäßig aktiviert.

Funktionsweise:

- Bei jeder erneuten Registrierung eines VDAs (z. B. nach einem Neustart der Maschine) wird der Cache aktualisiert. Außerdem überprüft jeder Controller bzw. Cloud Connector alle 90 Minuten die Sitedatenbank. Wenn seit der letzten Überprüfung ein Controller bzw. Cloud Connector

hinzugefügt oder entfernt wurde oder bei einer Änderung der Richtlinie, die sich auf die VDA-Registrierung auswirkt, sendet der Controller bzw. Cloud Connector eine aktualisierte Liste an die bei ihm registrierten VDAS und der Cache wird aktualisiert. Der VDA nimmt alle Verbindungen von allen Controllern bzw. Cloud Connectors in der aktuellen Liste im Cache an.

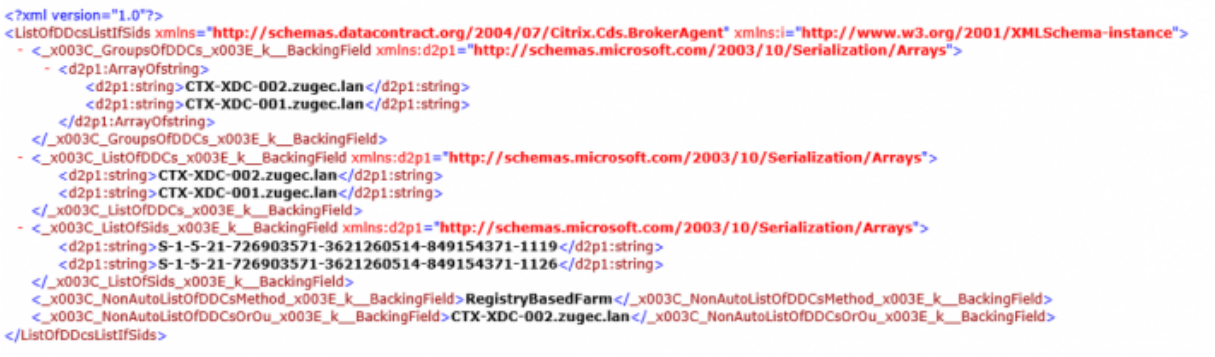
- Geht eine Liste ein, die den Controller bzw. Cloud Connector, bei dem der VDA registriert ist, nicht enthält (d. h. der Controller/Cloud Connector wurde aus der Site entfernt), nimmt der VDA eine neue Registrierung bei einem der Controller bzw. Cloud Connectors aus der Liste "ListOfDDCs"vor.

Beispiel:

- Die Bereitstellung hat die drei Controller A, B und C. Ein VDA wird bei Controller B registriert (dies wurde bei der Installation des VDAs festgelegt).
- Anschließend werden der Site zwei Controller (D und E) hinzugefügt. Innerhalb von 90 Minuten erhalten die VDAs aktualisierte Listen und akzeptieren Verbindungen von den Controllern A, B, C, D und E. Die Lastverteilung auf alle Controller erfolgt erst nach einem Neustart der VDAs.
- Controller B wird später in eine andere Site verschoben. Innerhalb von 90 Minuten erhalten die VDAs der ursprünglichen Site aktualisierte Listen, da seit der letzten Überprüfung eine Controlleränderung stattfand. Der ursprünglich bei (dem nun nicht mehr vorhandenen) Controller B registrierte VDA wird bei einem der anderen Controller der Liste (A, C, D oder E) registriert.

In einer Bereitstellung mit mehreren Zonen speichert die automatische Aktualisierung in einer Satellitenzone automatisch zuerst alle lokalen Controller. Alle Controller in der primären Zone werden in einer Sicherungsgruppe gespeichert. Wenn keine lokalen Controller in der Satellitenzone zur Verfügung stehen, wird eine Registrierung bei einem Controller in der primären Zone versucht.

Die Cachedatei enthält wie im folgenden Beispiel dargestellt Hostnamen und eine Liste von Sicherheits-IDs (ListOfSIDs). Der VDA fragt keine SIDs ab, wodurch die Active Directory-Last reduziert wird.



```
<?xml version="1.0"?>
<ListOfDDcsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
 - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    - <d2p1:ArrayOfstring>
        <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
        <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
      </d2p1:ArrayOfstring>
   </_x003C_GroupsOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
      <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
   </_x003C_ListOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
   </_x003C_ListOfSids_x003E_k__BackingField>
   <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
   <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDcsListIfSids>
```


Sie können die Cachedatei mit einem WMI-Aufruf abrufen. Allerdings ist sie an einem Speicherort gespeichert, auf den nur das SYSTEM-Konto Lesezugriff hat. Diese Angaben dienen lediglich der Information. ÄNDERN SIE DIESE DATEI NICHT. Änderungen an dieser Datei oder an dem Ordner führen zu einer nicht unterstützten Konfiguration.


```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "
Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

Wenn Sie die Liste "ListOfSIDs"aus Sicherheitsgründen (d. h. nicht zur Senkung der Active Directory-Last) manuell konfigurieren müssen, können Sie die automatische Aktualisierung nicht verwenden. Weitere Informationen finden Sie unten unter ListOfSIDs.

Ausnahme zur Priorität der automatischen Aktualisierung

Die automatische Aktualisierung besitzt zwar in der Regel die höchste Priorität unter allen VDA-Registrierungsmethoden und setzt die Einstellungen anderer Methoden außer Kraft, es gibt jedoch eine Ausnahme. Die `NonAutoListOfDDCs`-Elemente im Cache geben die anfängliche VDA-Konfigurationsmethode an. Die automatische Aktualisierung überwacht diese Informationen. Wenn sich die anfängliche Registrierungsmethode ändert, wird bei der Registrierung die automatische Aktualisierung übersprungen und die Methode mit der nächsthöchsten Priorität verwendet. Dies kann hilfreich sein, wenn Sie einen VDA in eine andere Site verschieben (zum Beispiel bei einer Notfallwiederherstellung).

Überlegungen zur Konfiguration

Controller- bzw. Cloud Connector-Adressen

Unabhängig davon, welche Methode Sie zum Angeben von Controllern bzw. Cloud Connectors verwenden, empfiehlt Citrix eine FQDN-Adresse. Eine IP-Adresse gilt nicht als vertrauenswürdige Konfiguration, da sie leichter als ein DNS-Datensatz angegriffen werden kann. Wenn Sie die Liste "ListOfSIDs" manuell erstellen, können Sie eine IP-Adresse in einer ListOfDDCs-Liste verwenden. Es wird dennoch empfohlen, FQDNs zu verwenden.

Lastausgleich

Wie bereits erwähnt, verteilt ein VDA die Verbindungen automatisch über alle Controller bzw. Cloud Connectors in der Liste "ListOfDDCs". Failover und Lastausgleich sind Teil des für die Vermittlung verwendeten Protokolls CBP (Citrix Brokering Protocol). Wenn Sie mehrere Controller bzw. Cloud Connectors in Ihrer Konfiguration angeben, erfolgt bei Bedarf bei der Registrierung automatisch ein Failover zwischen diesen. Bei der automatischen Aktualisierung erfolgt automatisch ein Failover für alle VDAS.

Aus Sicherheitsgründen können Sie keinen Netzwerk-Load Balancer wie etwa Citrix ADC verwenden. Bei der VDA-Registrierung wird die gegenseitige Authentifizierung über Kerberos verwendet, bei der der Client (VDA) dem Dienst (Controller) seine Identität beweisen muss. Doch auch der Controller bzw.

Cloud Connector muss dem VDA seine Identität beweisen. Das bedeutet, dass VDA und Controller/-Cloud Connector Server und Client zugleich sind. Wie bereits am Anfang dieses Artikels erwähnt, gibt es zwei Kommunikationskanäle: VDA zum Controller bzw. Cloud Connector und Controller bzw. Cloud Connector zum VDA.

Eine Komponente dieses Prozesses ist der Dienstprinzipalname (SPN), der als Eigenschaft in einem Active Directory-Computerobjekt gespeichert ist. Wenn der VDA sich mit einem Controller bzw. Cloud Connector verbindet, muss er angeben, mit wem er kommunizieren möchte. Diese Adresse ist ein SPN. Wenn Sie IP-Adressen und Lastausgleich verwenden, wird bei der gegenseitigen Kerberos-Authentifizierung richtig erkannt, dass die IP-Adresse nicht zu dem erwarteten Controller bzw. Cloud Connector gehört.

Weitere Informationen:

- Einführung in Kerberos: https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/
- Gegenseitige Authentifizierung mit Kerberos: https://docs.microsoft.com/en-us/windows/win32/ad/mutual-authentication-using-kerberos?redirectedfrom=MSDN

Automatische Aktualisierung ersetzt CNAME

Die automatische Aktualisierung ersetzt die CNAME-Funktion (DNS-Alias) von XenApp- und XenDesktop-Versionen vor 7.x. Die CNAME-Funktion ist ab XenApp- und XenDesktop-Version 7 deaktiviert. Verwenden Sie statt CNAME die automatische Aktualisierung. (Wenn Sie CNAME verwenden müssen, lesen Sie CTX137960. Damit die DNS-Aliasfunktion einwandfrei funktioniert, verwenden Sie CNAME und automatische Aktualisierung nicht gleichzeitig.)

Controller-/Cloud Connector-Gruppen

Es ist günstig, Controller oder Cloud Connectors in Gruppen zu verarbeiten. Bei Gruppen wird eine Gruppe bevorzugt und die andere Gruppe für ein Failover verwendet, wenn alle Controller/Cloud Connectors ausfallen. Controller bzw. Cloud Connectors werden zufällig aus der Liste ausgewählt, eine Gruppierung kann daher zur Durchsetzung einer bevorzugten Verwendung helfen.

Verwenden Sie Klammern, um Controller-/Connectorgruppen anzugeben. Beispiel für vier Controller (zwei primäre und zwei als Ersatz):

(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan).

In diesem Beispiel werden die Controller der ersten Gruppe (001, 002) zuerst verarbeitet. Wenn beide ausfallen, werden die Controller der zweiten Gruppe (003 und 004) verarbeitet.

ListOfSIDs

ListOfDDCs ist die Liste der Controller, die ein VDA zur Registrierung ansprechen kann. Ein VDA muss außerdem "wissen", welche Controller vertrauenswürdig sind. VDAS vertrauen nicht automatisch den Controllern in der Liste "ListOfDDCs". Die Liste der Sicherheits-IDs (ListOfSIDs) enthält die vertrauenswürdigen Controller. VDAs versuchen eine Registrierung nur mit vertrauenswürdigen Controllern.

In den meisten Umgebungen wird die Liste "ListOfSIDs"automatisch aus der Liste "ListOfDDCs"generiert. Sie können die Liste "ListOfSIDs"mit einer CDF-Ablaufverfolgung lesen.

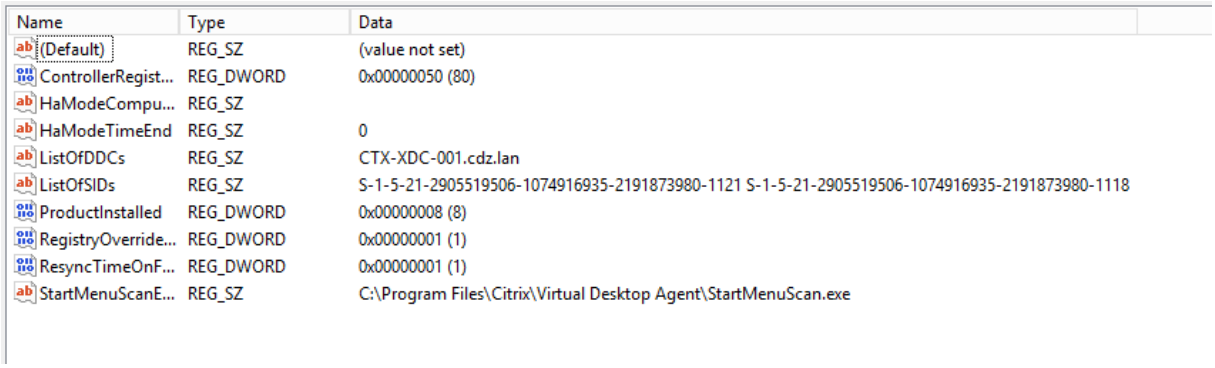
Im Allgemeinen besteht keine Notwendigkeit einer manuellen Änderung der Liste "ListOfSIDs". Es müssen allerdings einige Ausnahmen berücksichtigt werden. Die ersten beiden Ausnahmen sind nicht mehr relevant, da neuere Technologien zur Verfügung stehen.

- **Getrennte Rollen für Controller:** Vor der Einführung von Zonen in XenApp und XenDesktop 7.7 wurde die Liste "ListOfSIDs"manuell konfiguriert, wenn nur eine Teilgruppe von Controllern für die Registrierung verwendet wurde. Wenn beispielsweise XDC-001 und XDC-002 als XML-Broker verwendet wurden und XDC-003 und XDC-004 für die VDA-Registrierung, wurden alle Controller in der Liste "ListOfSIDs"sowie die Controller XDC-003 und XDC-004 in der Liste "ListOfDDCs" angegeben. Diese Konfiguration ist weder normal noch empfohlen und wird in neueren Umgebungen nicht eingesetzt. Verwenden Sie stattdessen Zonen.
- **Reduzierung der Active Directory-Last:** Vor Einführung der automatischen Aktualisierung in XenApp und XenDesktop 7.6 wurde die Liste "ListOfSIDs"zur Reduzierung der Last auf Domänencontrollern verwendet. Durch das Auffüllen der Liste "ListOfSIDs"vorab kann die Auflösung von DNS-Namen in SIDs ausgelassen werden. Durch die automatische Aktualisierung entfällt jedoch die Notwendigkeit für diesen Arbeitsschritt, da der persistente Cache SIDs enthält. Citrix empfiehlt, die automatische Aktualisierung aktiviert zu lassen.
- **Sicherheit:** In manchen hochsicheren Umgebungen wurden die SIDs vertrauenswürdiger Controller manuell konfiguriert, um mögliche Sicherheitsbedrohungen durch beeinträchtigte DNS-Server zu vermeiden. Hierfür müssen Sie jedoch auch die automatische Aktualisierung deaktivieren. Andernfalls wird die Konfiguration aus dem persistenten Cache verwendet.

Ändern Sie also die Liste "ListOfSIDs"nicht ohne spezifischen Grund.

Wenn Sie die Liste "ListOfSIDs"ändern müssen, erstellen Sie einen Registrierungsschlüssel namens "ListOfSIDs (REG_SZ)"unter HKLM\Software\Citrix\VirtualDesktopAgent. Der Wert ist eine vertrauenswürdige SID, bzw. eine Liste mehrerer, durch Leerzeichen getrennter SIDs.

Im folgenden Beispiel werden ein Controller für die VDA-Registrierung (ListOfDDCs) und zwei für die Vermittlung (ListOfSIDs) verwendet.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

Controllersuche während der VDA-Registrierung

Wenn ein VDA versucht, sich zu registrieren, führt der Broker-Agent zunächst eine DNS-Suche in der lokalen Domäne durch, um sicherzustellen, dass der angegebene Controller erreicht werden kann.

Wenn der Controller dabei nicht gefunden wird, kann der Broker-Agent eine Top-Down-Fallbacksuche in AD starten. Diese Abfrage durchsucht alle Domänen und wird mehrfach wiederholt. Wenn die Controlleradresse ungültig ist (z. B. weil der Administrator bei der Installation des VDA einen falschen FQDN eingegeben hat), kann die Abfrage zu einem verteilten Denial-of-Service (DDoS) auf dem Domänencontroller führen.

Der folgende Registrierungsschlüssel legt fest, ob der Broker-Agent die Top-Down-Fallbacksuche verwendet, wenn er bei der ersten Suche keinen Controller findet.

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- Name: `DisableDdcWildcardNameLookup`
- Typ: `DWORD`
- Wert: `1` (Standard) oder `0`

Bei Auswahl von `1` ist die Fallbacksuche deaktiviert. Wenn die erste Suche nach dem Controller fehlschlägt, sucht der Broker-Agent nicht weiter. Dies ist die Standardeinstellung.
Bei Auswahl von `0` ist die Fallbacksuche aktiviert. Wenn die erste Suche nach dem Controller fehlschlägt, wird die Top-Down-Fallbacksuche gestartet.

Problembehandlung bei der VDA-Registrierung

Wie bereits erwähnt, muss ein VDA bei einem Delivery Controller registriert sein, damit er beim Start gebrokerter Sitzungen in die Auswahl kommt. Nicht registrierte VDAs können eine mangelnde Auslastung verfügbarer Ressourcen zur Folge haben. Es gibt eine Reihe von Gründen, warum ein VDA nicht registriert sein könnte. Viele können vom Administrator behandelt werden. Studio bietet Informationen zur Problembehandlung im Assistenten zum Erstellen von Maschinenkatalogen und nach dem Erstellen einer Bereitstellungsgruppe.

Identifizieren von Problemen während der Maschinenkatalogerstellung:

Im Assistenten zum Erstellen von Maschinenkatalogen wird nach dem Hinzufügen vorhandener Maschinen in der Liste der Computerkontonamen angezeigt, ob die einzelnen Maschinen zum Hinzufügen zu dem Katalog geeignet sind. Zeigen Sie auf das Symbol neben jeder Maschine, um Informationen dazu einzublenden.

Wenn die Nachricht eine problematische Maschine identifiziert, können Sie diese Maschine entweder entfernen (über die Schaltfläche **Entfernen**) oder die Maschine hinzufügen. Wird beispielsweise gemeldet, dass die Maschineninformationen nicht abgerufen wurden (z. B. weil die Maschine bei keinem Delivery Controller registriert wurde) können Sie die Maschine auf Wunsch dennoch hinzufügen.

Die Funktionsebene eines Katalogs steuert, welche Produktfeatures den Maschinen in dem Katalog zur Verfügung stehen. Zur Verwendung von Features, die in neueren Produktversionen eingeführt wurden ist u. U. ein neuer VDA erforderlich. Das Festlegen einer Funktionsebene stellt den Maschinen in dem Katalog alle mit der entsprechenden Version (und höheren Versionen, wenn die Funktionsebene nicht geändert wird) eingeführten Features zur Verfügung. In dem Katalog enthaltene Maschinen mit einer älteren VDA-Version können dann allerdings nicht registriert werden.

Identifizieren von Problemen nach der Erstellung von Bereitstellungsgruppen:

Nach dem Erstellen einer Bereitstellungsgruppe werden in Studio Informationen zu Maschinen angezeigt, die der Gruppe zugeordnet sind. Im Detailbereich für eine Bereitstellungsgruppe wird die Anzahl der Maschinen angezeigt, die registriert sein müssten, es jedoch nicht sind. Es kann also Maschinen geben, die eingeschaltet und nicht im Wartungsmodus sind, jedoch nicht bei einem Controller registriert sind. Beim Anzeigen einer Maschine, die eigentlich registriert sein müsste, enthält die Registerkarte **Problembehandlung** im Detailbereich Informationen zu möglichen Ursachen und empfohlene Korrekturmaßnahmen.

Weitere Informationen finden Sie unter Erstellen von Maschinenkatalogen im Abschnitt *VDA-Versionen und Funktionsebenen*.

Weitere Informationen zur Fehlerbehebung bei der VDA-Registrierung finden Sie unter CTX136668.

Sie können auch den Citrix Health Assistant zur Problembehandlung bei der VDA-Registrierung und Sitzungsstarts verwenden. Weitere Informationen finden Sie unter CTX207624.

Sitzungen

August 18, 2021

Aufrechterhalten der Sitzungsaktivität ist wichtig für die beste Benutzererfahrung. Eine Unterbrechung der Verbindung aufgrund von unzuverlässigen Netzwerken, stark variierender Netzw-

erklatenz oder Bereichseinschränkungen von drahtlosen Geräten kann zu Frustrationen bei den Benutzern führen. Ein schneller Wechsel zwischen Arbeitsstationen und Zugriff auf dieselben Anwendungen bei jeder Anmeldung ist eine Priorität für viele mobile Mitarbeiter, z. B. von Mitarbeitern in einem Krankenhaus.

Die folgenden Features dienen dazu, die Sitzungszuverlässigkeit zu optimieren, Unannehmlichkeiten, Ausfallzeiten und Produktivitätsverluste zu reduzieren, und mobilen Benutzern einen schnellen und einfachen Wechsel zwischen Geräten zu ermöglichen.

Im Abschnitt Anmeldeintervall wird beschrieben, wie Sie die Standardeinstellung ändern.

Sie können Benutzer von einer Sitzung abmelden, Sitzungen trennen und Sitzungsvorabstart sowie Sitzungsfortbestehen konfigurieren. Informationen hierzu finden Sie im Artikel Verwalten von Bereitstellungsgruppen.

Sitzungszuverlässigkeit

Durch die Sitzungszuverlässigkeit bleiben Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkkonnektivität unterbrochen wird. Die Benutzer sehen so lange weiterhin die Anwendung, die sie verwenden, bis die Netzwerkkonnektivität wiederhergestellt ist.

Diese Funktion ist besonders für mobile Benutzer mit drahtlosen Verbindungen geeignet. Ein Benutzer mit einer drahtlosen Verbindung fährt z. B. in einen Tunnel und die Verbindung wird vorübergehend unterbrochen. Normalerweise würde die Sitzung getrennt und nicht mehr auf dem Bildschirm angezeigt. Der Benutzer müsste sich neu mit der getrennten Sitzung verbinden. Mit der Sitzungszuverlässigkeit bleibt die Sitzung auf der Maschine aktiv. Auf dem Client friert der Bildschirm ein und der Mauszeiger wird als Sanduhr angezeigt, bis die Verbindung am Ende des Tunnels wiederhergestellt ist. Der Benutzer kann während der Unterbrechung weiterhin auf die Anzeige zugreifen und mit der Anwendung weiterarbeiten, wenn die Netzwerkverbindung wiederhergestellt ist. Die Sitzungszuverlässigkeit verbindet Benutzer ohne Neuauthentifizierung wieder.

Citrix Receiver-Benutzer können die Controllereinstellung nicht überschreiben.

Sie können die Sitzungszuverlässigkeit mit Transport Layer Security (TLS) verwenden. Mit TLS werden nur die Daten verschlüsselt, die zwischen dem Benutzergerät und NetScaler Gateway gesendet werden.

Sie aktivieren und konfigurieren die Sitzungszuverlässigkeit mit den folgenden Einstellungen:

- Mit der Richtlinieneinstellung “Sitzungszuverlässigkeit - Verbindungen”können Sie die Sitzungszuverlässigkeit aktivieren oder deaktivieren.
- Der Standardwert für die Einstellung “Sitzungszuverlässigkeit - Timeout”ist 180 Sekunden (drei Minuten). Obwohl Sie den Zeitraum vergrößern können, den die Sitzungszuverlässigkeit eine Sitzung offen lässt, sollten Sie dabei berücksichtigen, dass diese Funktion den Benutzer nicht zu

einer Neuauthentifizierung auffordert, um den Bedienungskomfort zu erhöhen. Je länger eine Sitzung offen gelassen wird, desto höher ist das Risiko, dass der Benutzer abgelenkt wird und das Benutzergerät verlässt. Benutzer ohne Berechtigung hätten in dem Fall möglicherweise Zugriff auf die Sitzung.

- Eingehende Sitzungszuverlässigkeitsverbindungen verwenden Port 2598, es sei denn, die Portnummer wurde unter "Sitzungszuverlässigkeit - Portnummer"geändert.
- Verwenden Sie die Funktion zur automatischen Wiederverbindung von Clients, wenn Sie möchten, dass Benutzer eine Verbindung mit unterbrochenen Sitzungen nur mit einer Neuauthentifizierung wiederherstellen können. Sie können die Einstellung für die Citrix-Richtlinie Authentifizierung bei automatischer Wiederverbindung von Clients so konfigurieren, dass Benutzer aufgefordert werden, sich neu zu authentifizieren, wenn sie sich mit einer unterbrochenen Sitzung wieder verbinden.

Wenn Sie sowohl Sitzungszuverlässigkeit als auch die Funktion zur automatischen Wiederverbindung verwenden, werden beide Funktionen nacheinander ausgeführt. Die Sitzungszuverlässigkeit beendet oder trennt die Benutzersitzung, sobald der mit der Option "Sitzungszuverlässigkeit - Timeout" festgelegte Zeitraum abläuft. Anschließend werden die Richtlinieneinstellungen für die automatische Wiederverbindung von Clients wirksam und es wird versucht, eine Verbindung mit der unterbrochenen Sitzung wiederherzustellen.

Automatische Wiederverbindung von Clients

Mit der automatischen Wiederverbindung von Clients kann Citrix Receiver unabsichtlich getrennte ICA-Sitzungen erkennen und die Benutzer automatisch wieder mit den betroffenen Sitzungen verbinden. Wenn diese Funktion auf dem Server aktiviert ist, müssen Benutzer nicht manuell eine neue Verbindung herstellen, um mit ihrer Arbeit fortfahren zu können.

Bei Anwendungssitzungen versucht Citrix Receiver, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht.

Bei Desktopsitzungen versucht Citrix Receiver eine festgelegte Zeit lang, die Verbindung mit der Sitzung wiederherzustellen, bis die Wiederverbindung erfolgreich war oder der Benutzer die Wiederverbindung abbricht. Der Standardwert für diese Zeit ist fünf Minuten. Um die Zeit zu ändern, bearbeiten Sie die Registrierung auf dem Benutzergerät:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<Sekunden>

wobei <*Sekunden*> die Zeit in Sekunden ist, nach der keine weiteren Versuche zur Wiederverbindung unternommen werden.

Sie aktivieren und konfigurieren die automatische Wiederverbindung von Clients mit den folgenden Einstellungen:

- **Automatische Wiederverbindung von Clients**: Aktiviert oder deaktiviert die automatische Wiederverbindung von Citrix Receiver, nach dem die Verbindung unterbrochen wurde.
- **Authentifizierung bei automatischer Wiederverbindung von Clients**: Aktiviert oder deaktiviert die erforderliche Benutzerauthentifizierung bei der automatischen Wiederverbindung
- **Protokollierung der automatischen Wiederverbindung von Clients**: Aktiviert oder deaktiviert die Protokollierung von Wiederverbindungsereignissen im Ereignisprotokoll. Die Protokollierung ist standardmäßig deaktiviert. Wenn diese Einstellung aktiviert ist, werden Informationen zu erfolgreichen oder fehlgeschlagenen automatischen Wiederverbindungsereignissen im Systemprotokoll des Servers aufgezeichnet. Jeder Server speichert die Informationen zu Wiederverbindungsereignissen im eigenen Systemprotokoll; die Site stellt kein Protokoll aller Wiederverbindungsereignisse aller Server bereit.

Bei der automatischen Wiederverbindung von Clients findet eine Authentifizierung mit verschlüsselten Anmeldeinformationen statt. Wenn sich ein Benutzer anmeldet, verschlüsselt und speichert der Server die Anmeldeinformationen und erstellt und sendet ein Cookie mit einem Verschlüsselungsschlüssel an Citrix Receiver. Citrix Receiver übergibt den Schlüssel zum Wiederverbinden an den Server. Der Server entschlüsselt die Anmeldeinformationen und gibt sie an die Windows-Anmeldung für eine Authentifizierung weiter. Benutzer müssen sich beim Ablaufen von Cookies neu authentifizieren, um Sitzungen wiederherzustellen.

Cookies werden nicht verwendet, wenn Sie die Einstellung "Authentifizierung bei automatischer Wiederverbindung von Clients"aktivieren. Stattdessen wird der Benutzer in einem Dialogfeld zur Eingabe der Anmeldeinformationen aufgefordert, wenn Citrix Receiver versucht, die Verbindung automatisch wiederherzustellen.

Zum maximalen Schutz der Anmeldeinformationen von Benutzern und von Sitzungen verwenden Sie die Verschlüsselung für die gesamte Kommunikation zwischen Clients und Site.

Sie deaktivieren die automatische Wiederverbindung in Citrix Receiver für Windows mit der Datei icaclient.adm. Diese Datei liegt derzeit nur in Englisch vor. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Version von Citrix Receiver für Windows.

Einstellungen für Verbindungen wirken sich auch auf die automatische Wiederverbindung von Clients aus:

- In der Standardeinstellung wird die automatische Wiederverbindung von Clients durch Richtlinieneinstellungen auf der Siteebene aktiviert (siehe oben). Der Benutzer muss sich nicht authentifizieren. Wenn jedoch die ICA-TCP-Verbindung eines Servers so konfiguriert wurde, dass Sitzungen mit einer unterbrochenen Kommunikationsverbindung zurückgesetzt werden, findet die automatische Wiederverbindung nicht statt. Die automatische Wiederverbindung von Clients funktioniert nur, wenn der Server Sitzungen trennt, wenn eine unterbrochene Verbindung oder eine Verbindungstimeout vorliegt. In diesem Zusammenhang verweist "ICA-TCP-Verbindung"auf den virtuellen Serverport (nicht auf eine tatsächliche

Netzwerkverbindung), der für Sitzungen in TCP/IP-Netzwerken verwendet wird.

- Standardmäßig ist die ICA-TCP-Verbindung auf einem Server so eingestellt, dass Sitzungen mit unterbrochenen Verbindungen oder Verbindungen, die das Zeitlimit überschritten haben, getrennt werden. Getrennte Sitzungen bleiben im Systemspeicher intakt und stehen für eine Wiederverbindung durch Citrix Receiver zur Verfügung.
- Die Verbindung kann so konfiguriert werden, dass Sitzungen mit unterbrochenen Verbindungen oder Verbindungen mit Timeouts zurückgesetzt oder abgemeldet werden. Wenn eine Sitzung zurückgesetzt wird, wird bei einem Wiederverbindungsversuch eine neue Sitzung eingeleitet; die Umgebung des Benutzers wird in der verwendeten Anwendung nicht wiederhergestellt, sondern die Anwendung wird neu gestartet.
- Wenn der Server für das Zurücksetzen von Sitzungen konfiguriert ist, erstellt die automatische Wiederverbindung von Clients eine neue Sitzung. Benutzer müssen dann ihre Anmeldeinformationen eingeben, um sich am Server anzumelden.
- Die automatische Wiederverbindung kann fehlschlagen, wenn Citrix Receiver oder das Plug-In falsche Authentifizierungsinformationen übergibt (dies kann während eines Angriffs passieren), oder wenn der Server feststellt, dass zu viel Zeit seit dem Erkennen der unterbrochenen Verbindung verstrichen ist.

ICA-Keep-Alive

ICA-Keep-Alive verhindert, dass Sitzungen durch unterbrochene Verbindungen getrennt werden. Wenn der Server keine Aktivität erkennt (z. B. keine Zeitänderungen, Mausbewegungen oder Bildschirmaktualisierungen) wird verhindert, dass die Sitzung durch die Remotedesktopdienste getrennt wird. Der Server sendet alle paar Sekunden Keep-Alive-Pakete, um zu erkennen, ob die Sitzung aktiv ist. Wenn die Sitzung nicht mehr aktiv ist, wird die Sitzung vom Server als "Getrennt" gekennzeichnet.

> **Hinweis:**
>
> ICA-Keep-Alive funktioniert nur, wenn Sie die Sitzungszuverlässigkeit nicht verwenden. Die Sitzungszuverlässigkeit hat eigene Mechanismen für das Aufrechterhalten von Verbindungen. Konfigurieren Sie ICA-Keep-Alive nur für Verbindungen, die keine Sitzungszuverlässigkeit verwenden.

ICA-Keep-Alive-Einstellungen überschreiben Keep-Alive-Einstellungen, die für Microsoft Windows-Gruppenrichtlinien konfiguriert wurden.

Sie aktivieren und konfigurieren ICA-Keep-Alive mit den folgenden Einstellungen:

- **ICA-Keep-Alive - Timeout**: Gibt das Intervall (1-3600 Sekunden) für das Senden von ICA-Keep-Alive-Meldungen an. Konfigurieren Sie diese Option nicht, wenn die Netzwerksoftware inak-

tive Sitzungen schließen soll und unterbrochene Verbindungen in der Umgebung so selten sind, dass die Wiederverbindung mit Sitzungen nicht wichtig ist.

Die Standardeinstellung von 60 Sekunden bedeutet, dass alle 60 Sekunden ICA-Keep-Alive-Pakete an Benutzergeräte gesendet werden. Antwortet ein Benutzergerät nicht in 60 Sekunden, wird der Status der ICA-Verbindung auf "Getrennt"gesetzt.

- **ICA-Keep-Alives**: Sendet oder verhindert das Senden von ICA-Keep-Alive-Meldungen.

Workspace Control

Mit Workspace Control können Desktops und Anwendungen einem Benutzer von einem Gerät zum anderen folgen. Diese Roamingfähigkeit ermöglicht Benutzern den Zugriff auf alle Desktops oder offene Anwendungen von einem beliebigen Ort aus, ohne Neustart des Desktops oder der Anwendungen auf jedem einzelnen Gerät. Sie müssen sich lediglich anmelden. Mit Workspace Control kann das Pflegepersonal in einem Krankenhaus beispielsweise schnell an eine andere Arbeitsstation wechseln und nach der Anmeldung auf dieselben Anwendungen zugreifen. Bei entsprechender Konfiguration von Workspace Control können die Mitarbeiter die Verbindung zu mehreren Anwendungen auf einem Clientgerät trennen und die Verbindung zu denselben Anwendungen auf einem anderen Clientgerät wiederherstellen.

Workspace Control wirkt sich auf die folgenden Aktivitäten aus:

- **Anmelden:** Standardmäßig ermöglicht Workspace Control den Benutzern, die Verbindung mit allen ausgeführten Desktops und Anwendungen bei der Anmeldung automatisch wiederherzustellen, ohne sie erneut manuell zu öffnen. Mit Workspace Control können Benutzer getrennte Desktops oder Anwendungen öffnen sowie alle, die auf einem anderen Clientgerät aktiv sind. Beim Trennen der Verbindung mit einem Desktop bzw. einer Anwendung wird das Desktop bzw. die Anwendung weiterhin auf dem Server ausgeführt. Bei Benutzern im Roamingbetrieb, die einige Desktops oder Anwendungen auf einem Clientgerät ausführen müssen, während sie auf einem anderen Clientgerät eine Wiederverbindung zu einem Teil ihres Desktops bzw. ihrer Anwendungen durchführen möchten, können Sie das Wiederverbindungsverhalten bei der Anmeldung so konfigurieren, dass nur die Desktops bzw. Anwendungen geöffnet werden, die zuvor getrennt wurden.
- **Wiederverbinden:** Nach der Anmeldung am Server können die Benutzer eine Verbindung zu all ihren Desktops oder Anwendungen jederzeit wiederherstellen, indem Sie auf "Wiederverbinden"klicken. Beim Wiederverbinden werden standardmäßig sowohl getrennte Desktops oder Anwendungen geöffnet als auch alle aktiven Anwendungen, die derzeit auf einem anderen Clientgerät ausgeführt werden. Sie können die Wiederverbindung so konfigurieren, dass nur die Desktops oder Anwendungen geöffnet werden, deren Verbindung der Benutzer zuvor getrennt hat.

- **Abmelden:** Bei Benutzern, die Desktops oder Anwendungen über StoreFront öffnen, können Sie den Abmeldebefehl so konfigurieren, dass Benutzer entweder von StoreFront und allen aktiven Sitzungen gleichzeitig oder nur von StoreFront abgemeldet werden.
- **Verbindung wird getrennt:** Die Benutzer können die Verbindung mit allen ausgeführten Desktops und Anwendungen gleichzeitig trennen.

Workspace Control ist nur für Benutzer von Citrix Receiver verfügbar, die über eine Citrix StoreFront-Verbindung auf Desktops und Anwendungen zugreifen. Workspace Control ist standardmäßig für virtuelle Desktopsitzungen deaktiviert, für gehostete Anwendungen aber aktiviert. Die Sitzungsfreigabe zwischen veröffentlichten Desktops und veröffentlichten Anwendungen in diesen Desktops erfolgt nicht standardmäßig.

Benutzerrichtlinien, Clientlaufwerkzuordnungen und Druckerkonfigurationen ändern sich entsprechend, wenn ein Benutzer ein neues Clientgerät verwendet. Diese Richtlinien und Zuordnungen werden auf dem Clientgerät angewendet, auf dem der Client derzeit bei der Sitzung angemeldet ist. Wenn sich Pflegepersonal z. B. von einem Clientgerät in der Notaufnahme des Krankenhauses abmeldet und dann bei einer Arbeitsstation in der Röntgenabteilung anmeldet, gelten für die Sitzung die Richtlinien, Druckerzuordnungen und Clientlaufwerkzuordnungen der Röntgenabteilung, solange die Sitzung gestartet wird.

Sie können die den Benutzern angezeigten Drucker je nach Standort anpassen. Außerdem können Sie steuern, ob Benutzer auf lokalen Druckern drucken können, wie viel Bandbreite bei einer Remoteverbindung verwendet wird sowie andere Aspekte des Druckens.

Weitere Informationen zur Aktivierung und Konfiguration von Workspace Control für Benutzer finden Sie in der StoreFront-Dokumentation.

Sitzungsroaming

Standardmäßig wechseln Sitzungen zusammen mit dem Benutzer von Clientgerät zu Clientgerät. Wenn ein Benutzer eine Sitzung startet und dann mit einem anderen Gerät weiterarbeitet, wird die gleiche Sitzung verwendet und die Anwendungen stehen auf beiden Geräten zur Verfügung. Die Anwendungen folgen dem Benutzer unabhängig von dem Gerät und davon, ob aktuelle Sitzungen vorhanden sind. In vielen Fällen folgen auch Drucker und andere Ressourcen, die einer Anwendung zugewiesen sind.

Dieses Standardverhalten bietet viele Vorteile, ist aber nicht in allen Fällen ideal. Sie können das Sitzungsroaming mit dem PowerShell-SDK verhindern.

Beispiel 1: Ein Mitarbeiter eines Krankenhauses verwendet beim Ausfüllen eines Versicherungsformulars einen Desktop-PC und ein Tablet zum Anzeigen von Patientendaten.

- Bei aktiviertem Sitzungsroaming werden beide Anwendungen auf beiden Geräten angezeigt

(eine auf einem Gerät gestartete Anwendung ist auf allen Geräten zu sehen). Dies entspricht möglicherweise nicht den Sicherheitsanforderungen.
- Wenn das Sitzungsroaming deaktiviert ist, werden die Patientendaten nicht auf dem PC angezeigt und das Versicherungsformular nicht auf dem Tablet.

Beispiel 2: Ein Produktionsmanager startet eine Anwendung auf dem PC im Büro. Gerätename und Standort bestimmen, welche Drucker und anderen Ressourcen für die Sitzung verfügbar sind. Später nimmt er bei einer Besprechung in einem anderen Gebäude teil und muss etwas ausdrucken.

- Bei aktiviertem Sitzungsroaming kann er wahrscheinlich nicht auf die Drucker in der Nähe des Besprechungsraums zugreifen, da ihm durch den Anwendungsstart Drucker und Ressourcen für den Standort Büro zugewiesen wurden.
- Ist das Sitzungsroaming deaktiviert, wird bei der Anmeldung bei einem anderen Gerät (mit denselben Anmeldeinformationen) eine neue Sitzung gestartet und Drucker und Ressourcen in der Nähe werden verfügbar.

Konfigurieren des Sitzungsroamings

Zum Konfigurieren des Sitzungsroamings verwenden Sie die folgenden Anspruchsrichtlinienregel-Cmdlets mit der Eigenschaft "SessionReconnection". Optional können Sie auch die Eigenschaft "LeasingBehavior"festlegen. Weitere Informationen finden Sie weiter unten unter "Verbindungsleasing und Sitzungsroaming".

Desktopsitzungen:

Set-BrokerEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed | Disallowed

Anwendungssitzungen:

Set-BrokerAppEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed | Disallowed

<*value*> kann folgenden Wert annehmen:

- **Always**. Das Sitzungsroaming ist immer aktiviert, unabhängig vom Clientgerät und davon, ob die Sitzung verbunden oder getrennt ist. Dies ist der Standardwert.
- **DisconnectedOnly**: Eine Wiederverbindung erfolgt nur bei Sitzungen, die bereits getrennt sind. Andernfalls wird eine neue Sitzung gestartet. (Sitzungen können zwischen Clientgeräten wechseln, indem sie zunächst getrennt werden oder das Roaming für sie explizit mit Workspace Control durchgeführt wird.) Eine aktive verbundene Sitzung von einem anderen Clientgerät wird nie verwendet, stattdessen wird eine neue Sitzung gestartet.

- **SameEndpointOnly**: Der Benutzer erhält eine eigene Sitzung für jedes verwendete Clientgerät. Damit wird das Sitzungsroaming vollständig deaktiviert. Die Benutzer können eine Wiederverbindung nur auf dem Gerät vornehmen, das zuvor für die Sitzung verwendet wurde.

Die Eigenschaft "LeasingBehavior"wird weiter unten beschrieben.

Auswirkungen anderer Einstellungen

Das in den Anwendungseigenschaften einer Bereitstellungsgruppe über "Nur eine Anwendungsinstanz pro Benutzer zulassen"festgelegte Anwendungslimit hat Auswirkungen auf die Deaktivierung des Sitzungsroamings.

- Wenn Sie das Sitzungsroaming deaktivieren, deaktivieren auch die Option "Nur eine Anwendungsinstanz pro Benutzer zulassen".
- Wenn Sie die Option "Nur eine Anwendungsinstanz pro Benutzer zulassen"aktivieren, konfigurieren Sie keinen der beiden Werte, durch die neue Sitzungen auf neuen Geräten zugelassen werden.

Verbindungsleasing und Sitzungsroaming

Wenn Sie nicht mit dem Verbindungsleasing vertraut sind, lesen Sie den Artikel Verbindungsleasing.

Wenn ein Controller auf eine geleaste Verbindung schaltet, tritt für die Sitzungswiederverbindung wieder der Standardwert in Kraft, d. h. die Wiederverbindung erfolgt nur mit einer aktiven oder getrennten Sitzung für den Desktop bzw. die Anwendung.

Zur Gewährleistung zusätzlicher Sicherheit sollten Sie, wenn Sie für das Sitzungsroaming einen anderen als den Standardwert konfiguriert haben und mehrere Benutzer auf mehreren Geräten dieselben Anmeldeinformationen verwenden, das Verbindungsleasing für die Bereitstellungsgruppe, die das verwendete Benutzerkonto enthält, deaktivieren.

Warum? In diesem Szenario wird eine Sitzung auf allen Geräten gemeinsam verwendet. Das ist möglicherweise unerwünscht, z. B. wenn ein Benutzer vertrauliche Informationen anzeigt, die andere Benutzer, die sich mit denselben Anmeldeinformationen wieder verbinden, während der Controller im Leasingverbindungsmodus ausgeführt wird, nicht sehen sollen.

Durch Deaktivieren des Verbindungsleasings in der Anspruchsrichtlinie wird dies verhindert, d. h. Benutzer können die Sitzung anderer mit den gleichen Anmeldeinformationen angemeldeter Benutzer nicht sehen, selbst wenn der Controller im Leasingverbindungsmodus ausgeführt wird. Andere Anspruchsrichtlinien können bestehen bleiben; einzelne Benutzerkonten können das Verbindungsleasing über separate Ansprüche nutzen.

Zum Deaktivieren des Verbindungsleasings in einer Anspruchrichtlinie fügen Sie die Eigenschaft "LeasingBehavior Disallowed"dem Cmdlet der Anspruchsrichtlinie hinzu. Wenn Sie das

Verbindungsleasing deaktivieren, müssen Sie alle für die Anspruchsrichtlinie bereits erstellten und zwischengespeicherten Startleases manuell löschen. Andernfalls können sich die Benutzer nach wie vor wieder verbinden, wenn es zum Ausfall der Datenbank kommt.

Anmeldeintervall

Wenn eine virtuelle Maschine mit einem Desktop-VDA geschlossen wird, bevor die Anmeldung abgeschlossen ist, können Sie dem Prozess mehr Zeit zuteilen. Die Standardeinstellung in Version 7.6 und höher ist 180 Sekunden (die Standardeinstellung für Version 7.0-7.5 ist 90 Sekunden).

Legen Sie auf der Maschine (oder dem im Maschinenkatalog verwendeten Masterimage) folgenden Registrierungsschlüssel fest:

Schlüssel: HKLM\SOFTWARE\Citrix\PortICA

Wert: AutoLogonTimeout

Typ: DWORD

Geben Sie die Zeit als Dezimalwert in Sekunden ein, zulässig ist ein Wert von 0 bis 3600.

Wenn Sie ein Masterimage ändern, aktualisieren Sie den Katalog.

> **Hinweis:**
>
> Diese Einstellung gilt nur für VMs mit Desktop-VDAs, das Anmeldetimeout auf Server-VDAs wird von Microsoft gesteuert.

Verwenden der Suche in Studio

August 18, 2021

Verwenden Sie die Suchfunktion, um bestimmte Maschinen, Sitzungen, Maschinenkataloge, Anwendungen oder Bereitstellungsgruppen zu finden.

1. Wählen Sie im Studio-Navigationsbereich Suchen aus.

   Hinweis: Sie können mit dem Suchfeld der Registerkarten “Maschinenkataloge”oder “Bereitstellungsgruppen”keine Suche durchführen. Verwenden Sie den Suchknoten im Navigationsbereich.

   Zum Anzeigen weiterer Suchkriterien klicken Sie auf das Pluszeichen neben den Dropdownlisten. Klicken Sie zum Entfernen von Suchkriterien auf das Minuszeichen.

2. Geben Sie den Namen ein oder verwenden Sie die Dropdownliste, um eine andere Suchoption für das gesuchte Element auszuwählen.
3. Speichern Sie Ihre Suche, falls gewünscht, durch Wählen von Speichern unter. Die Suche wird in der Liste Gespeicherte Suchvorgänge angezeigt.

Sie können auch auf das Symbol "Suche erweitern"(doppelte nach unten gerichtete spitze Klammern) klicken, um eine Dropdownliste mit Sucheigenschaften anzuzeigen. Führen Sie eine erweiterte Suche durch, indem Sie einen Ausdruck anhand der Eigenschaften in der Dropdownliste zusammenstellen.

Tipps zur Verbesserung der Suche:

- Um zusätzliche Eigenschaften in die Anzeige zu integrieren, anhand derer Sie dann suchen und sortieren können, klicken Sie mit der rechten Maustaste auf eine Spalte und wählen Sie Spalten auswählen.
- Wählen Sie zum Suchen eines mit einer Maschine verbundenen Benutzergeräts Client (IP) und Ist und geben Sie die IP-Adresse des Geräts ein.
- Wenn Sie aktive Sitzungen suchen, verwenden Sie Sitzungszustand, Ist und Verbunden.
- Um alle Maschinen in einer Bereitstellungsgruppe aufzuführen, wählen Sie im Navigationsbereich Bereitstellungsgruppen, wählen Sie die Gruppe aus und wählen Sie dann im Aktionsbereich Maschinen anzeigen.

Tags

January 6, 2023

Einführung

Tags sind Zeichenfolgen zur Identifizierung von Elementen wie z. B. Maschinen, Anwendungen, Desktops, Bereitstellungsgruppen, Anwendungsgruppen und Richtlinien. Durch Erstellen und Hinzufügen von Tags können Sie festlegen, dass bestimmte Vorgänge nur an Elementen stattfinden, die ein spezifisches Tag haben.

- Anpassen der Suchanzeige in Studio

Wenn Sie beispielsweise nur Anwendungen anzeigen möchten, die für Testzwecke optimiert wurden, erstellen Sie ein Tag mit dem Namen "Test"und fügen es den Anwendungen hinzu. Sie können dann die Suche in Studio nach dem Tag "Test"filtern.

- Veröffentlichen von Anwendungen aus einer Anwendungsgruppe oder von bestimmten Desktops aus einer Bereitstellungsgruppe unter ausschließlicher Berücksichtigung einer Teilmenge der Maschinen in den ausgewählten Bereitstellungsgruppen Dies wird als *Tagbeschränkung* bezeichnet.

Mit Tagbeschränkungen können Sie Ihre vorhandenen Maschinen für mehrere Veröffentlichungstasks verwenden und sparen so die Kosten für die Bereitstellung und Verwaltung zusätzlicher Maschinen. Die Verwendung von Tagbeschränkungen kann man sich als Unterteilung (oder Partitionierung) der Maschinen in einer Bereitstellungsgruppe vorstellen. Die Funktionsweise von Tagbeschränkungen ähnelt der von Workergruppen in XenApp-Releases vor 7.x, ist mit dieser jedoch nicht identisch.

Anwendungsgruppen und Desktops mit Tagbeschränkungen können auch zur Isolierung von Maschinengruppen in einer Bereitstellungsgruppe zur Problembehandlung nützlich sein.

Weitere Informationen zur Verwendung von Tagbeschränkungen finden Sie weiter unten.

- Planen regelmäßiger Neustarts für eine Teilmenge der Maschinen in einer Bereitstellungsgruppe

Unter Einsatz einer Tagbeschränkung für Maschinen können Sie neue PowerShell-Cmdlets zum Konfigurieren mehrerer Neustart-Zeitpläne für Teilmengen von Maschinen in einer Bereitstellungsgruppe verwenden. Beispiele und weitere Informationen finden Sie unter "Erstellen mehrerer Neustartzeitpläne für Maschinen in einer Bereitstellungsgruppe"im Artikel Verwalten von Bereitstellungsgruppen.

- Zielgerichtete Anwendung (Zuweisung) von Citrix Richtlinien auf eine Teilmenge von Maschinen in Bereitstellungsgruppen, Bereitstellungsgruppentypen oder Organisationseinheiten, die ein bestimmtes Tag haben oder nicht haben

Wenn Sie beispielsweise eine Citrix Richtlinie nur auf leistungsstarke Arbeitsstationen anwenden möchten, fügen Sie diesen Maschinen ein Tag mit dem Namen "Hohe Leistung"hinzu. Wählen Sie dann auf der Seite **Richtlinie zuweisen** des Assistenten zum Erstellen von Richtlinien dieses Tag und das Kontrollkästchen **Aktivieren**. Sie können auch einer Bereitstellungsgruppe ein Tag hinzufügen und eine Citrix Richtlinie auf die Gruppe anwenden. Weitere Informationen finden Sie unter Erstellen von Richtlinien. (Hinweis: Die Studio-Benutzeroberfläche zum Hinzufügen eines Tags zu einer Maschine hat sich seit Veröffentlichung des Blogbeitrags geändert.)

Sie können Tags auf folgende Elemente anwenden:

- Maschinen
- Anwendungen
- Bereitstellungsgruppen
- Anwendungsgruppen

Sie können Tagbeschränkungen beim Erstellen und Bearbeiten der folgenden Elemente in Studio konfigurieren:

- Desktops in einer freigegebenen Bereitstellungsgruppe
- Anwendungsgruppen

Tagbeschränkungen für Desktops oder Anwendungsgruppen

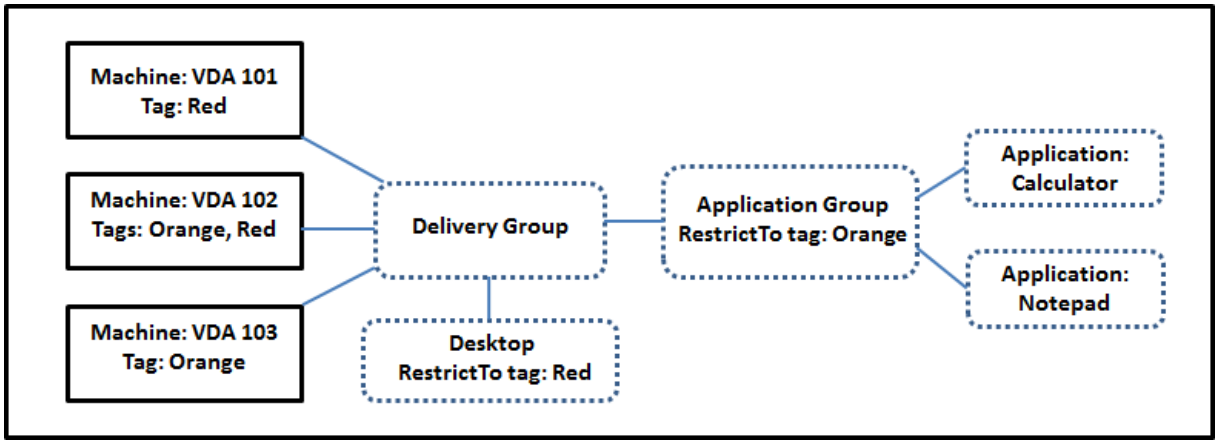
Das Erstellen von Tagbeschränkungen umfasst mehrere Schritte:

- Erstellen Sie das Tag und fügen Sie es Maschinen hinzu.
- Erstellen oder bearbeiten Sie eine Gruppe mit der Tagbeschränkung (d. h. beschränken Sie Starts auf Maschinen mit Tag "x").

Tagbeschränkungen erweitern die Maschinenauswahl durch den Broker. Der Broker wählt Maschinen aus Bereitstellungsgruppen auf der Basis der Zugriffsrichtlinie, konfigurierten Benutzerlisten, der Zonenpräferenz, der Startbereitschaft und, falls vorhanden, der Tagbeschränkung aus. Bei Anwendungen berücksichtigt der Broker Bereitstellungsgruppen in der Reihenfolge der Priorität unter Anwendung der gleichen Maschinenauswahlregeln für jede Bereitstellungsgruppe.

Beispiel 1

Dieses Beispiel ist eine einfache Anordnung mit Tagbeschränkungen, die festlegen, welche Maschinen für bestimmte Desktop- und Anwendungsstarts in Betracht gezogen werden. Die Site hat eine freigegebene Bereitstellungsgruppe, einen veröffentlichten Desktop und eine Anwendungsgruppe mit zwei Anwendungen.



- Allen drei Maschinen (VDA 101–103) wurden Tags hinzugefügt.
- Der Desktop in der Bereitstellungsgruppe wurde mit der Tagbeschränkung "Red"erstellt und kann daher nur auf Maschinen in der Bereitstellungsgruppe gestartet werden, die das Tag "Red" haben: VDA 101 und 102.

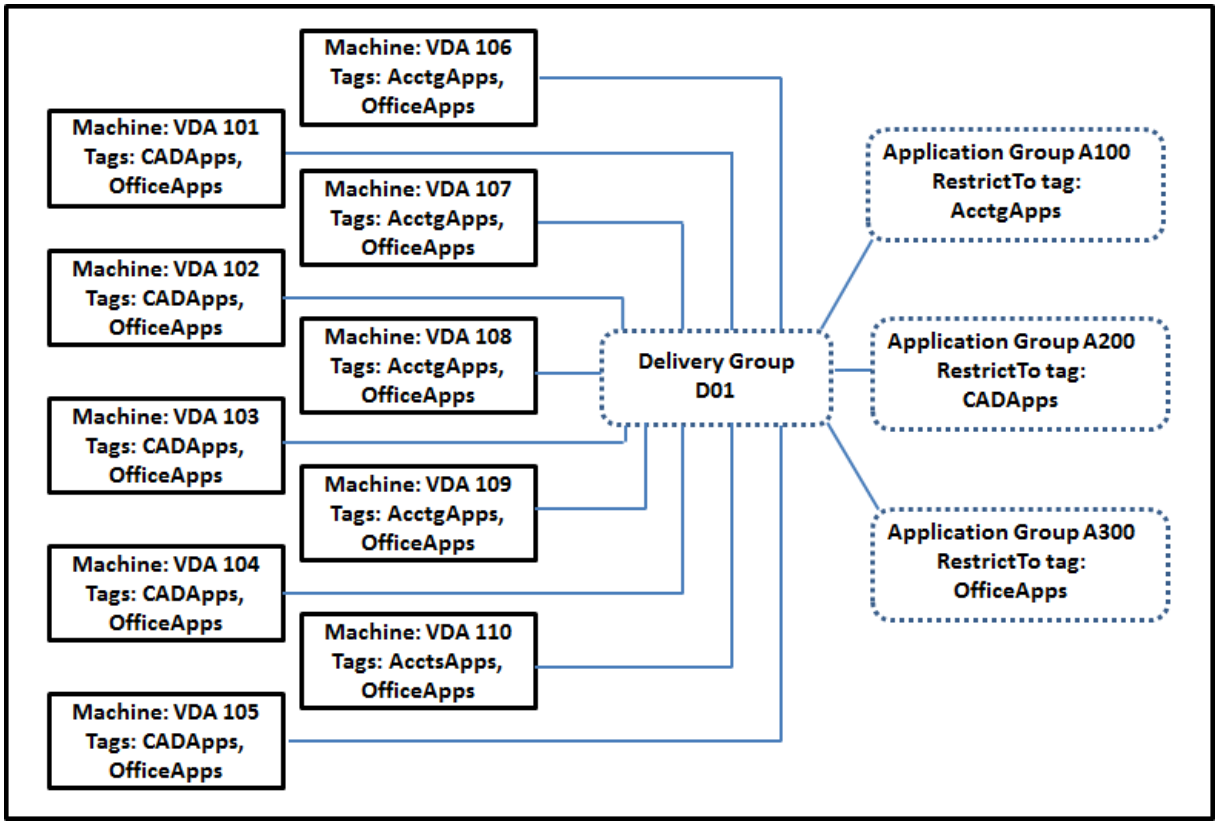
- Die Anwendungsgruppe wurde mit der Tagbeschränkung "Orange"erstellt, sodass alle ihre Anwendungen (Rechner und Editor) nur auf Maschinen gestartet werden können, die das Tag "Orange"haben: VDA 102 und 103.

VDA 102 hat beide Tags (Rot und Orange) und kann daher für das Starten von Anwendungen und Desktops verwendet werden.

Beispiel 2

Dieses Beispiel enthält mehrere Anwendungsgruppen mit Tagbeschränkungen. Auf diese Weise können mehr Anwendungen mit weniger Maschinen als bei bloßer Verwendung von Bereitstellungsgruppen bereitgestellt werden.

(Im Abschnitt "Konfigurieren von Beispiel 2"werden die Schritte zum Erstellen und Anwenden der Tags und zum Konfigurieren der Tagbeschränkungen erläutert.)



In diesem Beispiel hat die Umgebung zehn Maschinen (VDA 101–110), eine Bereitstellungsgruppe (D01) und drei Anwendungsgruppen (A100, A200, A300). Durch Anwenden von Tags auf jede Maschine und Festlegen von Tagbeschränkungen beim Erstellen jeder Anwendungsgruppe wird Folgendes erreicht:

- Die Benutzer der Gruppe "Accounting"können auf die benötigten Anwendungen auf fünf Maschinen (101–105) zugreifen.

- CAD-Designer können auf die benötigten Anwendungen auf fünf Maschinen (106–110) zugreifen.
- Benutzer, die Office-Anwendungen benötigen, können auf Office-Anwendungen auf zehn Maschinen (VDA 101–110) zugreifen.

Es werden nur zehn Maschinen und nur eine Bereitstellungsgruppe verwendet. Bei ausschließlicher Verwendung von Bereitstellungsgruppen ohne Anwendungsgruppen würden doppelt so viele Maschinen benötigt, da jede Maschine nur zu einer Bereitstellungsgruppe gehören kann.

Verwalten von Tags und Tagbeschränkungen

Zum Erstellen (Anwenden), Bearbeiten und Löschen von Tags für ausgewählte Elemente wird die Aktion **Tags verwalten** in Studio verwendet.

Ausnahme: Tags für Richtlinienzuweisungen werden über die Aktion **Tags verwalten** in Studio erstellt, bearbeitet und gelöscht, angewendet (zugewiesen) werden sie jedoch, wenn Sie die Richtlinie erstellen (siehe Erstellen von Richtlinien).

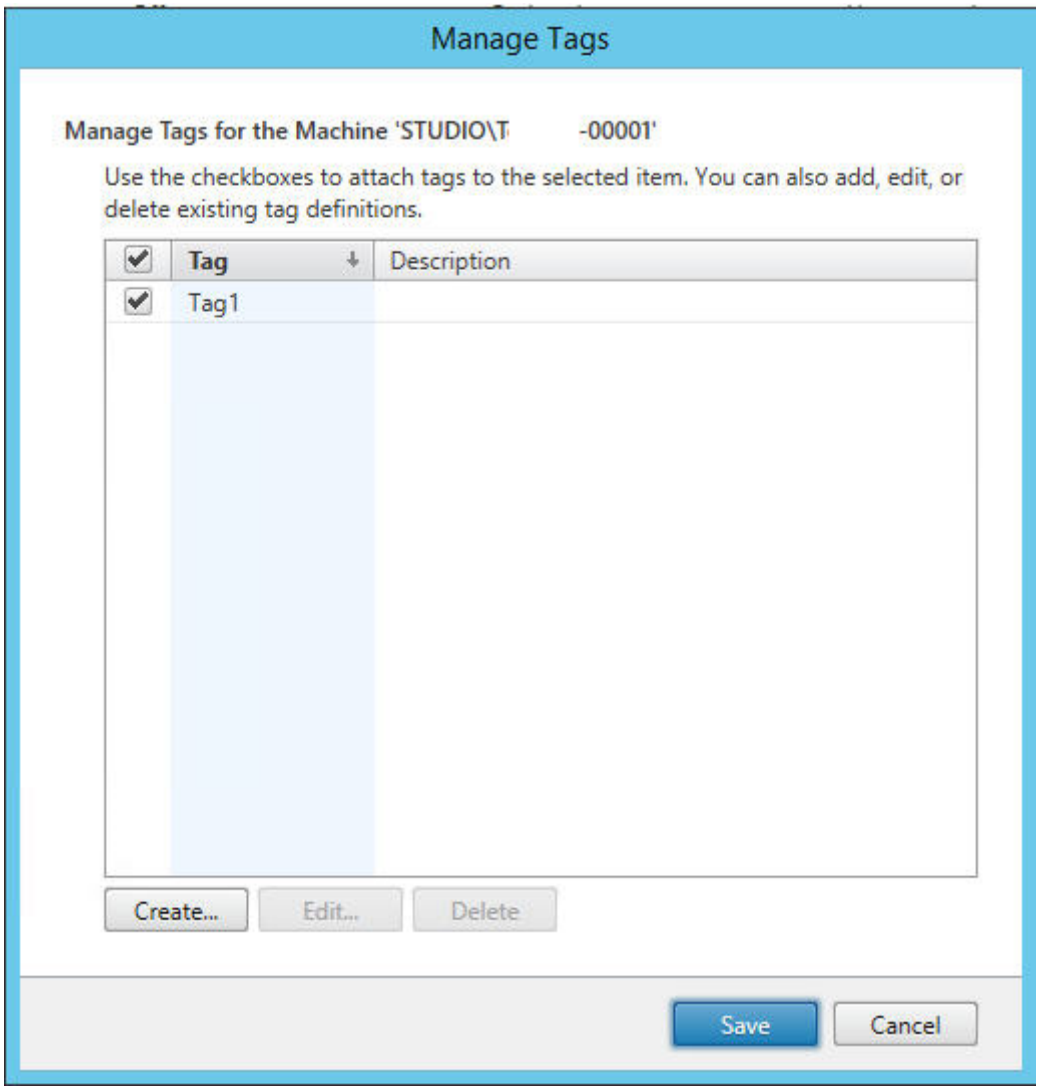
Tagbeschränkungen konfigurieren Sie beim Erstellen oder Bearbeiten von Desktops in Bereitstellungsgruppen und beim Erstellen und Bearbeiten von Anwendungsgruppen. Weitere Informationen zum Erstellen und Bearbeiten von Gruppen finden Sie in den folgenden Artikeln:

- Erstellen von Bereitstellungsgruppen
- Verwalten von Bereitstellungsgruppen
- Erstellen von Anwendungsgruppen
- Verwalten von Anwendungsgruppen

Verwenden der Dialogfelder “Tags verwalten”in Studio

Wählen Sie in Studio die Elemente aus, auf die Sie ein Tag anwenden möchten (eine oder mehrere Maschinen oder Anwendungen, einen Desktop, eine Bereitstellungsgruppe oder eine Anwendungsgruppe), und wählen Sie dann im Aktionsbereich **Tags verwalten**. Das Dialogfeld Tags verwalten enthält alle in der Site erstellten Tags und nicht nur diejenigen, die für die ausgewählten Elemente erstellt wurden.

- Ein Kontrollkästchen mit Häkchen kennzeichnet Tags, die den ausgewählten Elementen bereits hinzugefügt wurden. (In der Abbildung unten hat die ausgewählte Maschine das Tag “Tag1”.)
- Wenn Sie mehrere Elemente auswählen, wird durch ein Kontrollkästchen mit einem Strich angezeigt, wenn das Tag einigen (aber nicht allen) Elementen hinzugefügt wurde.



Die folgenden Aktionen stehen im Dialogfeld Tags verwalten zur Verfügung. Lesen Sie in diesem Zusammenhang unbedingt den Abschnitt "Hinweise zum Hinzufügen, Entfernen oder Löschen von Tags von Elementen".

Tags erstellen:

Klicken Sie auf **Erstellen**. Geben Sie einen Namen und eine Beschreibung ein. Tagnamen müssen eindeutig sein, die Groß- und Kleinschreibung spielt keine Rolle. Klicken Sie dann auf **OK**. (Durch das Erstellen eines Tags wird es nicht automatisch auf Elemente angewendet, die Sie ausgewählt haben. Verwenden Sie zum Anwenden die Kontrollkästchen.)

Hinzufügen von Tags:

Aktivieren Sie die Kontrollkästchen neben den Tagnamen. **Hinweis:** Wenn Sie mehrere Elemente ausgewählt haben, das Kontrollkästchen neben einem Tag einen Strich enthält (d. h. das Tag wurde bereits auf einige, jedoch nicht alle ausgewählten Elemente angewendet), und Sie das Kontrollkästchen mit einem Häkchen versehen, wirkt sich dies auf alle ausgewählten Maschinen aus.

Wenn Sie versuchen, ein als Einschränkung in einer Anwendungsgruppe verwendetes Tag einer oder mehreren Maschinen hinzuzufügen, werden Sie gewarnt, dass die Aktion dazu führen kann, dass die Maschinen für Starts verfügbar gemacht werden. Wenn dies beabsichtigt ist, fahren Sie fort.

Entfernen von Tags:

Deaktivieren Sie die Kontrollkästchen neben den entsprechenden Tagnamen. **Hinweis:** Wenn Sie mehrere Elemente ausgewählt haben, das Kontrollkästchen neben einem Tag einen Strich enthält (d. h. das Tag wurde bereits auf einige, jedoch nicht alle ausgewählten Elemente angewendet), und Sie das Kontrollkästchen deaktivieren, wird das Tag von allen ausgewählten Maschinen entfernt.

Wenn Sie versuchen, ein Tag von einer Maschine zu entfernen, für die es als Einschränkung verwendet wird, wird eine Warnmeldung angezeigt, die angibt, dass diese Aktion sich auf die für Starts infrage kommenden Maschinen auswirken kann. Wenn dies beabsichtigt ist, fahren Sie fort.

Bearbeiten von Tags:

Wählen Sie das Tag und klicken Sie dann auf **Bearbeiten**. Ändern Sie den Namen und/oder die Beschreibung. Sie können immer nur ein Tag bearbeiten.

Löschen von Tags:

Wählen Sie die Tags aus und klicken Sie auf **Löschen**. Im Dialogfeld Tag löschen wird angezeigt, von wie vielen Elementen die ausgewählten Tags verwendet werden (z. B. "2 Maschinen"). Durch Klicken auf ein Element können Sie weitere Informationen aufrufen. Wenn Sie beispielsweise auf "2 Maschinen"klicken, werden die Namen der beiden Maschinen angezeigt, auf die das Tag angewendet wird. Bestätigen Sie, dass Sie die Tags löschen möchten.

Sie können mit Studio keine Tags löschen, die als Einschränkung verwendet werden. Sie müssen zuerst die Anwendungsgruppe bearbeiten und die Tagbeschränkung entfernen oder ein anderes Tag auswählen.

Wenn Sie im Dialogfeld "Tags verwalten"fertig sind, klicken Sie auf **Speichern**.

Tipp: Um festzustellen, ob auf eine Maschine Tags angewendet werden, gehen Sie folgendermaßen vor:

Wählen Sie im Navigationsbereich **Bereitstellungsgruppen** aus. Wählen Sie im mittleren Bereich eine Bereitstellungsgruppe und wählen Sie dann im Aktionsbereich **Maschinen anzeigen**. Wählen Sie im mittleren Bereich eine Maschine und dann im Bereich darunter die Registerkarte "Tags".

Tagbeschränkungen verwalten

Das Verfahren zum Konfigurieren von Tagbeschränkungen besteht aus mehreren Schritten. Zunächst erstellen das Tag und wenden es auf Maschinen an. Anschließend fügen Sie der Anwendungsgruppe oder dem Desktop die Einschränkung hinzu.

Tag erstellen und anwenden:

Erstellen Sie mithilfe des Dialogfelds **Tags verwalten** das Tag und wenden Sie es dann auf die Maschinen an, für die die Beschränkung gelten soll (siehe weiter oben).

Tagbeschränkung einer Anwendungsgruppe hinzufügen:

Erstellen oder bearbeiten Sie die Anwendungsgruppe. Wählen Sie auf der Seite "Bereitstellungsgruppen"**Starts auf Maschinen mit Tag beschränken** und dann aus der Dropdownliste das Tag.

Tagbeschränkung für eine Anwendungsgruppe ändern/entfernen:

Bearbeiten Sie die Gruppe. Wählen Sie auf der Seite "Bereitstellungsgruppen"ein anderes Tag aus der Dropdownliste oder entfernen Sie die Tagbeschränkung vollständig durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.

Tagbeschränkung einem Desktop hinzufügen:

Erstellen oder bearbeiten Sie eine Bereitstellungsgruppe. Klicken Sie auf der Seite "Desktops"auf **Hinzufügen** oder **Bearbeiten**. Wählen Sie **Starts auf Maschinen mit Tag beschränken** und dann aus der Dropdownliste das Tag.

Ändern/Entfernen von Tagbeschränkung für eine Bereitstellungsgruppe:

Bearbeiten Sie die Gruppe. Klicken Sie auf der Seite "Desktops"auf **Bearbeiten**. Wählen Sie in dem Dialogfeld ein anderes Tag aus der Dropdownliste oder entfernen Sie die Tagbeschränkung vollständig durch Deaktivieren der Option **Starts auf Maschinen mit Tag beschränken**.

Hinweise zum Hinzufügen, Entfernen oder Löschen von Tags von Elementen

Tags können zu verschiedenen Zwecken auf Elemente angewendet werden. Das Hinzufügen, Entfernen und Löschen eines Tags kann daher ungewollte Auswirkungen haben. Sie können ein Tag dazu verwenden, die Anzeige von Maschinen im Studio-Suchfeld zu sortieren. Sie können dasselbe Tag beim Konfigurieren einer Anwendungsgruppe oder eines Desktops als Einschränkung verwenden, um die beim Starten des Desktops berücksichtigten Maschinen auf diejenigen zu beschränken, die das Tag haben.

Wenn Sie versuchen, ein Tag einer Maschine hinzuzufügen, nachdem Sie es als Tagbeschränkung für einen Desktop oder eine Anwendungsgruppe konfiguriert haben, werden Sie von Studio gewarnt, dass die Maschine durch das Hinzufügen des Tags zum Starten zusätzlicher Anwendungen oder Desktops verfügbar gemacht werden könnte. Wenn dies beabsichtigt ist, fahren Sie fort. Fall nicht, können Sie den Vorgang abbrechen.

Angenommen, Sie erstellen eine Anwendungsgruppe mit der Tagbeschränkung "Rot". Später fügen Sie der von der Anwendungsgruppe verwendeten Bereitstellungsgruppe mehrere Maschinen hinzu. Wenn Sie versuchen, das Tag "Rot"den Maschinen hinzuzufügen, zeigt Studio folgende Meldung an:

Das Tag "Rot"dient als Beschränkung auf folgende Anwendungsgruppen. Durch das Hinzufügen des Tags werden die ausgewählten Maschinen möglicherweise für den Start von Anwendungen in dieser Anwendungsgruppe verfügbar gemacht. Sie können das Hinzufügen des Tags zu den zusätzlichen Maschinen dann bestätigen oder abbrechen.

Wenn ein Tag in einer Anwendungsgruppe zum Beschränken von Starts verwendet wird, zeigt Studio eine Warnung an, dass Sie es erst löschen können, wenn Sie es durch Bearbeiten der Gruppe als Beschränkung entfernt haben. (Wenn Sie in einer Anwendungsgruppe als Beschränkung verwendete Tags löschen dürften, könnte das dazu führen, dass Anwendungen auf allen Maschinen in den der Anwendungsgruppe zugewiesenen Bereitstellungsgruppen gestartet werden könnten). Das Löschen ist auch nicht möglich, wenn ein Tag als Beschränkung für Desktopstarts verwendet wird. Sobald Sie die Tagbeschränkung von der Anwendungsgruppe oder dem Desktop in der Bereitstellungsgruppe entfernt haben, können Sie das Tag löschen.

Nicht alle Maschinen haben unbedingt den gleichen Satz Anwendungen. Ein Benutzer kann mehreren Anwendungsgruppen mit unterschiedlichen Tagbeschränkungen und verschiedenen oder einander überlagernden Maschinengruppen aus Bereitstellungsgruppen angehören. Die folgende Tabelle enthält Informationen dazu, welche Maschinen für einen Start berücksichtigt werden.

Anwendung gehört zu	Für Starts berücksichtigte Maschinen in den ausgewählten Bereitstellungsgruppen
Einer Anwendungsgruppe ohne Tagbeschränkung	Beliebige Maschinen
Einer Anwendungsgruppe mit Tagbeschränkung A	Maschinen mit Tag A
Zwei Anwendungsgruppen, die eine mit Tagbeschränkung A, die zweite mit Tagbeschränkung B	Maschinen mit Tag A und B; sind keine solchen verfügbar, Maschinen mit Tag A oder Tag B
Zwei Anwendungsgruppen, die eine mit Tagbeschränkung A, die zweite ohne Tagbeschränkung	Maschinen mit Tag A; sind keine solchen verfügbar, beliebige Maschinen

Wenn Sie eine Tagbeschränkung in einem Neustartzeitplan für Maschinen verwenden, treten Änderungen an der Anwendung von Tags bzw. an Tagbeschränkungen beim nächsten Neustartzyklus in Kraft. Auf Neustartzyklen, die während der Durchführung von Änderungen laufen, haben diese keine Auswirkungen. (Weitere Informationen finden Sie im Artikel "Verwalten von Bereitstellungsgruppen").

Konfigurieren von Beispiel 2

Nachfolgend wird erläutert, wie die im zweiten Beispiel oben gezeigten Tags erstellt und angewendet und die Tagbeschränkungen für die Anwendungsgruppen konfiguriert werden.

Die VDAs und Anwendungen wurden bereits auf den Maschinen installiert und die Bereitstellungsgruppe wurde erstellt.

Tags erstellen und auf Maschinen anwenden

1. Wählen Sie in Studio die Bereitstellungsgruppe "D01"und im Aktionsbereich **Maschinen anzeigen**.
2. Wählen Sie die Maschinen VDA 101–105 und dann im Aktionsbereich **Tags verwalten**.
3. Klicken Sie im Dialogfeld "Tags verwalten"auf **Erstellen** und erstellen Sie ein Tag mit dem Namen "CADApps". Klicken Sie auf **OK**.
4. Klicken Sie erneut auf **Erstellen** und erstellen Sie ein Tag namens "OfficeApps". Klicken Sie auf **OK**.
5. Fügen Sie im Dialogfeld "Tags verwalten"die neu erstellten Tags den ausgewählten Maschinen hinzu, indem Sie die Kontrollkästchen neben den Tagnamen ("CADApps"und "OfficeApps") aktivieren, und schließen Sie das Dialogfeld.
6. Wählen Sie die Bereitstellungsgruppe "D01"und dann im Aktionsbereich **Maschinen anzeigen**.
7. Wählen Sie die Maschinen VDA 106–110 und dann im Aktionsbereich **Tags verwalten**.
8. Klicken Sie im Dialogfeld "Tags verwalten"auf **Erstellen** und erstellen Sie ein Tag mit dem Namen "AcctgApps". Klicken Sie auf **OK**.
9. Fügen Sie die neu erstellten Tags "AcctgApps"und "OfficeApps"den ausgewählten Maschinen hinzu, indem Sie auf die Kontrollkästchen neben den Tagnamen klicken, und schließen Sie das Dialogfeld.

Anwendungsgruppen mit Tagbeschränkungen erstellen

1. Wählen Sie im Studio-Navigationsbereich **Anwendungen** und im Aktionsbereich **Anwendungsgruppe erstellen**. Der Assistent zum Erstellen einer Anwendungsgruppe wird angezeigt.
2. Wählen Sie auf der Seite **Bereitstellungsgruppen** des Assistenten die Bereitstellungsgruppe "D01". Wählen Sie **Starts auf Maschinen mit Tag beschränken** und wählen Sie dann das Tag "AcctgApps"aus der Dropdownliste aus.
3. Füllen Sie die restlichen Seiten des Assistenten unter Angabe der Benutzer und Anwendungen des Buchhaltungsteams aus. (Wählen Sie beim Hinzufügen der Anwendung als Quelle "Vom Startmenü", damit die Anwendung auf den Maschinen mit dem Tag "AcctgApps"gesucht wird.) Geben Sie auf der Seite **Zusammenfassung** als Namen für die Gruppe "A100"ein.
4. Wiederholen Sie diese Schritte zum Erstellen der Anwendungsgruppe A200, wobei Sie Maschinen mit dem Tag "CADApps"sowie die entsprechenden Benutzer und Anwendungen angeben.
5. Wiederholen Sie diese Schritte zum Erstellen der Anwendungsgruppe A300, wobei Sie Maschinen mit dem Tag "OfficeApps"sowie die entsprechenden Benutzer und Anwendungen angeben.

Weitere Informationen

Blogbeitrag: How to assign desktops to specific servers.

Unterstützung für IPv4/IPv6

August 18, 2021

Dieses Release unterstützt reines IPv4, reines IPv6 und Bereitstellungen mit dualem Stapel, bei denen überlappende IPv4- und IPv6-Netzwerke verwendet werden.

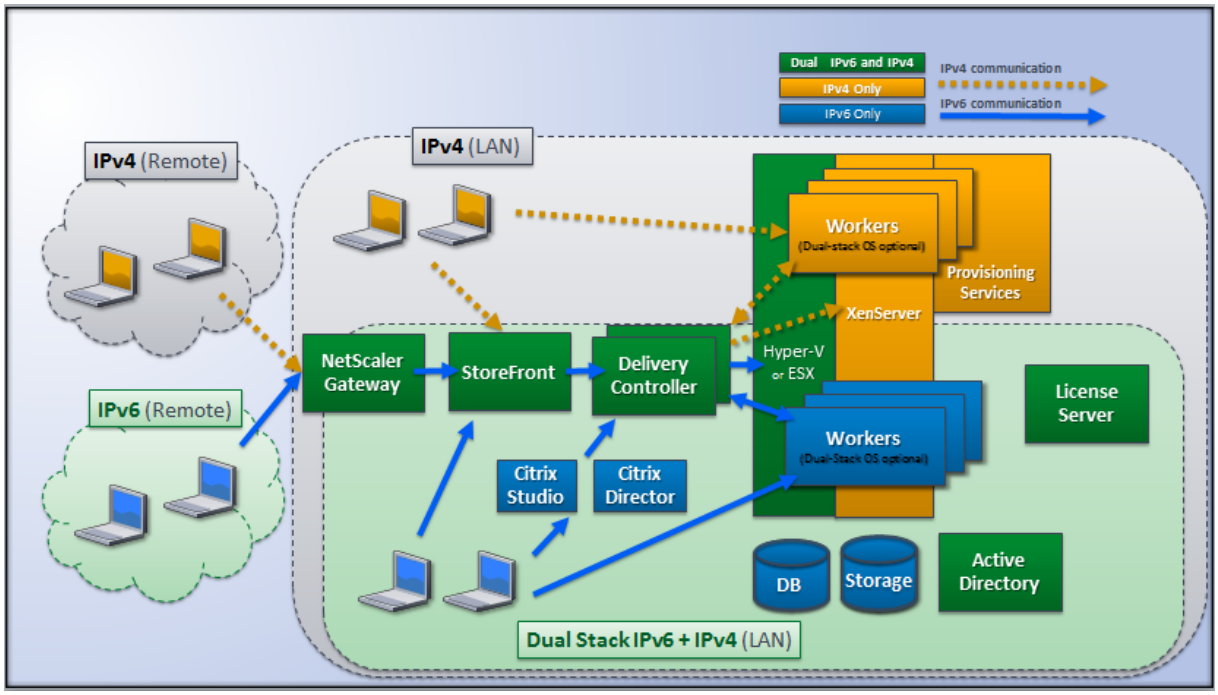
Die IPv6-Kommunikation wird mit zwei verbindungsspezifischen Citrix Richtlinieneinstellungen für Virtual Delivery Agent (VDA) gesteuert:

- Die primäre Einstellung erzwingt die Verwendung von IPv6: Nur IPv6-Controllerregistrierung verwenden.
- Die abhängige Einstellung definiert eine IPv6-Netzwerkmaske: IPv6-Netzwerkmaske für Controllerregistrierung.

Wenn Nur IPv6-Controllerregistrierung verwenden aktiviert ist, erfolgt die VDA-Registrierung bei einem Delivery Controller für eingehende Verbindungen über eine IPv6-Adresse.

IPv4-/IPv6-Bereitstellung mit dualem Stapel

Die folgende Abbildung zeigt eine IPv4-/IPv6-Bereitstellung mit dualem Stapel. In diesem Szenario ist ein Worker ein auf einem Hypervisor oder auf einer physischen Maschine installierter VDA, der primär zum Aktivieren von Verbindungen für Anwendungen und Desktops verwendet wird. Komponenten, die für den Parallelbetrieb von IPv6 und IPv4 ausgelegt sind, werden auf Betriebssystemen ausgeführt, die Tunneling oder Dual Protocol-Software nutzen.



Diese Citrix Produkte, Komponenten und Features unterstützen nur IPv4:

- Provisioning Services
- XenServer Version 6.x
- Nicht über die Richtlinieneinstellung **Nur IPv6-Controllerregistrierung verwenden** gesteuerte VDAs
- XenApp-Versionen vor 7.5, XenDesktop-Versionen vor 7 und Director

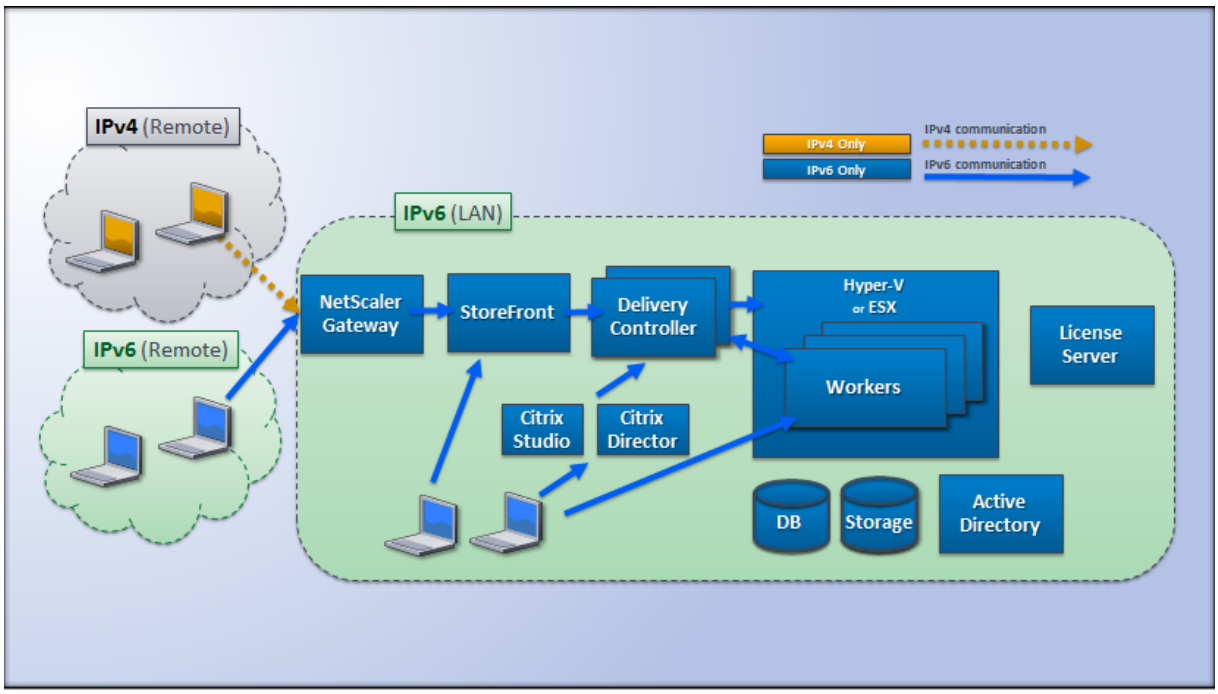
In dieser Bereitstellung gilt:

- Wenn ein Team häufig ein IPv6-Netzwerk verwendet und der Administrator die Nutzung von IPv6-Datenverkehr wünscht, veröffentlicht der Administrator IPv6-Desktops und -Anwendungen für die Benutzer auf der Basis eines Workerimages oder einer Organisationseinheit, für das bzw. die die primäre IPv6-Richtlinieneinstellung (Nur IPv6-Controllerregistrierung verwenden) aktiviert ist.
- Wenn ein Team häufig ein IPv4-Netzwerk verwendet, veröffentlicht der Administrator IPv4-Desktops und -Anwendungen für die Benutzer auf der Basis eines Workerimages oder einer Organisationseinheit, für das bzw. die die primäre IPv6-Richtlinieneinstellung deaktiviert ist (d. h. Nur IPv6-Controllerregistrierung verwenden ist deaktiviert = Standardeinstellung).

Reine IPv6-Bereitstellung

Die folgende Abbildung zeigt eine reine IPv6-Bereitstellung. Für dieses Szenario gilt:

- Die Komponenten werden auf Betriebssystemen ausgeführt, die ein IPv6-Netzwerk unterstützen.
- Die primäre Citrix Richtlinieneinstellung (Nur IPv6-Controllerregistrierung verwenden) ist für alle VDAs aktiviert; sie müssen sich beim Controller mit einer IPv6-Adresse registrieren.



Richtlinieneinstellungen für IPv6

Bei reiner IPv6-Implementierung bzw. Implementierung von IPv4/IPv6 mit dualem Stapel sind zwei Citrix Richtlinieneinstellungen relevant. Konfigurieren Sie die folgenden verbindungsbezogenen Einstellungen:

- **Nur IPv6 Controllerregistrierung verwenden:** steuert das Adressformat, mit dem der Virtual Delivery Agent (VDA) beim Delivery Controller registriert wird. Standard = deaktiviert
  - Wenn der VDA mit dem Controller kommuniziert, wird eine IPv6-Adresse verwendet, deren Auswahl folgender Reihenfolge unterliegt: globale IP-Adresse, Unique Local Address (ULA), Link-Local-Adresse (nur wenn keine anderen IPv6-Adressen verfügbar sind).
  - Ist die Einstellung deaktiviert, wird der VDA mit der IPv4-Adresse der Maschine für die Kommunikation beim Controller registriert.
- **IPv6-Netzwerkmaske für Controllerregistrierung:** Eine Maschine kann über mehrere IPv6-Adressen verfügen. Mit dieser Richtlinieneinstellung können Administratoren den VDA auf ein bevorzugtes Subnetz beschränken (anstelle einer globalen IP, sofern registriert). Mit dieser Einstellung wird das Netzwerk festgelegt, in dem der VDA registriert wird: Der VDA wird nur bei

der ersten Adresse registriert, die mit der angegebenen Netzwerkmaske übereinstimmt. Diese Einstellung ist nur gültig, wenn die Richtlinieneinstellung Nur IPv6-Controllerregistrierung verwenden aktiviert ist. Standard = leere Zeichenfolge

Wichtig: Die Verwendung von IPv4 oder IPv6 durch einen VDA wird ausschließlich über diese Richtlinieneinstellungen gesteuert. Das bedeutet, um die IPv6-Adressierung nutzen zu können, muss der VDA von einer Citrix Richtlinie gesteuert werden, bei der die Einstellung
Nur IPv6-Controllerregistrierung verwenden aktiviert ist.

Überlegungen zur Bereitstellung

Wenn Ihre Umgebung sowohl IPv4- und IPv6-Netzwerke umfasst, benötigen Sie separate Bereitstellungsgruppenkonfigurationen für IPv4-exklusive Clients und für die Clients, die Zugriff auf das IPv6-Netzwerk haben. Verwenden Sie ggf. Namen, die manuelle Active Directory-Gruppenzuweisung oder SmartAccess-Filter zur Unterscheidung der Benutzer.

Die Wiederverbindung mit einer Sitzung kann fehlschlagen, wenn die Verbindung auf einem IPv6-Netzwerk gestartet wird und dann Wiederverbindungsversuche von einem internen Client erfolgen, der nur IPv4-Zugriff hat.

Benutzerprofile

June 7, 2022

Standardmäßig wird bei der Installation des Virtual Delivery Agents die Citrix Profilverwaltung ohne Benutzereingriff auf Masterimages installiert. Sie muss jedoch nicht als Profillösung verwendet werden.

Mit XenApp- und XenDesktop-Richtlinien können Sie auf die Maschinen jeder Bereitstellungsgruppe ein anderes Profilverhalten anwenden, um die Profile an unterschiedliche Benutzerbedürfnisse anzupassen. Beispiel: Eine Bereitstellungsgruppe erfordert möglicherweise verbindliche Citrix Profile, deren Vorlage an einem Netzwerkspeicherort gespeichert ist, aber eine andere Bereitstellungsgruppe erfordert möglicherweise Citrix Roamingprofile an einem anderen Speicherort mit mehreren umgeleiteten Ordnern.

- Wenn andere Administratoren in Ihrer Organisation für XenApp- und XenDesktop-Richtlinien zuständig sind, stimmen Sie gemeinsam ab, welche profilbezogenen Richtlinien für die Bereitstellungsgruppen gelten.
- Richtlinien zur Profilverwaltung können auch in der Gruppenrichtlinie sowie in der INI-Datei der Profilverwaltung und lokal auf einzelnen virtuellen Maschinen festgelegt werden. Diese

verschiedenen Methoden zum Definieren des Profilverhaltens werden in der folgenden Reihenfolge gelesen:

1. Gruppenrichtlinie (ADM- oder ADMX-Dateien)
2. XenApp- und XenDesktop-Richtlinien im Knoten "Richtlinie"
3. Lokale Richtlinien auf der virtuellen Maschine, zu der der Benutzer eine Verbindung herstellt
4. INI-Datei der Profilverwaltung

Beispiel: Wenn Sie die gleiche Richtlinie sowohl in der Gruppenrichtlinie als auch im Knoten "Richtlinie"konfigurieren, wird die Richtlinieneinstellung in der Gruppenrichtlinie vom System gelesen und die XenApp- bzw. XenDesktop-Richtlinieneinstellung wird ignoriert.

Unabhängig davon, für welche Lösung Sie sich entscheiden, können Director-Administratoren auf Diagnoseinformationen zugreifen und Problembehandlung für Benutzerprofile durchführen. Weitere Informationen finden Sie in der Dokumentation für Director.

Wenn Sie das Personal vDisk-Feature verwenden, werden Citrix Benutzerprofile standardmäßig auf den persönlichen vDisks der virtuellen Desktops gespeichert. Löschen Sie die Kopie eines Profils im Benutzerspeicher nicht, wenn gleichzeitig eine Kopie auf der persönlichen vDisk verbleibt. Dies würde einen Profilverwaltungsfehler auslösen und dazu führen, dass für Anmeldungen an dem virtuellen Desktop ein temporäres Profil verwendet wird.

Automatische Konfiguration

Der Desktoptyp wird automatisch basierend auf der VDA-Installation erkannt und entsprechende Standardwerte für die Profilverwaltung werden neben Ihrer Konfigurationsauswahl in Studio festgelegt.

Die Richtlinien, die von der Profilverwaltung angepasst werden, werden in der Tabelle unten angezeigt. Nicht-Standard-Richtlinieneinstellungen bleiben erhalten und werden nicht von diesem Feature überschrieben. Weitere Informationen zu jeder Richtlinie finden Sie in der Dokumentation zur Profilverwaltung. Die Maschinentypen, für die Profile erstellt werden, wirken sich auf die angepassten Richtlinien aus. Wichtig ist, ob Maschinen persistent oder bereitgestellt sind, und ob sie von mehreren Benutzern gemeinsam verwendet werden oder nur einem dedizierten Benutzer zugeordnet sind.

Persistente Systeme verfügen über einen lokalen Speicher, dessen Inhalt auch nach dem Abschalten des Systems bestehen bleibt. Persistente Systeme imitieren u. U. mit Speichertechnologien wie SANs (Speichernetzwerke) einen lokalen Datenträger. Bereitgestellte Systeme werden dagegen bei Bedarf von einem Basisdatenträger und einem Identitätsdatenträger erstellt. Der lokale Speicher wird üblicherweise durch eine RAM-Disk oder Netzwerkdisk imitiert. Letztere wird oft über ein SAN mit einer Hochgeschwindigkeitsverbindung zur Verfügung gestellt. Für die Bereitstellung wird allgemein

Provisioning Services oder die Maschinenerstellungsdienste (oder ein entsprechendes Produkt eines Drittanbieters) verwendet. Manchmal haben bereitgestellte Systeme persistenten lokalen Speicher, der möglicherweise durch persönliche vDisks zur Verfügung gestellt wird; diese werden als persistent klassifiziert.

Zusammen definieren diese beiden Faktoren die folgenden Maschinentypen:

- **Permanent und dediziert** - Beispiele sind Desktopbetriebssystemmaschinen mit festen Zuweisungen und einer persönlichen vDisk, die mit den Maschinenerstellungsdiensten erstellt wurden, Desktops mit persönlichen vDisks, die in VDI-in-a-Box erstellt wurden, physische Arbeitsstationen und Laptops
- **Permanent und freigegeben:** Beispiele sind Serverbetriebssystemmaschinen, die mit den Maschinenerstellungsdiensten erstellt wurden.
- **Bereitgestellt und dediziert:** Beispiele sind Desktopbetriebssystemmaschinen mit statischen Zuweisungen, aber ohne persönliche vDisk, die mit Provisioning Services erstellt wurden.
- **Bereitgestellt und freigegeben:** Beispiele sind Desktopbetriebssystemmaschinen mit zufälliger Zuweisung, die mit Provisioning Services erstellt wurden, und Desktops ohne persönliche vDisks, die mit VDI-in-a-Box erstellt wurden.

Die folgenden Richtlinieneinstellungen der Profilverwaltung werden für die verschiedenen Maschinentypen empfohlen. Sie funktionieren in den meisten Fällen gut, aber Sie müssen sie ggf. an die Anforderungen Ihrer Bereitstellung anpassen.

Wichtig:
“Lokal zwischengespeicherte Profile nach Abmeldung löschen”,
“Profilstreaming”und
“Immer zwischenspeichern”werden durch die automatische Konfiguration erzwungen. Passen Sie die anderen Richtlinien manuell an.

Persistente Maschinen

Richtlinie	Persistent und dediziert	Persistent und freigegeben
Lokal zwischengespeicherte Profile nach der Abmeldung löschen	Deaktiviert	Aktiviert
Profilstreaming	Deaktiviert	Aktiviert
Immer zwischenspeichern	Aktiviert (Hinweis 1)	Deaktiviert (Hinweis 2)
Aktives Zurückschreiben	Deaktiviert	Deaktiviert (Hinweis 3)
Anmeldungen lokaler Administratoren verarbeiten	Aktiviert	Deaktiviert (Hinweis 4)

Bereitgestellte Maschinen

Richtlinie	Bereitgestellt und dediziert	Bereitgestellt und freigegeben
Lokal zwischengespeicherte Profile nach der Abmeldung löschen	Deaktiviert (Hinweis 5)	Aktiviert
Profilstreaming	Aktiviert	Aktiviert
Immer zwischenspeichern	Deaktiviert (Hinweis 6)	Deaktiviert
Aktives Zurückschreiben	Aktiviert	Aktiviert
Anmeldungen lokaler Administratoren verarbeiten	Aktiviert	Aktiviert (Hinweis 7)

1. Da Profilstreaming für diesen Maschinentyp deaktiviert ist, wird die Einstellung Immer zwischenspeichern immer ignoriert.
2. Deaktivieren Sie Immer zwischenspeichern. Sie können sicherstellen, dass große Dateien möglichst bald nach der Anmeldung in Profile geladen werden, wenn Sie diese Richtlinie aktivieren und mit ihr ein Dateigrößenlimit definieren (in MB). Dateien, die diese Größe überschreiten, werden so schnell wie möglich lokal zwischengespeichert.
3. Deaktivieren Sie Aktiv zurückschreiben, außer wenn Sie Änderungen in Profilen für Benutzer speichern, die zwischen XenApp-Servern roamen. Aktivieren Sie in dieser Situation diese Richtlinie.
4. Deaktivieren Sie Anmeldungen lokaler Administratoren verarbeiten, außer für gehostete, freigegebene Desktops. Aktivieren Sie in dieser Situation diese Richtlinie.
5. Deaktivieren Sie Lokal zwischengespeicherte Profile nach Abmeldung löschen. Damit bleiben lokal zwischengespeicherte Profile erhalten. Da die Maschinen beim Abmelden zurückgesetzt werden, aber einzelnen Benutzern zugewiesen sind, ist die Anmeldung mit zwischengespeicherten Profile schneller.
6. Deaktivieren Sie Immer zwischenspeichern. Sie können sicherstellen, dass große Dateien möglichst bald nach der Anmeldung in Profile geladen werden, wenn Sie diese Richtlinie aktivieren und mit ihr ein Dateigrößenlimit definieren (in MB). Dateien, die diese Größe überschreiten, werden so schnell wie möglich lokal zwischengespeichert.
7. Aktivieren Sie "Anmeldungen lokaler Administratoren verarbeiten", außer für Benutzer, die zwischen XenApp und XenDesktop-Servern roamen. Deaktivieren Sie in dieser Situation diese Richtlinie.

Ordnerumleitung

Die Ordnerumleitung ermöglicht das Speichern von Benutzerdaten auf Netzwerkfreigaben, die nicht zum Speichern von Profilen verwendet werden. Dies verringert die Profilgröße und die Ladezeit, hat aber möglicherweise Auswirkungen auf die Netzwerkbandbreite. Zur Ordnerumleitung müssen keine Citrix Benutzerprofile verwendet werden. Sie können die Benutzerprofile selbst verwalten und dennoch Ordner umleiten.

Konfigurieren Sie die Ordnerumleitung mit den Citrix Richtlinien in Studio.

- Stellen Sie sicher, dass die Netzwerkspeicherorte zum Speichern des Inhalts von umgeleiteten Ordnern verfügbar sind, und die erforderlichen Berechtigungen richtig sind. Die Speicherorteigenschaften werden überprüft.
- Umgeleitete Ordner werden im Netzwerk eingerichtet und mit Inhalten der virtuellen Desktops bei der Anmeldung aufgefüllt.

Hinweis: Konfigurieren Sie die Ordnerumleitung entweder mit den Citrix Richtlinien oder den Active Directory-Gruppenrichtlinienobjekten, jedoch nicht mit beiden. Das Konfigurieren der Ordnerumleitung mit beiden Richtlinienengines kann zu unvorhersehbarem Verhalten führen.

Erweiterte Ordnerumleitung

In Bereitstellungen mit mehreren Betriebssystemen können Sie Teile eines Benutzerprofils für jedes Betriebssystem freigeben. Der Rest des Profils ist nicht freigegeben und kann nur von einem Betriebssystem verwendet werden. Um sicherzustellen, dass die Benutzererfahrung für alle Betriebssysteme konsistent ist, benötigen Sie für jedes Betriebssystem eine andere Konfiguration. Dies ist die erweiterte Ordnerumleitung. Beispiel: Bei verschiedenen Versionen einer Anwendung auf zwei Betriebssystemen muss möglicherweise eine freigegebene Datei gelesen oder bearbeitet werden. Sie entscheiden daher, sie an einen einzigen Speicherort im Netzwerk umzuleiten, von dem beide Versionen auf sie zugreifen können. Alternativ, da die Inhalte des Startmenüordners der beiden Betriebssysteme unterschiedlich strukturiert sind, können Sie entscheiden, nur einen Ordner umzuleiten, nicht beide. Hierdurch werden die Startmenüordner und die Inhalte auf jedem Betriebssystem getrennt, und die Benutzererfahrung ist konsistent.

Wenn Sie die erweiterte Ordnerumleitung in Ihrer Bereitstellung benötigen, müssen Sie die Struktur der Profildaten Ihrer Benutzer genau kennen und festlegen, welche Teile davon zwischen Betriebssystemen freigegeben werden können. Dies ist wichtig, weil eine falsch angewendete Ordnerumleitung zu unvorhersehbarem Verhalten führen kann.

Umleiten von Ordnern in erweiterten Bereitstellungen

- Verwenden Sie eine separate Bereitstellungsgruppe für jedes Betriebssystem.

- Informieren Sie sich, wo die Benutzerdaten und -einstellungen von den virtuellen Anwendungen, einschließlich solcher auf virtuellen Desktops, gespeichert werden, und wie die Daten strukturiert sind.
- Leiten Sie die Ordner bei freigegebenen Profildaten, bei denen ein sicheres Datenroaming gewährleistet ist (da sie in jedem Betriebssystem identisch strukturiert sind), in jeder Bereitstellungsgruppe um.
- Bei nicht freigegebenen Profildaten, für die kein Roaming möglich ist, leiten Sie den Ordner nur in einer Desktopgruppe um. Dies ist in der Regel diejenige mit dem am häufigsten verwendeten Betriebssystem oder diejenige mit den relevantesten Daten. Alternativ können Sie bei nicht freigegebenen Daten, für die kein Roaming zwischen Betriebssystemen möglich ist, die Ordner beider Betriebssysteme an separate Netzwerkadressen umleiten.

Beispiel einer erweiterten Bereitstellung: Die Bereitstellung hat Anwendungen, einschließlich Versionen von Microsoft Outlook und Internet Explorer, die auf Windows 8-Desktops ausgeführt werden, und Anwendungen, einschließlich andere Versionen von Outlook und Internet Explorer, die von Windows Server 2008 bereitgestellt werden. Sie haben hierfür bereits zwei Bereitstellungsgruppen für die beiden Betriebssysteme eingerichtet. Die Benutzer möchten auf dieselben Kontakte und Favoriten in beiden Versionen dieser beiden Anwendungen zugreifen.

Wichtig: Die folgenden Entscheidungen und Hinweise gelten für die hier beschriebenen Betriebssysteme und die beschriebene Bereitstellung. Die Ordner, die Sie in Ihrer Organisation umleiten oder freigeben, hängen von mehreren Faktoren ab, die nur für Ihre Bereitstellung relevant sind.

- Sie leiten mit Richtlinien, die auf Bereitstellungsgruppen angewendet werden, die folgenden Ordner um:

Ordner	Umleitung in Windows 8?	Umleitung in Windows Server 2008?
Dokumente	Ja	Ja
Anwendungsdaten	Nein	Nein
Kontakte	Ja	Ja
Desktop	Ja	Nein
Downloads	Nein	Nein
Favoriten	Ja	Ja
Verknüpfungen	Ja	Nein
Eigene Musik	Ja	Ja
Eigene Bilder	Ja	Ja
Eigene Videos	Ja	Ja

Ordner	Umleitung in Windows 8?	Umleitung in Windows Server 2008?
Suchen	Ja	Nein
Gespeicherte Spiele	Nein	Nein
Startmenü	Ja	Nein

- Bei freigegebenen, umgeleiteten Ordnern:
  - Nach der Analyse der Datenstruktur der von anderen Versionen von Outlook und Internet Explorer gespeicherten Daten entscheiden Sie, dass es sicher ist, die Ordner für Kontakte und Favoriten freizugeben.
  - Sie wissen, dass die Struktur der Ordner "Eigene Dateien", "Eigene Musik", "Eigene Bilder" und "Eigene Videos"betriebssystemübergreifend standardisiert ist. Daher ist es sicher, diese Ordner für jede Bereitstellungsgruppe am gleichen Netzwerkspeicherort zu speichern.
- Bei nicht freigegebenen, umgeleiteten Ordnern:
  - Die Ordner "Desktop", "Verknüpfungen", "Suchen"oder "Startmenü"werden nicht in die Windows Server-Bereitstellungsgruppe umgeleitet, da die Daten dieser Ordner in den beiden Betriebssystemen unterschiedlich angeordnet sind. Eine Freigabe ist daher nicht möglich.
  - Um ein vorhersagbares Verhalten für diese nicht freigegebenen Daten sicherzustellen, leiten Sie sie nur in der Windows 8-Bereitstellungsgruppe um. Sie entscheiden dies, da Windows 8 öfter von den Benutzern bei ihrer täglichen Arbeit verwendet wird, die vom Server bereitgestellten Anwendungen hingegen werden nur gelegentlich genutzt. Außerdem sind in diesem Fall die nicht freigegebenen Daten relevanter für eine Desktop- als für eine Anwendungsumgebung. Desktopverknüpfungen werden beispielsweise im Ordner Desktop gespeichert und sind nützlich, wenn sie von einer Windows 8-Maschine, aber nicht von einer Windows Server-Maschine stammen.
- Bei nicht umgeleiteten Ordnern:
  - Die Server sollen keine von Benutzern heruntergeladene Dateien ansammeln, und Sie leiten den Ordner "Downloads"daher nicht um.
  - Daten von einzelnen Anwendungen können zu Kompatibilitäts- und Leistungsproblemen führen. Daher leiten Sie den Ordner "Anwendungsdaten"nicht um.

Weitere Informationen zur Ordnerumleitung finden Sie unter https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766489(v=ws.10)?redirectedfrom=MSDN.

Ordnerumleitung und Ausschlüsse

In der Citrix Profilverwaltung (nicht aber in Studio) können Sie mit einer Leistungsverbesserung die Ordnerverarbeitung mit Ausschlüssen verhindern. Wenn Sie dieses Feature verwenden, schließen Sie keine umgeleiteten Ordner aus. Die Ordnerumleitung und Ausschlüsse funktionieren zusammen. Wenn Sie also sicherstellen, dass keine umgeleiteten Ordner ausgeschlossen sind, können sie von der Profilverwaltung zurück in die Profilordnerstruktur verschoben werden. Gleichzeitig bleibt die Datenintegrität erhalten, wenn Sie später die Ordner nicht mehr umleiten möchten. Weitere Informationen zu Ausschlüssen finden Sie unter Aufnehmen und Ausschließen von Objekten.

Citrix Insight Services

August 18, 2021

Citrix Insight Services (CIS) ist eine Plattform von Citrix für Instrumentierung, Telemetrie und Ablaufverfolgung. Mit ihren Funktionen für Instrumentierung und Telemetrie können technische Benutzer (Kunden, Partner und Techniker) Probleme selbst diagnostizieren und beseitigen und die IT-Umgebung optimieren. Einzelheiten und aktuelle Informationen zu CIS und seiner Funktionsweise finden Sie unter https://cis.citrix.com (Citrix Anmeldeinformationen sind erforderlich).

Die Features von Citrix Insight Services werden kontinuierlich erweitert und sind jetzt zentraler Teil von Citrix Smart Tools. Mit Citrix Smart Tools können Sie Bereitstellungsaufgaben, Systemdiagnosen und die Energieverwaltung automatisieren. Informationen über die zugehörigen Technologien finden Sie in der Dokument zu Citrix Smart Tools.

Die an Citrix hochgeladenen Informationen werden für die Problembehandlung und zu Diagnosezwecken verwendet sowie zum Verbessern der Qualität, Zuverlässigkeit und Leistung von Produkten. Dabei gelten folgende Richtlinien:

- Citrix Insight Services-Richtlinie unter https://cis.citrix.com/legal
- Citrix Datenschutzrichtlinie unter https://www.citrix.com/about/legal/privacy.html

Dieses Release von XenApp und XenDesktop unterstützt die nachfolgend aufgeführten Tools und Technologien.

- Installations- und Upgradeanalyse für XenApp und XenDesktop
- Citrix Programm zur Verbesserung der Benutzerfreundlichkeit
- Citrix Smart Tools
- Citrix Call Home (Teil von Citrix Smart Tools)
- Citrix Scout

Analysedaten zu Installationen und Upgrades

Wenn Sie mit dem Produktinstallationsprogramm XenApp- oder XenDesktop-Komponenten bereitstellen oder aktualisieren, werden anonyme Informationen über den Installationsvorgang gesammelt und auf der Maschine gespeichert, auf der Sie die Komponente installieren/aktualisieren. Mithilfe dieser Daten verbessert Citrix das Kundenerlebnis bei der Installation.

Die Informationen werden lokal unter %ProgramData%\Citrix\CTQs gespeichert.

Der automatische Upload dieser Daten ist in der grafischen Oberfläche und der Befehlszeilenschnittstelle des Installationsprogramms für das komplette Produkt standardmäßig aktiviert.

- Sie können die Standardeinstellung über eine Registrierungseinstellung ändern. Wenn Sie die Registrierungseinstellung vor dem Installieren/Upgrade ändern, wird der gewählte Wert angewendet, wenn Sie das Installationsprogramm für das komplette Produkt verwenden.
- Sie können die Standardeinstellung beim Installieren bzw. Upgrade für die Befehlszeilenschnittstelle außer Kraft setzen, indem Sie eine Option mit dem Befehl eingeben.

Registrierungseinstellung zur Steuerung des automatischen Uploads von Installations-/Upgradeanalysedaten (Standard = 1):

Location: HKLM:\Software\Citrix\MetaInstall
Name: SendExperienceMetrics
Value: 0 = disabled, 1 = enabled

Das folgende PowerShell-Cmdlet deaktiviert den automatischen Upload von Installations-/Upgradeanalysedaten:

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -Value 0

Zum Deaktivieren des automatischen Uploads über den Befehl “XenDesktopServerSetup.exe”oder “XenDesktopVDASetup.exe”verwenden Sie die Option “/disableexperiencemetrics”.

Zum Aktivieren des automatischen Uploads über den Befehl “XenDesktopServerSetup.exe”oder “XenDesktopVDASetup.exe”verwenden Sie die Option “/sendexperiencemetrics”.

Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Wenn Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen, werden anonyme Statistiken und Nutzungsinformationen an Citrix gesendet, damit Citrix die Qualität und Leistung seiner Produkte verbessern kann. Weitere Informationen finden Sie unter https://more.citrix.com/XD-CEIP.

Registrierung bei Erstellung/Upgrade der Site

Beim Erstellen einer XenApp- oder XenDesktop-Site werden Sie (nach Installation des ersten Delivery Controllers) automatisch für das Programm zur Verbesserung der Benutzerfreundlichkeit registriert. Der erste Datenupload erfolgt ca. sieben Tage nach dem Erstellen der Site. Sie können Ihre Teilnahme nach der Siteerstellung jederzeit beenden. Wählen Sie hierfür im Studio-Navigationsbereich **Konfiguration**, anschließend die Registerkarte "Produktsupport"und folgen Sie den Anweisungen.

Bei dem Upgrade einer XenApp- oder XenDesktop-Bereitstellung:

- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP nicht unterstützte, werden Sie gefragt, ob Sie teilnehmen möchten.
- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP unterstützte und die Teilnahme war aktiviert, ist CEIP in der aktualisierten Site aktiviert.
- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP unterstützte und die Teilnahme war deaktiviert, ist CEIP in der aktualisierten Site deaktiviert.
- Wenn Sie ein Upgrade von einer Version durchführen, die CEIP unterstützte und die Teilnahme ist nicht bekannt, werden Sie gefragt, ob Sie teilnehmen möchten.

Die erfassten Informationen sind anonym, daher können sie nach dem Upload auf Citrix Insight Services nicht angezeigt werden.

Registrierung beim Installieren eines VDAs

Standardmäßig werden Sie automatisch beim CEIP registriert, wenn Sie einen Windows-VDA installieren. Sie können die Standardeinstellung über eine Registrierungseinstellung ändern. Wenn Sie die Registrierungseinstellung ändern, bevor Sie den VDA installieren, wird der neue Wert verwendet.

Registrierungseinstellung zur Steuerung der automatischen Registrierung in CEIP (Standard = 1):

Location: HKLM:\Software\Citrix\Telemetry\CEIP
Name: Enabled
Value: 0 = disabled, 1 = enabled

Standardmäßig ist die Eigenschaft "Enabled"in der Registrierung verborgen. Wird sie nicht festgelegt, dann ist der automatische Upload aktiviert.

Mit dem folgenden PowerShell-Cmdlet wird die Registrierung beim CEIP deaktiviert:

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0

Die erfassten Laufzeitdatenpunkte werden regelmäßig als Datei in einen Ausgabeordner geschrieben (standardmäßig %programdata%/Citrix/VdaCeip).

Der erste Datenupload erfolgt ca. sieben Tage nach der Installation des VDAs.

Registrierung bei der Installation anderer Produkte und Komponenten

Sie können auch am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen, wenn Sie andere Produkte, Komponenten und Technologien von Citrix installieren, z. B. Provisioning Services, AppDNA, Citrix Lizenzserver, Citrix Receiver für Windows, den universellen Druckserver und Sitzungsaufzeichnung. Standardwerte für die Installation und Teilnahme finden Sie in der Dokumentation dieser Komponenten.

Citrix Smart Tools

Sie können den Smart Tools-Zugang aktivieren, wenn Sie einen Delivery Controller installieren.

Die Option zum Aktivieren des Smart Tools-Zugangs (und, falls nicht bereits aktiviert, der Teilnahme an Call Home) ist standardmäßig aktiviert. Klicken Sie auf **Verbinden**. Es wird ein Browserfenster geöffnet und automatisch eine Smart Services-Webseite aufgerufen, auf der Sie Ihre Citrix Cloud-Anmeldeinformationen eingeben. Wenn Sie kein Citrix Cloud-Konto haben, geben Sie die Anmeldeinformationen für Ihr Citrix-Konto ein. Es wird dann automatisch ein Citrix Cloud-Konto für Sie erstellt. Nachdem Sie authentifiziert wurden, wird im Hintergrund ein Zertifikat im Verzeichnis des Smart Tools Agents installiert.

Informationen zur Verwendung von Smart Tools-Technologien finden Sie in der Smart Tools-Dokumentation.

Citrix Call Home

Wenn Sie bestimmte Komponenten und Features in XenApp oder XenDesktop installieren, wird Ihnen angeboten, an Citrix Call Home teilzunehmen. Call Home erfasst Diagnosedaten und lädt in regelmäßigen Abständen Telemetriepakete mit den Daten über HTTPS am Standardport 443 direkt zu Citrix Insight Services zur Analyse und Problembehandlung hoch.

Call Home wird in XenApp und XenDesktop als Hintergrunddienst unter dem Namen “Citrix Telemetry Service”ausgeführt. Weitere Informationen finden Sie unter https://more.citrix.com/XD-CALLHOME.

Die Call Home-Planungsfunktion ist auch in Citrix Scout verfügbar. Weitere Informationen finden Sie unter Citrix Scout.

Folgendes wird erfasst

Die Citrix Diagnostic Facility (CDF)-Ablaufverfolgung protokolliert Informationen, die für die Problembehandlung hilfreich sein können. Call Home erfasst eine Untergruppe der CDF-Ablaufverfolgungen,

die bei der Problembehandlung allgemeiner Fehler, z. B. bei VDA-Registrierungen und Starts von Anwendung und Desktops, hilfreich sein können. Diese Technologie wird auch als Always-On-Ablaufverfolgung (Always-On Tracing, AOT) bezeichnet. Call Home erfasst keine anderen ETW-Informationen (Ereignisablaufverfolgung für Windows) und kann auch nicht dafür konfiguriert werden.

Call Home erfasst auch andere Informationen, z. B.:

- Registrierungen, die von XenApp und XenDesktop in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix erstellt wurden
- Informationen zu Windows Management Instrumentation (WMI) unter dem Citrix Namespace
- Liste der aktuellen Prozesse
- Absturzabbilder von Citrix Prozessen, sie werden unter %PROGRAM DATA%\Citrix\CDF gespeichert

Die Ablaufverfolgungsinformationen werden bei der Erfassung komprimiert. Der Citrix Telemetriedienst speichert maximal 10 MB Ablaufverfolgungsinformationen in komprimierter Form für maximal acht Tage.

- Durch das Komprimieren der Daten benötigt Call Home nicht viel Speicherplatz auf dem VDA.
- Ablaufverfolgungen bleiben im Speicher erhalten, damit auf bereitgestellten Maschinen keine IOPS erfolgen müssen.
- Der Ablaufverfolgungspuffer verwendet einen kreisförmigen Mechanismus, um Ablaufverfolgungen im Speicher zu erhalten.

Call Home erfasst die unter Schlüsseldatenpunkte in Call Home aufgeführten wichtigen Datenpunkte.

Konfigurations- und Verwaltungszusammenfassung

Sie können sich bei Call Home mit dem Assistenten des Produktinstallationsprogramms oder später mit PowerShell-Cmdlets registrieren. Wenn Sie sich registrieren, werden standardmäßig Diagnosedaten erfasst und jeden Sonntag um ca. 03.00 Uhr Ortszeit an Citrix hochgeladen. Der Zeitpunkt des Uploads wird innerhalb eines Zwei-Stunden-Fensters ab dem angegebenen Zeitpunkt zufällig festgelegt. Dies bedeutet, dass ein Upload nach dem Standardzeitplan zwischen 03:00 und 05:00 Uhr morgens erfolgt.

Wenn Sie keine Diagnosedaten nach Plan hochladen oder den Zeitplan ändern möchten, können Sie mit PowerShell-Cmdlets Call Home-Daten manuell erfassen und hochladen.

Bei der Registrierung für geplante Call Home-Uploads und beim manuellen Hochladen von Diagnoseinformationen an Citrix geben Sie Ihre Anmeldeinformationen für Ihr Citrix Konto oder Citrix Cloud an.

Citrix ersetzt die Anmeldeinformationen durch ein Uploadtoken zum Identifizieren des Kunden und Hochladen der Daten. Die Anmeldeinformationen werden nicht gespeichert.

Wenn Upload ausgeführt wird, wird per E-Mail eine Benachrichtigung an die Adresse des Citrix Kontos gesendet.

Voraussetzungen

- Auf der Maschine muss PowerShell 3.0 oder höher ausgeführt werden.
- Der Citrix Telemetriedienst muss auf der Maschine ausgeführt werden.
- Die Systemvariable "PSModulePath"muss auf den Installationspfad des Telemetriediensts festgelegt werden (z. B. C:\Programme\Citrix\Telemetry Service\)

Aktivieren von Call Home während der Komponenteninstallation

VDA-Installation/-Upgrade: Wenn Sie einen Virtual Delivery Agent über die grafische Benutzeroberfläche des Produktinstallationsprogramms installieren oder aktualisieren, werden Sie gefragt, ob Sie an Call Home teilnehmen möchten. Es gibt zwei Optionen:

- An Call Home teilnehmen
- Nicht an Call Home teilnehmen

Wenn Sie einen VDA aktualisieren und zuvor für Call Home registriert waren, wird diese Seite des Assistenten nicht angezeigt.

Controller-Installation/-Upgrade: Wenn Sie einen Delivery Controller über die grafische Benutzeroberfläche installieren oder aktualisieren, werden Sie gefragt, ob Sie an Call Home teilnehmen und eine Verbindung mit Citrix Smart Tools herstellen möchten. Es gibt drei Optionen:

- Verbindung mit Citrix Smart Tools einschließlich Call Home über den Smart Tools Agent herstellen: Diese (Standard-)Option wird empfohlen. Wenn Sie diese Option auswählen, wird der Smart Tools Agent konfiguriert. (Der Smart Tools Agent wird installiert, unabhängig davon, ob diese Option ausgewählt wird.)
- Nur an Call Home ohne Verbindung mit Smart Tools teilnehmen: Wenn Sie diese Option auswählen, wird der Smart Tools Agent installiert, jedoch konfiguriert. Die Call Home-Funktionen stehen über Citrix Telemetry Service und Citrix Insight Services zur Verfügung.
- Nicht an Call Home teilnehmen und keine Verbindung mit Smart Tools herstellen:

Wenn Sie einen Controller installieren, können Sie nicht mehr zum Konfigurieren von Informationen über das Call Home Seite des Installationsassistenten wenn der Server über eine Active Directory-Gruppenrichtlinienobjekt mit der Richtlinieneinstellung "Anmelden als Dienst"angewendet. Weitere Informationen finden Sie unter CTX218094.

Wenn Sie einen Controller aktualisieren und bereits bei Call Home registriert sind, werden Sie nur gefragt, ob Sie eine Verbindung mit Smart Tools herstellen möchten. Wenn Sie bei Call Home registriert sind und der Smart Tools Agent installiert ist, wird die Seite des Assistenten nicht angezeigt.

Informationen zu Smart Tools finden Sie in der Smart Tools-Dokumentation.

PowerShell-Cmdlets

Die PowerShell-Hilfe enthält umfassende Syntax, einschließlich Beschreibungen von Cmdlets und Parametern, die nicht so häufig verwendet werden.

Informationen zur Verwendung eines Proxyservers für Uploads finden Sie unter Konfigurieren eines Proxyservers.

Aktivieren geplanter Uploads

Diagnosesammlungen werden automatisch an Citrix hochgeladen. Wenn Sie keine zusätzlichen Cmdlets für einen benutzerdefinierten Zeitplan eingeben, wird der Standardzeitplan verwendet.

```
$cred = Get-Credential
Enable-CitrixCallHome -Credential $cred
```

Um sicherzustellen, dass geplante Uploads aktiviert sind, geben Sie Get-CitrixCallHome ein. Folgendes sollte wiedergegeben werden: IsEnabled=True und IsMasterImage=False.

Aktivieren von geplanten Uploads für Maschinen, die von einem Masterimage erstellt wurden

Wenn Sie geplante Uploads in einem Masterimage konfigurieren, brauchen Sie nicht jede einzelne im Maschinenkatalog erstellte Maschine zu konfigurieren.

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

Um sicherzustellen, dass geplante Uploads aktiviert sind, geben Sie Get-CitrixCallHome ein. Folgendes sollte zurückgegeben werden: IsEnabled=True und IsMasterImage=True.

Erstellen eines benutzerdefinierten Zeitplans

Es kann ein Zeitplan für die tägliche oder wöchentliche Erfassung und Übermittlung von Diagnosedaten erstellt werden.

```
$timespan = New-TimeSpan –Hours <hours> -Minutes <minutes>
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek <day> -UploadFrequency {Daily|Weekly}
```


Abbrechen von geplanten Uploads

Wenn Sie geplante Uploads abbrechen, können Sie weiterhin Diagnosedaten mit PowerShell-Cmdlets hochladen.

Disable-CitrixCallHome

Um sicherzustellen, dass geplante Uploads deaktiviert sind, geben Sie Get-CitrixCallHome ein. Folgendes sollte zurückgegeben werden: IsEnabled=False und IsMasterImage=False.

Beispiele

Das folgende Cmdlet erstellt einen Zeitplan, nach dem Datenpakete jeden Abend um 23:20 Uhr erstellt und hochgeladen werden. Beachten Sie, dass der Parameter für Stunden das 24-Stunden-Format verwendet. Wenn der Wert für den Parameter "UploadFrequency"auf "Daily"festgelegt ist, wird der Parameter "DayOfWeek"ignoriert, wenn er angegeben ist.

```
$timespan –New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

Um den Zeitplan zu überprüfen, geben Sie Get-CitrixCallHomeSchedule ein. Für das oben aufgeführte Beispiel sollte Folgendes zurückgegeben werden: StartTime=22:20:00, DayOfWeek=Sunday (ignoriert), Upload Frequency=Daily.

Das folgende Cmdlet erstellt einen Zeitplan, nach dem Datenpakete mittwochabends um 23:20 Uhr erstellt und hochgeladen werden.

```
$timespan –New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -UploadFrequency Weekly
```

Um den Zeitplan zu überprüfen, geben Sie Get-CitrixCallHomeSchedule ein. Für das oben aufgeführte Beispiel sollte Folgendes zurückgegeben werden: StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly.

Konfigurieren eines Proxyservers für Call Home-Uploads

Führen Sie die folgenden Aufgaben auf der Maschine aus, auf der Call Home aktiviert ist. Die Beispiele im nachfolgenden Verfahren enthalten die Serveradresse und Port 10.158.139.37:3128. Die entsprechenden Adressen in Ihrer Umgebung sind anders.

Schritt 1. Geben Sie Proxyserverinformationen im Browser ein. Wählen Sie in Internet Explorer **Internetoptionen > Verbindungen > LAN-Einstellungen**. Wählen Sie **Proxyserver für das LAN verwenden** und geben Sie die Adresse und Portnummer des Proxyservers ein.

Schritt 2. Führen Sie PowerShell **netsh winhttp import proxy source=ie** aus.


```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

Schritt 3. Bearbeiten Sie mit einem Text-Editor die Konfigurationsdatei TelemetryService.exe in C:\Programme\Citrix\Telemetry Service. Fügen Sie die in dem roten Feld unten dargestellten Informationen hinzu.

Schritt 4. Starten Sie den Telemetriedienst neu.

Führen Sie die Call Home-Cmdlets in PowerShell aus.

Manuelles Erfassen und Hochladen von Diagnoseinformationen

Sie können über die CIS-Website ein Diagnoseinformationspaket nach CIS hochladen. Sie können auch PowerShell-Cmdlets zum Erfassen und Hochladen von Diagnoseinformationen nach CIS verwenden.

Hochladen eines Pakets über die CIS-Website

1. Melden Sie sich mit Ihren Citrix Kontoanmeldeinformationen an Citrix Insight Services an.
2. Wählen Sie **My Workspace**.
3. Wählen Sie **Healthcheck** und navigieren Sie zum Speicherort der Daten.

CIS unterstützt mehrere PowerShell-Cmdlets, die Datenuploads verwalten. In dieser Dokumentation werden die Cmdlets für zwei häufige Fälle behandelt:

- Verwenden Sie das Cmdlet Start-CitrixCallHomeUpload, um ein Diagnoseinformationspaket manuell zu sammeln und nach CIS hochzuladen. (Das Paket wird nicht lokal gespeichert.)
- Verwenden Sie das Cmdlet Start-CitrixCallHomeUpload, um Daten manuell zu sammeln und ein Diagnoseinformationspaket lokal zu speichern. Auf diese Weise können Sie eine Vorschau der Daten anzeigen. Zu einem späteren Zeitpunkt können Sie dann das Cmdlet Send-CitrixCallHomeBundle verwenden, um eine Kopie des Pakets manuell nach CIS hochzuladen. (Die ursprünglichen Daten bleiben lokal gespeichert.)

Die PowerShell-Hilfe enthält umfassende Syntax, einschließlich Beschreibungen von Cmdlets und Parametern, die nicht so häufig verwendet werden.

Wenn Sie ein Cmdlet zum Hochladen von Daten nach CIS eingeben, werden Sie aufgefordert, den Upload zu bestätigen. Wenn ein Timeout des Cmdlets erfolgt, bevor der Upload abgeschlossen ist, überprüfen Sie den Status des Uploads im Systemereignisprotokoll. Die Uploadanforderung wird möglicherweise abgelehnt, wenn der Dienst bereits einen Upload ausführt.

Sammeln von Daten und Hochladen des Pakets nach CIS

Start-CitrixCallHomeUpload [-Credential] <PSCredential> [-InputPath <String>] [-Description <String>] [-IncidentTime <String>] [-SRNumber <String>] [-Name <String>] [-UploadHeader <String>] [-AppendHeaders <String>] [-Collect <String>] [<CommonParameters>]

Sammeln von Daten und lokales Speichern

Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath <String>] [-Description <String>] [-IncidentTime <String>] [-SRNumber <String>] [-Name <String>] [-UploaderHeader <String>] [-AppendHeaders <String>] [-Collect <String>] [<CommonParameters>]

Parameter	Beschreibung
Anmeldeinformationen	Leitet den Upload nach CIS.
InputPath	Speicherort der ZIP-Datei, die zum Paket gehört. Das kann eine weitere Datei sein, die Citrix Support benötigt. Stellen Sie sicher, dass die Erweiterung .zip eingeschlossen ist.
OutputPath	Speicherort, an dem die Diagnoseinformationen gespeichert werden. Dieser Parameter ist erforderlich, wenn Call Home-Daten lokal gespeichert werden.
Description and Incident Time	Formlose Informationen zum Upload.

Parameter	Beschreibung
SRNumber	Incident-Nummer des technischen Supports von Citrix.
Name	Name des Pakets.
UploadHeader	Zeichenfolge im JSON-Format zur Angabe der Uploadheader, die nach CIS hochgeladen werden.
AppendHeaders	Zeichenfolge im JSON-Format zur Angabe der angefügten Header, die nach CIS hochgeladen werden.
Collect	Zeichenfolge im JSON-Format zur Angabe, welche Daten erfasst oder ausgelassen werden, das Format ist {‘collector’:{‘enabled’:Boolean}}, wobei Boolean “true”oder “false”ist. Gültige Collector-Werte: wmi, process, registry, crashreport, trace, localdata, sitedata, sfb. Standardmäßig sind alle Datensammelpunkte außer “sfb”aktiviert. Der Datensammelpunkt “sfb”ist für die Verwendung bei Bedarf zur Diagnose von Problemen mit Skype for Business vorgesehen. Neben dem Parameter “enabled” unterstützt sfb die Parameter “account”und “accounts”zur Angabe von Zielbenutzern. Verwenden Sie eine der folgenden Varianten: “-Collect “{‘sfb’:{‘account’:’domain\user1’}}”; -Collect “{‘sfb’:{‘accounts’:[‘domain\user1’, ‘domain\user2’]}}”
Allgemeine Parameter	Weitere Informationen finden Sie in der PowerShell-Hilfe.

Hochladen von Daten, die zuvor lokal gespeichert waren

Send-CitrixCallHomeBundle -Credential <PSCredential> -Path <String> [<CommonParameters>]

Mit dem Path-Parameter geben Sie den Speicherort des zuvor gespeicherten Pakets an.

Beispiele

Mit dem folgenden Cmdlet wird ein Upload von Call Home-Daten (mit Ausnahme von Daten vom WMI-Datensammelpunkt) nach CIS angefordert. Diese Daten beziehen sich auf Registrierungsfehler bei PVS VDAs, die um 14:30 Uhr für den Citrix Supportfall 123456 bemerkt wurden. Zusätzlich zu den Call Home-Daten wird die Datei c:\Diagnostics\ExtraData.zip in das Uploadpaket eingeschlossen.

C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip"-Description "Registration failures with PVS VDAs"-IncidentTime "14:30"-SRNumber 123456 -Name "RegistrationFailure-021812016"-Collect "{'wmi':{'enabled':false}}"-UploadHeader "{'key1':'value1'}"-AppendHeaders "{'key2':'value2'}"

Das folgende Cmdlet speichert Call Home-Daten, die sich auf den Citrix Supportfall 223344 beziehen, der um 8:15 Uhr bemerkt wurde. Die Daten werden in der Datei mydata.zip auf einer Netzwerkfreigabe gespeichert. Zusätzlich zu den Call Home-Daten wird die Datei c:\Diagnostics\ExtraData.zip in das gespeicherte Paket eingeschlossen.

C:\PS>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"-Description "Diagnostics for incident number 223344"-IncidentTime "8:15"-SRNumber 223344

Das folgende Cmdlet lädt das Datenpaket hoch, das Sie zuvor gespeichert haben.

$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip

Citrix Scout

Vollständige Informationen finden Sie unter Citrix Scout.

Citrix Scout

October 21, 2021

Einführung

Citrix Scout erfasst Diagnosedaten, die zur vorbeugenden Wartung der XenApp- und XenDesktop-Bereitstellung verwendet werden können. Citrix bietet eine umfassende, automatisierte Analyse über Citrix Insight Services an. Mit Scout können Sie Probleme selbst oder mit Unterstützung des Citrix Supports behandeln. Sie können Datensammlungen an Citrix zur Analyse hochladen, wenn Sie

Hilfe vom Citrix Support benötigen. Alternativ können Sie eine Datensammlung für eigene Zwecke lokal speichern und dann später an Citrix zur Analyse hochladen.

Scout bietet drei Hauptverfahren:

- **Sammeln:** Eine einmalige Sammlung von Diagnosedaten wird auf den von Ihnen in der Site ausgewählten Maschinen durchgeführt. Anschließend laden Sie die Datei mit der Sammlung an Citrix hoch oder speichern sie lokal.
- **Ablauf verfolgen und reproduzieren:** Eine manuelle Ablaufverfolgung auf den ausgewählten Maschinen wird gestartet. Sie können dann die Probleme auf den Maschinen reproduzieren. Sobald ein Problem reproduziert wurde, wird die Ablaufverfolgung gestoppt. Scout sammelt dann weitere Diagnosedaten und lädt diese zusammen mit der Ablaufdatei an Citrix hoch (bzw. speichert sie lokal).
- **Planen:** Ein Zeitplan für die tägliche oder wöchentliche Diagnosedatensammlung zu einer bestimmten Zeit auf den von Ihnen ausgewählten Maschinen wird erstellt. Die Datei mit der Sammlung wird automatisch an Citrix hochgeladen.

Die in diesem Artikel beschriebene grafische Benutzeroberfläche ist die primäre Methode zur Steuerung von Scout. Alternativ können Sie mit der PowerShell-Schnittstelle einmalige oder geplante Diagnosesammlungen und Uploads konfigurieren. Siehe Call Home.

Ort der Ausführung von Scout

- In einer lokalen XenApp- und XenDesktop-Bereitstellung führen Sie Scout auf einem Delivery Controller aus, wenn Diagnosedaten auf einem oder mehreren VDAs und Delivery Controllern gesammelt werden sollen. Sie können Scout auch auf einem VDA ausführen, um lokale Diagnosedaten zu sammeln.
- Führen Sie Scout in einer Citrix Cloud-Umgebung, in der der XenApp und XenDesktop Service verwendet wird, auf einem VDA zum Sammeln lokaler Diagnosedaten aus.

Folgendes wird erfasst

Die von Scout gesammelten Diagnosedaten enthalten Ablaufprotokolldateien von Citrix Diagnostic Facility (CDF). Außerdem ist eine Untergruppe der CDF-Ablaufverfolgungen (Always-On-Ablaufverfolgung, AOT) enthalten. AOT-Informationen können bei der Behandlung häufiger Probleme, etwa im Zusammenhang mit der VDA-Registrierung oder mit Anwendungs-/Desktopstarts, helfen. Es werden keine anderen ETW-Informationen (Ereignisablaufverfolgung für Windows) gesammelt.

Gesammelte Daten:

- Von XenApp und XenDesktop unter HKEY_LOCAL_MACHINE\SOFTWARE\CITRIX erstellte Registrierungseinträge

- Informationen zu Windows Management Instrumentation (WMI) unter dem Citrix Namespace.
- Ausgeführte Prozesse
- Absturzabbilder von Citrix Prozessen, die unter %PROGRAM DATA%\Citrix\CDF gespeichert wurden

Hinweise zu Ablaufverfolgungsdaten

- Die Ablaufverfolgungsdaten werden beim Sammeln komprimiert und erfordern nur wenig Speicherplatz auf der Maschine.
- Der Citrix Telemetriedienst speichert auf jeder Maschine maximal 10 MB Ablaufverfolgungsinformationen in komprimierter Form für maximal acht Tage.
- Ablaufverfolgungen bleiben im Speicher erhalten, damit auf bereitgestellten Maschinen keine IOPS erfolgen müssen.
- Der Ablaufverfolgungspuffer verwendet einen kreisförmigen Mechanismus, um Ablaufverfolgungen im Speicher zu erhalten.

Eine Liste der Datenpunkte, die Scout erfasst, finden Sie unter Wichtige Datenpunkte in Scout.

Voraussetzungen und Überlegungen

Berechtigungen

- Sie müssen lokaler Administrator und Domänenbenutzer jeder Maschine sein, auf der Sie Diagnosedaten sammeln.
- Sie benötigen Berechtigung zum Schreiben in das Verzeichnis “LocalAppData”auf jeder Maschine.
- Verwenden Sie **Als Administrator ausführen**, wenn Sie Scout starten.

Für jede Maschine, auf der Sie Diagnosedaten erfassen, gilt Folgendes:

- Scout muss mit der Maschine kommunizieren können.
- Die Datei- und Druckerfreigabe muss aktiviert sein.
- PSRemoting und WinRM müssen aktiviert sein. Auf der Maschine muss PowerShell 3.0 oder höher ausgeführt werden.
- Der Citrix Telemetriedienst muss auf der Maschine ausgeführt werden.
- Zum Festlegen eines Zeitplans für die Erfassung von Diagnosedaten muss auf der Maschine eine Scout-Version ausgeführt werden, die mit XenApp und XenDesktop 7.14 oder eine späteren, unterstützten Version geliefert wurde.

Von Scout werden die von Ihnen ausgewählten Maschinen auf Erfüllung dieser Bedingungen geprüft.

Tests zur Überprüfung

Vor Ausführung einer Diagnosesammlung wird automatisch jede ausgewählte Maschine überprüft. Diese Prüfung gewährleistet, dass die oben aufgeführten Anforderungen erfüllt sind. Besteht eine Maschine den Test nicht, wird in Scout eine Meldung mit einem Maßnahmenvorschlag angezeigt.

Fehlermeldung	Korrekturmaßnahme
Scout kann diese Maschine nicht erreichen.	Vergewissern Sie sich, dass die Maschine eingeschaltet ist. Vergewissern Sie sich, dass die Verbindung mit dem Netzwerk ordnungsgemäß funktioniert. (Dazu gehört u. U. eine Überprüfung der ordnungsgemäßen Konfiguration der Firewall.) Vergewissern Sie sich, dass, dass die Datei- und Druckerfreigabe aktiviert ist. Weitere Informationen finden Sie in der Microsoft Dokumentation.
Aktivieren von PSRemoting und WinRM	Sie können PowerShell-Remoting und WinRM gleichzeitig aktivieren. Führen Sie das Cmdlet **Enable-PSRemoting** als Administrator aus. Weitere Informationen finden Sie in der Microsoft-Hilfe zu dem Cmdlet.
Scout erfordert mindestens PowerShell 3.0	Installieren Sie PowerShell 3.0 auf der Maschine und aktivieren Sie dann PowerShell Remoting.
Zugriff auf das Verzeichnis ‘LocalAppData’ist auf dieser Maschine nicht möglich	Stellen Sie sicher, dass das Konto Schreibberechtigung für das Verzeichnis “LocalAppData”auf der Maschine hat.
Citrix Telemetriedienst wurde nicht gefunden	Stellen Sie sicher, dass der Citrix Telemetriedienst auf der Maschine installiert und gestartet wurde.
Zeitplan kann nicht abgerufen werden	Aktualisieren Sie die Maschine auf (mindestens) XenApp- und XenDesktop 7.14.

Versionskompatibilität

Diese Version von Scout (3.x) ist für die Ausführung auf Controllern und VDAs unter XenApp und XenDesktop ab Version 7.14 vorgesehen.

Eine ältere Version von Scout steht für ältere XenApp- und XenDesktop-Bereitstellungen zur Verfügung. Weitere Informationen hierzu finden Sie unter CTX130147.

Wenn Sie einen Controller oder VDA älter als Version 7.14 auf Version 7.14 (oder eine höhere unterstützte Version) aktualisieren, wird die ältere Scout-Version durch die aktuelle ersetzt.

Feature	Scout 2.23	Scout 3.0
Unterstützung von Citrix XenApp und XenDesktop 7.14 (Minimum)	Ja	Ja
Unterstützung von XenDesktop 5.x, 7.1 bis 7.13	Ja	Nein
Unterstützung von XenApp 6.x, 7.5 bis 7.13	Ja	Nein
Erhältlich mit Produkt	7.1 bis 7.13	Ab 7.14
Kann aus CTX-Artikel heruntergeladen werden	Ja	Nein
Sammlung von CDF-Ablaufverfolgungen	Ja	Ja
Erfassung von Always-On-Ablaufverfolgungen (AOT)	Nein	Ja
Sammlung von Diagnosedaten zulassen	Bis zu 10 Maschinen gleichzeitig (in der Standardeinstellung)	Unbegrenzt (je nach Ressourcenverfügbarkeit)
Übermittlung von Diagnosedaten an Citrix zulassen	Ja	Ja
Lokale Speicherung von Diagnosedaten zulassen	Ja	Ja
Unterstützung von Citrix Cloud-Anmeldeinformationen	Nein	Ja
Unterstützung von Citrix Anmeldeinformationen	Ja	Ja
Unterstützung von Proxyservern für Uploads	Ja	Ja
Anpassen von Zeitplänen	Nicht zutreffend	Ja
Unterstützung von Skripts	Befehlszeile (nur lokaler Controller)	PowerShell mit Call Home-Cmdlets (jede Maschine mit installiertem Telemetriedienst)

Installieren

Standardmäßig wird Scout automatisch als Teil des Citrix Telemetriediensts installiert, wenn Sie einen VDA oder Controller installieren.

Wenn Sie den Citrix Telemetriedienst bei der VDA-Installation ausgelassen oder nach der Installation entfernt haben, führen Sie TelemetryServiceInstaller_xx.msi im Ordner x64\Virtual Desktop Components bzw. x86\Virtual Desktop Components des XenApp bzw. XenDesktop ISO-Images aus.

Uploadautorisierung

Wenn Sie Diagnosesammlungen an Citrix hochladen möchten, benötigen Sie ein Citrix Konto oder ein Citrix Cloud-Konto. Dies sind die Anmeldeinformationen, die Sie für Citrix Downloads oder das Citrix Cloud Control Center verwenden. Wenn die Anmeldeinformationen überprüft wurden, wird ein Token ausgestellt.

- Bei Authentifizierung mit einem Citrix Konto ist die Tokenausstellung kein sichtbarer Vorgang. Sie geben einfach Ihre Anmeldeinformationen ein. Wenn Citrix die Anmeldeinformationen überprüft hat, können Sie mit dem Scout-Assistenten fortfahren.
- Wenn Sie sich mit einem Citrix Cloud-Konto authentifizieren, klicken Sie auf einen Link für den Zugriff auf die Citrix Cloud unter Verwendung von HTTPS und Ihres Standardbrowsers. Nach Eingabe der Citrix Cloud-Anmeldeinformationen wird das Token angezeigt. Kopieren Sie das Token und fügen Sie es in Scout ein. Sie können dann mit dem Scout-Assistenten fortfahren.

Das Token wird auf der Maschine gespeichert, auf der Sie Scout ausführen. Wenn Sie das Token das nächste Mal bei Auswahl von **Sammeln** oder **Ablauf verfolgen** und reproduzieren verwenden möchten, aktivieren Sie das Kontrollkästchen **Speichern Sie das Token und überspringen Sie zukünftig diesen Schritt**.

Sie müssen jedes Mal, wenn Sie auf der Startseite von Scout **Zeitplan** auswählen, eine erneute Autorisierung durchführen. Ein gespeichertes Token kann beim Erstellen oder Ändern eines Zeitplans nicht verwendet werden.

Verwenden eines Proxyservers für Uploads

Wenn Sie beim Upload von Sammlungen an Citrix einen Proxyserver verwenden möchten, können Sie Scout zur Verwendung der Internet-Proxyeinstellungen Ihres Browsers konfigurieren oder die IP-Adresse und Portnummer des Proxyservers angeben.

Sammeln von Diagnosedaten

Das Verfahren Sammeln umfasst die Auswahl der Maschinen, die Diagnosesammlung und den Upload der Datei mit den gesammelten Daten an Citrix bzw. die lokale Speicherung der Datei.

Schritt 1. Starten Sie Scout.

Wählen Sie im Startmenü der Maschine **Citrix > Citrix Scout**. Klicken Sie auf der Startseite auf **Sammeln**.

Schritt 2. Maschinen auswählen.

Auf der Seite "Maschinen wählen"werden alle VDAs und Controller der Site aufgelistet. Sie können die Anzeige nach Maschinennamen filtern. Aktivieren Sie das Kontrollkästchen neben jeder Maschine, auf der Sie Diagnosedaten sammeln möchten, und klicken Sie auf **Weiter**.

Scout überprüft automatisch jede ausgewählte Maschine auf Erfüllung der unter Tests zur Überprüfung aufgeführten Kriterien. Wenn eine Maschine die Überprüfung nicht besteht, wird eine Meldung in der Spalte Status angezeigt und das Kontrollkästchen deaktiviert. Sie haben nun folgende Möglichkeiten:

- Beheben Sie das Problem und aktivieren Sie das Kontrollkästchen erneut. Dadurch wird eine Wiederholung des Tests ausgelöst.
- Überspringen Sie die Maschine (Kontrollkästchen deaktiviert lassen). Auf ihr werden dann keine Diagnosedaten gesammelt.

Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.

Schritt 3. Sammeln Sie Diagnosedaten von den Maschinen.

In der Zusammenfassung werden alle Maschinen aufgelistet, auf denen Diagnosedaten gesammelt werden, d. h. die Maschinen, die Sie ausgewählt haben und die den Test bestanden haben. Klicken Sie auf **Sammeln**.

Während der Sammlung geschieht Folgendes:

- In der Spalte Status wird der aktuelle Status der Sammlung für die Maschinen angezeigt.
- Um die laufende Sammlung für eine einzelne Maschine zu stoppen, klicken Sie in der Spalte "Aktion"für diese Maschine auf **Abbrechen**.
- Um alle laufenden Sammlungen zu stoppen, klicken Sie unten rechts auf der Seite auf **Sammlung stoppen**. Diagnosedaten von Maschinen, deren Sammlung abgeschlossen war, werden beibehalten. Zum Fortsetzen der Sammlung klicken Sie in der Spalte "Aktion"für jede Maschine auf **Wiederholen**.
- Wenn die Sammlung für alle ausgewählten Maschinen abgeschlossen ist, ändert sich die Schaltfläche **Sammlung stoppen** in der unteren rechten Ecke in **Weiter**.

- Um die Diagnosedaten einer Maschine nach erfolgreicher Erfassung erneut zu erfassen, klicken Sie in der Spalte **Aktion** der betreffenden Maschine auf Erneut sammeln. Die neuere Sammlung überschreibt die ältere.
- Schlägt eine Sammlung fehl, können Sie in der Spalte "Aktion"auf **Wiederholen** klicken. Nur erfolgreiche Sammlungen werden hochgeladen oder gespeichert.
- Wenn die Sammlung für alle ausgewählten Maschinen abgeschlossen ist, klicken Sie NICHT auf **Zurück**. Wenn Sie auf diese Schaltfläche klicken und die Aktion bestätigen, geht die Sammlung verloren.

Wenn die Sammlung abgeschlossen ist, klicken Sie auf **Weiter**.

Schritt 4. Sammlung speichern oder hochladen.

Wählen Sie, ob die Datei mit den Diagnosedaten an Citrix hochgeladen oder auf der lokalen Maschine gespeichert werden soll.

Wenn Sie die Datei hochladen, fahren Sie mit Schritt 5 fort.

Wenn Sie die Datei lokal speichern:

- Es wird ein Windows-Dialogfeld zum Speichern angezeigt. Navigieren Sie zu dem gewünschten Speicherort.
- Wenn die lokale Speicherung abgeschlossen ist, wird der Pfad der Datei angezeigt und verlinkt. Sie können die Datei anzeigen. Sie können die Datei später an Citrix hochladen. Informationen hierzu finden Sie unter CTX136396 (Citrix Insight Services) oder hier (Smart Tools).

Klicken Sie auf **Fertig**, um zur Scout-Startseite zurückzukehren. Sie brauchen keine weiteren Schritte auszuführen.

Schritt 5. Authentifizieren Sie sich für Uploads und geben Sie optional den Proxy an.

Einzelheiten zu diesem Verfahren finden Sie unter Uploadautorisierung.

- Wenn Sie sich noch nicht über Scout authentifiziert haben, fahren Sie mit diesem Schritt fort.
- Wenn Sie bereits über Scout authentifiziert sind, wird das gespeicherte Autorisierungstoken standardmäßig verwendet. Wenn Sie damit einverstanden sind, wählen Sie diese Option und klicken Sie auf **Weiter**. Sie müssen keine Anmeldeinformationen für diese Sammlung eingeben. Fahren Sie mit Schritt 6 fort.
- Wenn Sie sich bereits authentifiziert haben, jedoch ein neues Token wünschen, klicken Sie auf **Ändern/Neu autorisieren** und fahren Sie mit diesem Schritt fort.

Wählen Sie aus, ob Sie Citrix Konto- oder Citrix Cloud-Anmeldeinformationen für die Authentifizierung des Uploads verwenden möchten. Klicken Sie auf Weiter. Die Seite für die Anmeldeinformationen wird nur angezeigt, wenn Sie das gespeicherte Token nicht verwenden.

Führen Sie auf der Seite "Anmeldeinformationen"folgende Schritte aus:

- Wenn Sie einen Proxyserver für den Dateiupload verwenden möchten, klicken Sie auf **Proxy konfigurieren**. Sie können Scout zur Verwendung der Internet-Proxyeinstellungen Ihres Browsers konfigurieren oder die IP-Adresse und Portnummer des Proxyservers angeben. Schließen Sie das Proxydialogfeld.
- Bei Verwendung eines Citrix Cloud-Kontos klicken Sie auf **Token generieren**. Der Standardbrowser wird mit einer Citrix Cloud-Seite gestartet, auf der ein Token angezeigt wird. Kopieren Sie das Token und fügen Sie es auf der Scout-Seite ein.
- Wenn Sie ein Citrix Konto verwenden, geben Sie die zugehörigen Anmeldeinformationen ein.

Wenn Sie fertig sind, klicken Sie auf **Weiter**.

Schritt 6. Geben Sie Informationen zum Upload an.

Geben Sie folgende Informationen zum Upload ein:

- Das Feld "Name"enthält den Standardnamen für die Datei mit den gesammelten Diagnosedaten. Er eignet sich für die meisten Sammlungen, Sie können ihn aber ändern. Wenn Sie die Standardnamen löschen und das Namensfeld leer lassen, wird der Standardname verwendet.
- Geben Sie optional eine 8-stellige Citrix-Supportfallnummer ein.
- Geben Sie optional im Feld Beschreibung eine Beschreibung des Problems ein und geben Sie ggf. an, wann es aufgetreten ist.

Wenn Sie fertig sind, klicken Sie auf **Upload starten**.

Während des Uploads wird unten links auf der Seite der ungefähre Prozentsatz hochgeladener Daten angezeigt. Um einen laufenden Upload abzubrechen, klicken Sie auf **Upload stoppen**.

Wenn der Upload abgeschlossen ist, wird die URL des Speicherorts angezeigt und verlinkt. Sie können den Link kopieren oder über ihn zu dem Speicherort bei Citrix navigieren und eine Uploadanalyse anzeigen.

Klicken Sie auf **Fertig**, um zur Scout-Startseite zurückzukehren.

Verfolgen und Reproduzieren von Abläufen

Das Verfahren zum Verfolgen und Reproduzieren von Abläufen umfasst die Auswahl der Maschinen, das Starten der Ablaufverfolgung und das Reproduzieren von Problemen auf diesen Maschinen, die Diagnosesammlung und den Upload der Datei mit der Ablaufverfolgung und Sammlung an Citrix bzw. die lokale Speicherung der Datei.

Dieses Verfahren ähnelt dem Standardverfahren Sammeln. Im Unterschied zu diesem wird auf den Maschinen eine Ablaufverfolgung gestartet und es können Probleme reproduziert werden. Alle Diagnosesammlungen umfassen AOT-Ablaufverfolgungsdaten. Die zusätzlichen CDF-Ablaufverfolgungsdaten können bei der Problembehandlung helfen.

Schritt 1. Starten Sie Scout.

Wählen Sie im Startmenü der Maschine **Citrix > Citrix Scout**. Klicken Sie auf der Startseite auf **Ablauf verfolgen und reproduzieren**.

Schritt 2. Maschinen auswählen.

Auf der Seite "Maschinen wählen"werden alle VDAs und Controller der Site aufgelistet. Sie können die Anzeige nach Maschinennamen filtern. Aktivieren Sie das Kontrollkästchen neben jeder Maschine, auf der Sie Ablaufverfolgungs- und Diagnosedaten sammeln möchten, und klicken Sie auf **Weiter**.

Scout überprüft automatisch jede ausgewählte Maschine auf Erfüllung der unter Tests zur Überprüfung aufgeführten Kriterien. Wenn eine Maschine die Überprüfung nicht besteht, wird eine Meldung in der Spalte Status angezeigt und das Kontrollkästchen deaktiviert. Sie haben nun folgende Möglichkeiten:

- Beheben Sie das Problem und aktivieren Sie das Kontrollkästchen erneut. Dadurch wird eine Wiederholung des Tests ausgelöst.
- Überspringen Sie die Maschine (Kontrollkästchen deaktiviert lassen). Auf ihr werden dann keine Ablaufverfolgungs-/Diagnosedaten gesammelt.

Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.

Schritt 3. Tracingbericht.

Die Zusammenfassung enthält alle Maschinen, auf denen Ablaufverfolgungsdaten gesammelt werden. Klicken Sie auf **Ablaufverfolgung starten**.

Reproduzieren Sie auf einer oder mehreren Maschinen das aufgetretene Problem. Währenddessen wird die Ablaufverfolgung fortgesetzt. Wenn Sie das Problem reproduziert haben, klicken Sie in Scout auf **Weiter**. Damit wird die Ablaufverfolgung beendet.

Nach dem Beenden der Ablaufverfolgung geben Sie an, ob Sie das Problem reproduziert haben.

Schritt 4. Sammeln Sie Diagnosedaten von den Maschinen.

Klicken Sie auf **Sammeln**.

Während der Sammlung geschieht Folgendes:

- In der Spalte Status wird der aktuelle Status der Sammlung für die Maschinen angezeigt.
- Um die laufende Sammlung für eine einzelne Maschine zu stoppen, klicken Sie in der Spalte "Aktion"für diese Maschine auf **Abbrechen**.
- Um alle laufenden Sammlungen zu stoppen, klicken Sie unten rechts auf der Seite auf **Sammlung stoppen**. Diagnosedaten von Maschinen, deren Sammlung abgeschlossen war, werden beibehalten. Zum Fortsetzen der Sammlung klicken Sie in der Spalte "Aktion"für jede Maschine auf **Wiederholen**.

- Wenn die Sammlung für alle ausgewählten Maschinen abgeschlossen ist, ändert sich die Schaltfläche **Sammlung stoppen** in der unteren rechten Ecke in **Weiter**.
- Um die Diagnosedaten einer Maschine nach erfolgreicher Erfassung erneut zu erfassen, klicken Sie in der Spalte **Aktion** der betreffenden Maschine auf Erneut sammeln. Die neuere Sammlung überschreibt die ältere.
- Schlägt eine Sammlung fehl, können Sie in der Spalte "Aktion"auf **Wiederholen** klicken. Nur erfolgreiche Sammlungen werden hochgeladen oder gespeichert.
- Wenn die Sammlung für alle ausgewählten Maschinen abgeschlossen ist, klicken Sie NICHT auf **Zurück**. Wenn Sie auf diese Schaltfläche klicken und die Aktion bestätigen, geht die Sammlung verloren.

Wenn die Sammlung abgeschlossen ist, klicken Sie auf **Weiter**.

Schritt 5. Sammlung speichern oder hochladen.

Wählen Sie, ob die Datei mit den Diagnosedaten an Citrix hochgeladen oder auf der lokalen Maschine gespeichert werden soll.

Wenn Sie die Datei hochladen, fahren Sie mit Schritt 6 fort.

Wenn Sie die Datei lokal speichern:

- Es wird ein Windows-Dialogfeld zum Speichern angezeigt. Wählen Sie den gewünschten Speicherort.
- Wenn die lokale Speicherung abgeschlossen ist, wird der Pfad der Datei angezeigt und verlinkt. Sie können die Datei anzeigen. Sie können die Datei später an Citrix hochladen. Informationen hierzu finden Sie unter CTX136396 (Citrix Insight Services) oder Citrix Smart Tools.

Klicken Sie auf **Fertig**, um zur Scout-Startseite zurückzukehren. Sie brauchen keine weiteren Schritte auszuführen.

Schritt 6. Authentifizieren Sie sich für Uploads und geben Sie optional den Proxy an.

Einzelheiten zu diesem Verfahren finden Sie unter Uploadautorisierung.

- Wenn Sie sich noch nicht über Scout authentifiziert haben, fahren Sie mit diesem Schritt fort.
- Wenn Sie bereits über Scout authentifiziert sind, wird das gespeicherte Autorisierungstoken standardmäßig verwendet. Wenn Sie damit einverstanden sind, wählen Sie diese Option und klicken Sie auf **Weiter**. Sie müssen keine Anmeldeinformationen für diese Sammlung eingeben. Fahren Sie mit Schritt 7 fort.
- Wenn Sie sich bereits authentifiziert haben, jedoch ein neues Token wünschen, klicken Sie auf **Ändern/Neu autorisieren** und fahren Sie mit diesem Schritt fort.

Wählen Sie aus, ob Sie Citrix Konto- oder Citrix Cloud-Anmeldeinformationen für die Authentifizierung des Uploads verwenden möchten. Klicken Sie auf **Weiter**. Die Seite für die Anmeldeinformationen wird nur angezeigt, wenn Sie das gespeicherte Token nicht verwenden.

Führen Sie auf der Seite "Anmeldeinformationen"folgende Schritte aus:

- Wenn Sie einen Proxyserver für den Dateiupload verwenden möchten, klicken Sie auf **Proxy konfigurieren**. Wenn Sie beim Upload von Sammlungen an Citrix einen Proxyserver verwenden möchten, können Sie Scout zur Verwendung der Internet-Proxyeinstellungen Ihres Browsers konfigurieren oder die IP-Adresse und Portnummer des Proxyservers angeben. Schließen Sie das Proxydialogfeld.
- Bei Verwendung eines Citrix Cloud-Kontos klicken Sie auf **Token generieren**. Der Standardbrowser wird mit einer Citrix Cloud-Seite gestartet, auf der ein Token angezeigt wird. Kopieren Sie das Token und fügen Sie es auf der Scout-Seite ein.
- Wenn Sie ein Citrix Konto verwenden, geben Sie die zugehörigen Anmeldeinformationen ein.

Wenn Sie fertig sind, klicken Sie auf **Weiter**.

Schritt 7. Geben Sie Informationen zum Upload an.

Geben Sie folgende Informationen zum Upload ein:

- Das Feld "Name"enthält den Standardnamen für die Datei mit den gesammelten Diagnosedaten. Er eignet sich für die meisten Sammlungen, Sie können ihn aber ändern. Wenn Sie die Standardnamen löschen und das Namensfeld leer lassen, wird der Standardname verwendet.
- Geben Sie optional eine 8-stellige Citrix-Supportfallnummer ein.
- Geben Sie optional im Feld Beschreibung eine Beschreibung des Problems ein und geben Sie ggf. an, wann es aufgetreten ist.

Wenn Sie fertig sind, klicken Sie auf **Upload starten**.

Während des Uploads wird unten links auf der Seite der ungefähre Prozentsatz hochgeladener Daten angezeigt. Um einen laufenden Upload abzubrechen, klicken Sie auf **Upload stoppen**.

Wenn der Upload abgeschlossen ist, wird die URL des Speicherorts angezeigt und verlinkt. Sie können den Link kopieren oder über ihn zu dem Speicherort bei Citrix navigieren und eine Uploadanalyse anzeigen.

Klicken Sie auf **Fertig**, um zur Scout-Startseite zurückzukehren.

Planen der Sammlung

Das Verfahren zum Planen umfasst die Auswahl der Maschinen und die Einrichtung des Zeitplans (bzw. dessen Stornierung). Geplante Sammlungen werden automatisch an Citrix hochgeladen. Sie können geplante Sammlungen über die PowerShell-Schnittstelle lokal speichern. Informationen finden Sie unter Citrix Call Home.

Schritt 1. Starten Sie Scout.

Wählen Sie im Startmenü der Maschine **Citrix > Citrix Scout**. Wählen Sie **Zeitplan**.

Schritt 2. Maschinen auswählen.

Auf der Seite "Maschinen wählen"werden alle VDAs und Controller der Site aufgelistet. Sie können die Anzeige nach Maschinennamen filtern.

Bei der Installation von VDAs und Controllern über die grafische Benutzeroberfläche wurde die Option zur Teilnahme an Call Home angeboten. Weitere Informationen finden Sie unter Citrix Call Home. Call Home enthält wie Scout Zeitplanfunktionen. In Scout werden diese Einstellungen standardmäßig angezeigt. Sie können mit dieser Version von Scout einen neuen Zeitplan einrichten oder einen zuvor konfigurierten Zeitplan ändern.

Hinweis: Sie aktivieren/deaktivieren Call Home zwar für einzelne Maschinen, doch wenn Sie einen Zeitplan in Scout festlegen, gelten die gleichen Befehle für alle Maschinen, die Sie auswählen.

Aktivieren Sie das Kontrollkästchen neben jeder Maschine, auf der Sie Diagnosedaten sammeln möchten, und klicken Sie auf **Weiter**.

Scout überprüft automatisch jede ausgewählte Maschine auf Erfüllung der unter Tests zur Überprüfung aufgeführten Kriterien. Wenn eine Maschine die Überprüfung nicht besteht, wird eine Meldung in der Spalte Status angezeigt und das Kontrollkästchen deaktiviert. Sie haben nun folgende Möglichkeiten:

- Beheben Sie das Problem und aktivieren Sie das Kontrollkästchen erneut. Dadurch wird eine Wiederholung des Tests ausgelöst.
- Überspringen Sie die Maschine (Kontrollkästchen deaktiviert lassen). Auf ihr werden dann keine Diagnosedaten (oder Ablaufverfolgungsdaten) gesammelt.

Nach Abschluss der Überprüfung klicken Sie auf **Weiter**.

Auf der Seite Zusammenfassung werden die Maschinen aufgelistet, auf die der Zeitplan angewendet wird. Klicken Sie auf **Weiter**.

Schritt 3. Legen Sie den Zeitplan fest.

Geben Sie an, wann die Diagnosedaten gesammelt werden sollen. Nicht vergessen: Der Zeitplan gilt für alle ausgewählten Maschinen.

- Zum Konfigurieren eines wöchentlichen Zeitplans für die ausgewählten Maschinen klicken Sie auf **Wöchentlich**. Wählen Sie den Wochentag und geben Sie die Uhrzeit an, zu der die Datensammlung beginnen soll.
- Zum Konfigurieren eines täglichen Zeitplans für die ausgewählten Maschinen klicken Sie auf **Täglich**. Geben Sie die Uhrzeit an, zu der die Datensammlung beginnen soll.
- Zum Stornieren eines Zeitplans für die ausgewählten Maschinen, ohne diesen durch einen neuen zu ersetzen, klicken Sie auf **Aus**. Dadurch wird jeder Zeitplan storniert, der für diese Maschinen konfiguriert war.

Klicken Sie auf **Weiter**.

Schritt 4. Authentifizieren Sie sich für Uploads und geben Sie optional den Proxy an.

Einzelheiten zu diesem Verfahren finden Sie unter Uploadautorisierung. Nicht vergessen: Sie können kein gespeichertes Token zur Authentifizierung verwenden, wenn Sie mit einem Scout-Zeitplan arbeiten.

Wählen Sie aus, ob Sie Citrix Konto- oder Citrix Cloud-Anmeldeinformationen für die Authentifizierung des Uploads verwenden möchten. Klicken Sie auf **Weiter**.

Führen Sie auf der Seite "Anmeldeinformationen"folgende Schritte aus:

- Wenn Sie einen Proxyserver für den Dateiupload verwenden möchten, klicken Sie auf Proxy konfigurieren. Wenn Sie beim Upload von Sammlungen an Citrix einen Proxyserver verwenden möchten, können Sie Scout zur Verwendung der Internet-Proxyeinstellungen Ihres Browsers konfigurieren oder die IP-Adresse und Portnummer des Proxyservers angeben. Schließen Sie das Proxydialogfeld.
- Bei Verwendung eines Citrix Cloud-Kontos klicken Sie auf **Token generieren**. Der Standardbrowser wird mit einer Citrix Cloud-Seite gestartet, auf der ein Token angezeigt wird. Kopieren Sie das Token und fügen Sie es auf der Scout-Seite ein.
- Wenn Sie ein Citrix Konto verwenden, geben Sie die zugehörigen Anmeldeinformationen ein.

Wenn Sie fertig sind, klicken Sie auf **Weiter**.

Überprüfen Sie den konfigurierten Zeitplan. Klicken Sie auf **Fertig**, um zur Scout-Startseite zurückzukehren.

Für jede geplante Sammlung werden im Windows-Anwendungsprotokoll aller ausgewählten Maschinen entsprechende Einträge verzeichnet.

Überwachung

August 18, 2021

Administratoren und Helpdeskmitarbeiter können XenApp und XenDesktop-Sites mit einer Reihe von Features und Tools überwachen. Sie können Folgendes überwachen

- Benutzersitzungen und Sitzungsverwendung
- Anmeldungsleistung
- Verbindungen und Computer, einschließlich Ausfälle
- Lastauswertung
- Historische Trends
- Infrastruktur

Citrix Director

Director ist ein Echtzeitwebtool, mit dem Sie Endbenutzer überwachen, Fehler beheben und Support leisten können.

Weitere Informationen finden Sie in den Artikeln zu Director.

Sitzungsaufzeichnung

Die Sitzungsaufzeichnung ermöglicht das Aufzeichnen von Bildschirmaktivitäten in der Sitzung eines Benutzers über eine beliebige Verbindung von einem XenApp-Server (im Einklang mit den Unternehmensrichtlinien und gesetzlichen Vorschriften). Mit der Sitzungsaufzeichnung können Sie Sitzungen aufzeichnen, katalogisieren und archivieren und sie erneut aufrufen und wiedergeben.

Die Sitzungsaufzeichnung verwendet flexible Richtlinien, mit denen automatisch Aufnahmen von Anwendungssitzungen ausgelöst werden können. Das IT-Team kann damit die Benutzeraktivität von Anwendungen überwachen und prüfen, z. B. Buchhaltungs- und Patienteninformationssysteme für das Gesundheitswesen, und interne Kontrollen zur Einhaltung von gesetzlichen Vorschriften und die Sicherheitsüberwachung unterstützen. Die Sitzungsaufzeichnung vereinfacht auch den technischen Support, da die Problemerkennung und Behebung der Probleme beschleunigt werden.

Weitere Informationen finden Sie in den Artikeln zur Sitzungsaufzeichnung.

Konfigurationsprotokollierung

Die Konfigurationsprotokollierung ist ein Feature, mit dem Administratoren administrative Änderungen verfolgen, die an einer Site vorgenommen werden. Die Konfigurationsprotokollierung ermöglicht Administratoren die Diagnose und Problembehandlung nach der Durchführung von Konfigurationsänderungen, Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen sowie Berichte über Administratoraktivitäten.

Sie können Berichte mit protokollierten Informationen über Studio generieren und anzeigen. Zum Zweck der Benachrichtigung über Konfigurationsänderungen können Sie protokollierte Elemente außerdem in der Trendansicht von Director anzeigen. Dieses Feature ist für Administratoren nützlich, die keinen Zugriff auf Studio haben.

Die Trendansicht bietet historische Daten von Konfigurationsänderungen in einem bestimmten Zeitraum, sodass Administratoren beurteilen können, welche Änderungen wann und von wem an einer Site vorgenommen wurden, um die Ursache eines Problems zu finden. Konfigurationsinformationen werden in dieser Ansicht in drei Kategorien unterteilt.

- Verbindungsfehler
- Fehlgeschlagene Desktopmaschinen

- Fehlgeschlagene Servermaschinen

Weitere Informationen zum Aktivieren und Konfigurieren der Konfigurationsprotokollierung finden Sie unter Konfigurationsprotokollierung. Im Artikel Director wird beschrieben, wie protokollierte Informationen über dieses Tool angezeigt werden.

Ereignisprotokolle

In XenApp und XenDesktop-Diensten werden Ereignisse protokolliert. Ereignisprotokolle können zur Überwachung und Problembehandlung verwendet werden.

Weitere Informationen finden Sie im Artikel Ereignisprotokolle. Artikel zu einzelnen Features enthalten auch Informationen zu Ereignissen.

Sitzungsaufzeichnung 7.15

October 30, 2019

Die Sitzungsaufzeichnung ermöglicht das Aufzeichnen von Bildschirmaktivitäten in einer auf einem VDA für Server- oder Desktopbetriebssystemmaschinen gehosteten Sitzung eines Benutzers über eine beliebige Verbindung (im Einklang mit den Unternehmensrichtlinien und gesetzlichen Vorschriften). Mit der Sitzungsaufzeichnung können Sie Sitzungen aufzeichnen, katalogisieren und archivieren und sie erneut aufrufen und wiedergeben.

Die Sitzungsaufzeichnung bietet flexible Richtlinien, mit denen automatisch Aufnahmen von Anwendungs- und Desktopsitzungen ausgelöst werden können. Mit der Sitzungsaufzeichnung kann die IT die Benutzeraktivität in Anwendungs- und Desktopsitzungen überwachen und untersuchen. Sie unterstützt daher interne Kontrollen zur Einhaltung gesetzlicher Vorschriften und zur Sicherheitsüberwachung. Die Sitzungsaufzeichnung vereinfacht auch den technischen Support, da die Problemerkennung und Behebung der Probleme beschleunigt werden.

Vorteile

Erhöhte Sicherheit durch Protokollierung und Überwachung. Mit der Sitzungsaufzeichnung können Unternehmen die Aktivität der Benutzer auf dem Bildschirm für Anwendungen aufzeichnen, die vertrauliche Informationen verarbeiten. Dies ist besonders in stark regulierten Branchen wichtig, z. B. im Gesundheits- und Finanzwesen. Richtliniensteuerelemente ermöglichen eine selektive Aufzeichnung, wenn persönliche Daten ins Spiel kommen, die nicht aufgezeichnet werden dürfen.

Leistungsfähige Aktivitätsüberwachung. Die Sitzungsaufzeichnung erfasst und archiviert Bildschirmaktualisierungen, einschließlich Mausklicks und die visuelle Ausgabe von Tastaturanschlägen in gesicherten Videoaufzeichnungen, um die Aktivität für bestimmte Benutzer, Anwendungen und Server zu dokumentieren.

Die Sitzungsaufzeichnung ist nicht dafür ausgelegt oder vorgesehen, Beweismittel für Rechtsverfahren zu sammeln. Citrix empfiehlt, dass Unternehmen, die die Sitzungsaufzeichnung verwenden, andere Methoden der Beweismittelsammlung nutzen, z. B. konventionelle Videoaufzeichnungen in Kombination mit textbasierten eDiscovery-Tools.

Schnellere Problembehebung. Wenn sich Benutzer mit einem Problem an den Helpdesk wenden, das schwer zu reproduzieren ist, können die Supportmitarbeiter die Aufzeichnung von Benutzersitzungen aktivieren. Wenn das Problem wieder auftritt, stellt die Sitzungsaufzeichnung eine visuelle Aufzeichnung des Fehlers bereit, einschließlich Zeitstempel, mit der Benutzerprobleme schneller gelöst werden können.

Erste Schritte mit der Sitzungsaufzeichnung

April 17, 2020

Nach dem Durchführen der folgenden Schritte können Sie XenApp- und XenDesktop-Sitzungen aufzeichnen und prüfen.

1. Machen Sie sich mit den Komponenten der Sitzungsaufzeichnung vertraut.
2. Wählen Sie das Bereitstellungsszenario für die Umgebung.
3. Prüfen Sie die Installationsanforderungen.
4. Installieren Sie die erforderlichen Windows-Rollen und -Features.
5. Installieren Sie die Sitzungsaufzeichnung.
6. Konfigurieren Sie die Sitzungsaufzeichnungskomponenten für das Aufzeichnen und Anzeigen von Sitzungen.

Die Sitzungsaufzeichnung besteht aus fünf Komponenten:

- **Sitzungsaufzeichnungsagent:** Komponente, die auf jedem VDA für Server- bzw. Desktopbetriebssysteme zum Ermöglichen der Aufzeichnungen installiert wird. Mit dieser Komponente werden Sitzungsdaten aufgezeichnet.
- **Sitzungsaufzeichnungsserver:** Ein Server, auf dem die folgenden Programme ausgeführt werden:
  - Broker: Eine von IIS 6.0+ gehostete Webanwendung, die Such- und Dateidownloadanfragen vom Player und Richtlinienverwaltungsanforderungen von der Sitzungsaufzeichnungs-

Richtlinienkonsole handhabt und Aufzeichnungsrichtlinien für jede XenApp- und XenDesktop-Sitzung auswertet.
  - Speichermanager: Ein Windows-Dienst, der Sitzungsaufzeichnungsdateien verwaltet, die von jedem für die Sitzungsaufzeichnung aktivierten Computer mit XenApp bzw. XenDesktop empfangen werden.
  - Administratorprotokollierung: Optionale Teilkomponente, die auf dem Sitzungsaufzeichnungsserver zum Protokollieren von Verwaltungsaktivitäten installiert wird. Alle Protokollierungsdaten werden in einer separaten SQL Server-Datenbank gespeichert, die standardmäßig **CitrixSessionRecordingLogging** heißt. Sie können den Datenbanknamen anpassen.

- **Sitzungsaufzeichnungsplayer:** Eine Benutzeroberfläche, auf die Benutzer von der Arbeitsstation aus zugreifen und mit der aufgezeichnete XenApp- bzw. XenDesktop-Sitzungsdateien wiedergegeben werden.
- **Datenbank für die Sitzungsaufzeichnung:** Eine Komponente, die die SQL Server-Datenbank zum Speichern von Sitzungsaufzeichnungsdaten verwaltet. Wenn diese Komponente installiert ist, erstellt sie standardmäßig eine Datenbank mit dem Namen **CitrixSessionRecording**. Sie können den Datenbanknamen anpassen.
- **Richtlinienkonsole für die Sitzungsaufzeichnung.** Konsole zum Erstellen von Richtlinien, um anzugeben, welche Sitzungen aufgezeichnet werden sollen.

In dieser Abbildung werden die Komponenten der Sitzungsaufzeichnung und deren Beziehung zueinander dargestellt:

Im dargestellten Beispiel einer Bereitstellung befinden sich der Sitzungsaufzeichnungsagent, der Sitzungsaufzeichnungsserver, die Datenbank für die Sitzungsaufzeichnung, die Richtlinienkonsole für die Sitzungsaufzeichnung und der Sitzungsaufzeichnungsplayer hinter einer Sicherheitsfirewall. Der Sitzungsaufzeichnungsagent ist auf einem VDA für Server- oder Desktopbetriebssysteme installiert. Auf einem zweiten Server wird die Richtlinienkonsole für die Sitzungsaufzeichnung ausgeführt, ein dritter Server ist der Sitzungsaufzeichnungsserver und auf einem vierten Server wird die Datenbank für die Sitzungsaufzeichnung ausgeführt. Der Sitzungsaufzeichnungsplayer ist auf einer Arbeitsstation installiert. Ein Clientgerät außerhalb der Firewall kommuniziert mit dem VDA für Serverbetriebssysteme auf dem der Sitzungsaufzeichnungsagent installiert ist. Innerhalb der Firewall kommunizieren der Sitzungsaufzeichnungsagent, die Richtlinienkonsole für die Sitzungsaufzeichnung, der Sitzungsaufzeichnungsplayer und die Datenbank für die Sitzungsaufzeichnung mit dem Sitzungsaufzeichnungsserver.

Planen der Bereitstellung

August 18, 2021

Einschränkungen und Hinweise

Die Sitzungsaufzeichnung unterstützt nicht den Anzeigemodus der Desktopgestaltungsumleitung (DCR). Wenn eine Sitzung gemäß Aufzeichnungsrichtlinie aufgezeichnet werden muss, deaktiviert die Sitzungsaufzeichnung standardmäßig DCR für diese Sitzung. Sie können dieses Verhalten in den Eigenschaften des Sitzungsaufzeichnungsagents konfigurieren.

Die Sitzungsaufzeichnung unterstützt den Framehawk-Anzeigemodus nicht. Sitzungen im Framehawk-Anzeigemodus können nicht aufgezeichnet und einwandfrei wiedergegeben werden. Im Framehawk-Modus aufgezeichnete Sitzungen enthalten ggf. keine Sitzungsaktivitäten.

Die Sitzungsaufzeichnung kann keine Lync-Webcamvideos aufzeichnen, wenn das HDX RealTime Optimization Pack verwendet wird.

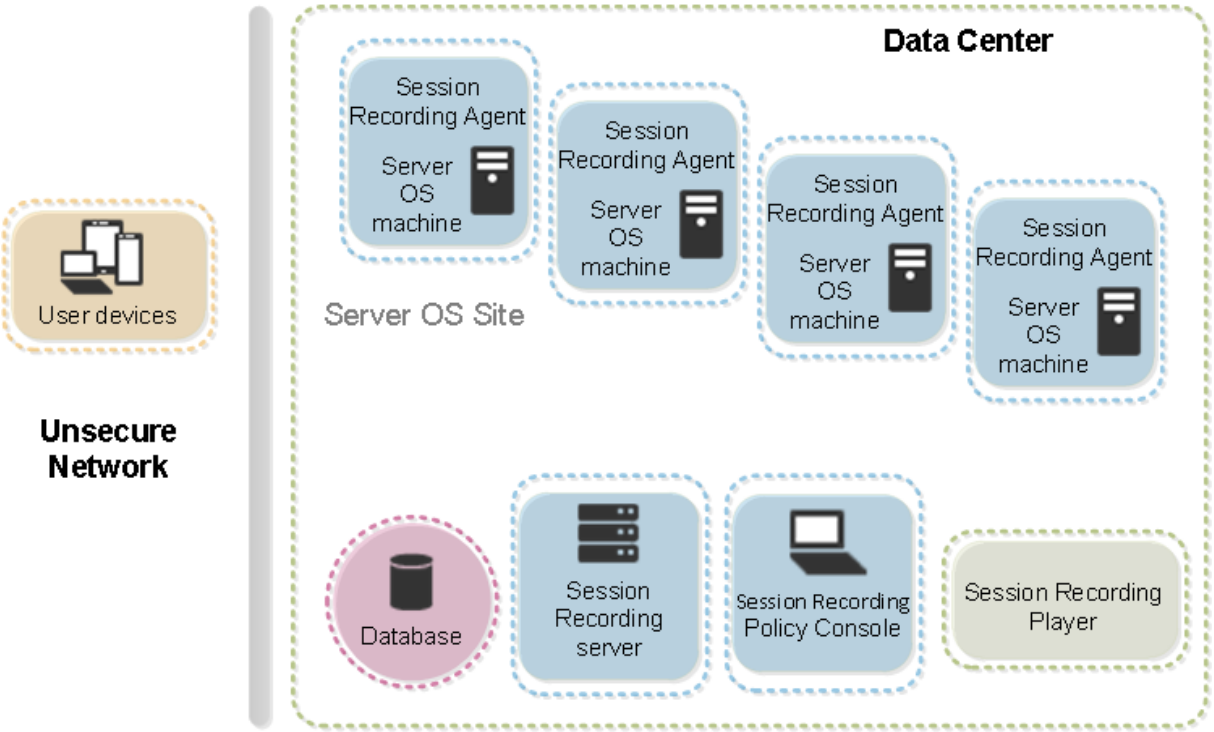
Abhängig von der Umgebung können Sie die Sitzungsaufzeichnungskomponenten in verschiedenen Szenarios bereitstellen.

Eine Sitzungsaufzeichnungsbereitstellung muss nicht auf eine Site begrenzt sein. Mit Ausnahme des Sitzungsaufzeichnungsagents sind alle Komponenten von der Serversite unabhängig. Sie können beispielsweise mehrere Sites für einen Sitzungsaufzeichnungsserver konfigurieren.

Wenn Sie jedoch eine große Site mit vielen Instanzen der Agentsoftware haben und viele grafikintensive Anwendungen (z. B. AutoCAD-Anwendungen) oder viele Sitzungen aufzeichnen möchten, kann dies zu einem hohen Leistungsbedarf auf einem Sitzungsaufzeichnungsserver führen. Sie können zur Vermeidung von Leistungsproblemen mehrere Sitzungsaufzeichnungsserver auf verschiedenen Maschinen installieren und die Instanzen des Sitzungsaufzeichnungsagents auf verschiedene Maschinen verweisen. Vergessen Sie jedoch nicht, dass eine Instanz der Agentsoftware nur jeweils auf einen Server verweisen kann.

Empfohlene Serversitebereitstellung

Verwenden Sie diesen Typ der Bereitstellung für die Aufzeichnung von Sitzungen für eine oder mehrere Sites. Der Sitzungsaufzeichnungsagent wird auf jedem VDA für Serverbetriebssysteme der Site installiert. Die Site befindet sich in einem Datencenter hinter einer Sicherheitsfirewall. Die Komponenten der Sitzungsaufzeichnungsverwaltung (Datenbank für die Sitzungsaufzeichnung, Sitzungsaufzeichnungsserver und Richtlinienkonsole für die Sitzungsaufzeichnung) sind außerhalb des Datencenters hinter der Firewall auf anderen Servern und der Sitzungsaufzeichnungsplayer ist auf einer Arbeitsstation installiert.



Wichtige Bereitstellungshinweise

- Die Komponenten der Sitzungsaufzeichnung können nur miteinander kommunizieren, wenn sie in derselben Domäne oder in vertrauenswürdigen Domänen mit einer gegenseitigen Vertrauensbeziehung installiert sind. Das System kann nicht in einer Arbeitsgruppe oder in Domänen mit einer externen Vertrauensbeziehung installiert werden.
- Aufgrund des hohen Grafikanteils und der Speichernutzung bei der Wiedergabe von großen Aufzeichnungen, empfehlen wir, dass der Sitzungsaufzeichnungsplayer nicht als veröffentlichte Anwendung installiert wird.
- Die Installation der Sitzungsaufzeichnung ist für die TLS/HTTPS-Kommunikation konfiguriert. Stellen Sie sicher, dass Sie ein Zertifikat auf dem Sitzungsaufzeichnungsserver installieren, und dass die Komponenten der Sitzungsaufzeichnung der Stammzertifizierungsstelle vertrauen.
- Wenn Sie die Datenbank für die Sitzungsaufzeichnung auf einem eigenständigen Server mit SQL Server 2016 Express Edition, SQL Server 2014 Express Edition, SQL Server 2012 Express Edition oder SQL Server 2008 R2 Express Edition ausführen, muss auf dem Server das TCP/IP-Protokoll aktiviert sein und der SQL Server-Browserdienst muss ausgeführt werden. Diese Einstellungen sind standardmäßig deaktiviert, müssen jedoch für die Kommunikation zwischen dem Sitzungsaufzeichnungsserver und der Datenbank aktiviert werden. Informationen zur Aktivierung dieser Einstellungen finden Sie in den Microsoft-Artikeln Enable TCP/IP Network Protocol for SQL Server und SQL Server Browser Service.
- Berücksichtigen Sie bei der Planung der Sitzungsaufzeichnungsbereitstellung die Auswirkun-

gen der Sitzungsfreigabe. Die Sitzungsfreigabe für veröffentlichte Anwendungen kann Konflikte mit Richtlinienregeln für Sitzungsaufzeichnungen für veröffentlichte Anwendungen verursachen. Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet. Wenn der Benutzer die erste Anwendung geöffnet hat, halten weitere Anwendungen, die in derselben Sitzung geöffnet werden, die Richtlinie ein, die für die erste Anwendung gilt. Beispiel: Wenn eine Richtlinie festlegt, dass nur Outlook aufgezeichnet wird, beginnt die Aufzeichnung, wenn der Benutzer Outlook öffnet. Wenn der Benutzer jedoch Microsoft Word als zweite veröffentlichte Anwendung öffnet (während Outlook ausgeführt wird), wird Word auch aufgezeichnet. Sollte die aktive Richtlinie jedoch nicht festlegen, dass Word aufgezeichnet wird, und der Benutzer startet Word vor Outlook (gemäß der Richtlinie wird Outlook aufgezeichnet), wird Outlook nicht aufgezeichnet.

- Das Installieren des Sitzungsaufzeichnungsservers auf einem Delivery Controller kann zu Leistungsbeeinträchtigungen führen und wir empfehlen es daher nicht; es ist jedoch grundsätzlich möglich.
- Sie können die Richtlinienkonsole für die Sitzungsaufzeichnung auf einem Delivery Controller installieren.
- Sie können den Sitzungsaufzeichnungsserver und die Richtlinienkonsole für die Sitzungsaufzeichnung auf demselben System installieren.
- Stellen Sie sicher, dass der NetBIOS-Name des Sitzungsaufzeichnungsservers nicht länger als 15 Zeichen ist (Microsoft begrenzt die Länge des Hostnamens auf max. 15 Zeichen).
- PowerShell 5.1 oder höher ist für die benutzerdefinierte Ereignisprotokollierung erforderlich. Aktualisieren Sie PowerShell, wenn Sie den Sitzungsaufzeichnungsagent unter Windows Server 2012 R2 installieren, für das PowerShell 4.0 installiert ist. Die Nichteinhaltung kann zu fehlgeschlagenen API-Aufrufen führen.

Sicherheitsempfehlungen

August 18, 2021

Die Sitzungsaufzeichnung wird in einem sicheren Netzwerk mit Zugriff durch Administratoren bereitgestellt und ist daher sicher. Die Standardbereitstellung ist einfach, und Sicherheitsfunktionen, z. B. digitale Signatur und Verschlüsselung, können optional konfiguriert werden.

Die Komponenten der Sitzungsaufzeichnung kommunizieren über die Internetinformationsdienste (IIS) und Microsoft Message Queuing (MSMQ). Internetinformationsdienste stellen die Webdienste-Kommunikationsverbindung zwischen den Komponenten der Sitzungsaufzeichnung bereit. MSMQ bietet eine zuverlässige Datentransportmethode zum Senden von Sitzungsaufzeichnungsdaten vom Sitzungsaufzeichnungsagent zum Sitzungsaufzeichnungsserver.

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Berücksichtigen Sie diese Sicherheitsempfehlungen bei der Planung der Bereitstellung:

- Die verschiedenen Administratorrollen im Unternehmensnetzwerk, in der Sitzungsaufzeichnung und auf einzelnen Maschinen müssen ordnungsgemäß isoliert werden. Andernfalls besteht Gefahr durch Sicherheitsbedrohungen Gefahr für den Systembetrieb und das System kann zweckentfremdet verwendet werden. Wir empfehlen, dass Sie unterschiedliche Administratorrollen verschiedenen Personen oder Konten zuweisen. Erteilen Sie normalen Sitzungsbenutzern keine Administratorprivilegien für das VDA-System.
  - Administratoren von XenApp und XenDesktop erteilen keinem Benutzer von veröffentlichten Anwendungen oder Desktops die lokale Administratorrolle für den VDA. Wird die lokale Administratorrolle benötigt, schützen Sie die Komponenten des Sitzungsaufzeichnungsagents über Windows-Methoden oder die Lösung eines anderen Herstellers.
  - Weisen Sie die Administratorrollen für die Datenbank und die Richtlinie der Sitzungsaufzeichnung separat zu.
  - Wir empfehlen, dass Sie VDA-Administratorrechte nicht allgemeinen Sitzungsbenutzern zuweisen, besonders, wenn Remote-PC-Zugriff verwendet wird.
  - Das lokale Administratorkonto des Sitzungsaufzeichnungsservers muss streng geschützt werden.
  - Steuern Sie den Zugriff auf Maschinen, auf denen der Sitzungsaufzeichnungsplayer installiert ist. Hat ein Benutzer keine Playerrollenberechtigung, weisen Sie ihm für keinerlei Player-Maschinen eine lokale Administratorrolle zu. Deaktivieren Sie den anonymen Zugriff.
  - Wir empfehlen, eine physische Maschine als Speicherserver für die Sitzungsaufzeichnung zu verwenden.
- Die Sitzungsaufzeichnung zeichnet Grafikaktivitäten ohne Berücksichtigung des Datenschutzes auf. Unter bestimmten Umständen können sensible Daten (z. B. Benutzeranmeldeinformationen, persönliche Daten oder Bildschirme von Drittanbietern) unbeabsichtigt aufgezeichnet werden. Ergreifen Sie folgende Maßnahmen, um ein Risiko zu vermeiden:
  - Deaktivieren Sie das Kernspeicherabbild für VDAs, es sei denn, es wird zur Problembehandlung benötigt.

Zum Deaktivieren des Kernspeicherabbilds gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Erweitert** und dann unter **Starten und Wiederherstellen** auf **Einstellungen**.
3. Wählen Sie für **Debuginformationen speichern** die Option **Keine**.

Weitere Informationen finden Sie im Microsoft-Artikel unter https://support.microsoft.com/en-us/kb/307973.

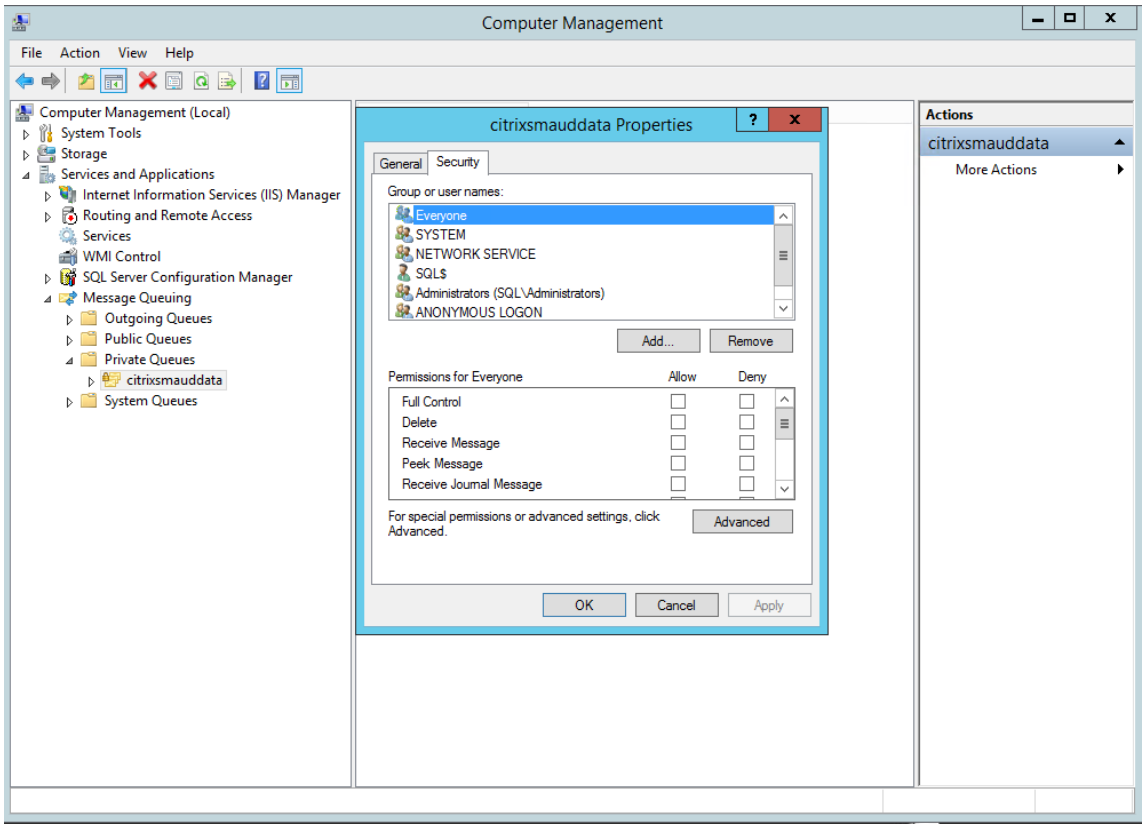
- Sitzungseigentümer machen die Teilnehmer darauf aufmerksam, dass Software von Online-Meetings und Remoteunterstützung im Rahmen einer Desktopsitzungsaufzeichnung aufgezeichnet werden kann.
- Stellen Sie sicher, dass keine Anmelde- und Sicherheitsinformationen in veröffentlichten lokalen Anwendungen oder Webanwendungen oder unternehmensintern verwendeten Anwendungen angezeigt werden. Andernfalls werden die Informationen durch die Sitzungsaufzeichnung aufgezeichnet.
- Schließen Sie vor Beginn einer ICA-Sitzung jede Anwendung, in der u. U. vertrauliche Informationen angezeigt werden.
- Für den Zugriff auf veröffentlichte Desktops oder SaaS-Anwendungen wird ausschließlich der Einsatz automatischer Authentifizierungsmethoden (z. B. Single Sign-On oder Smartcard) empfohlen.

- Zur ordnungsgemäßen Funktion und zur Erfüllung von Sicherheitsanforderungen bei der Sitzungsaufzeichnung ist eine spezifische Hardware/-infrastruktur (z. B. Unternehmensnetzwerkgeräte, Betriebssystem) erforderlich. Sorgen Sie auf Infrastrukturebene dafür, dass diese Elemente weder beschädigt noch missbraucht werden können und dass die Sitzungsaufzeichnung sicher und zuverlässig ausgeführt wird.
  - Schützen und Sie die für die Sitzungsaufzeichnung verwendete Netzwerkinfrastruktur und sorgen Sie für deren zuverlässige Verfügbarkeit.
  - Wir empfehlen, eine Sicherheitslösung eines Drittanbieters oder Windows-Mechanismen zum Schutz der Sitzungsaufzeichnungskomponenten zu verwenden. Die Sitzungsaufzeichnung umfasst folgende Komponenten:
    - Auf dem Sitzungsaufzeichnungsserver
      - Prozesse: SsRecStoragemanager.exe und SsRecAnalyticsService.exe
      - Dienste: CitrixSsRecStorageManager und CitrixSsRecAnalyticsService
      - Alle Dateien im Installationsordner des Sitzungsaufzeichnungsservers
      - Registrierungswerte unter HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server
    - Auf dem Sitzungsaufzeichnungsagent

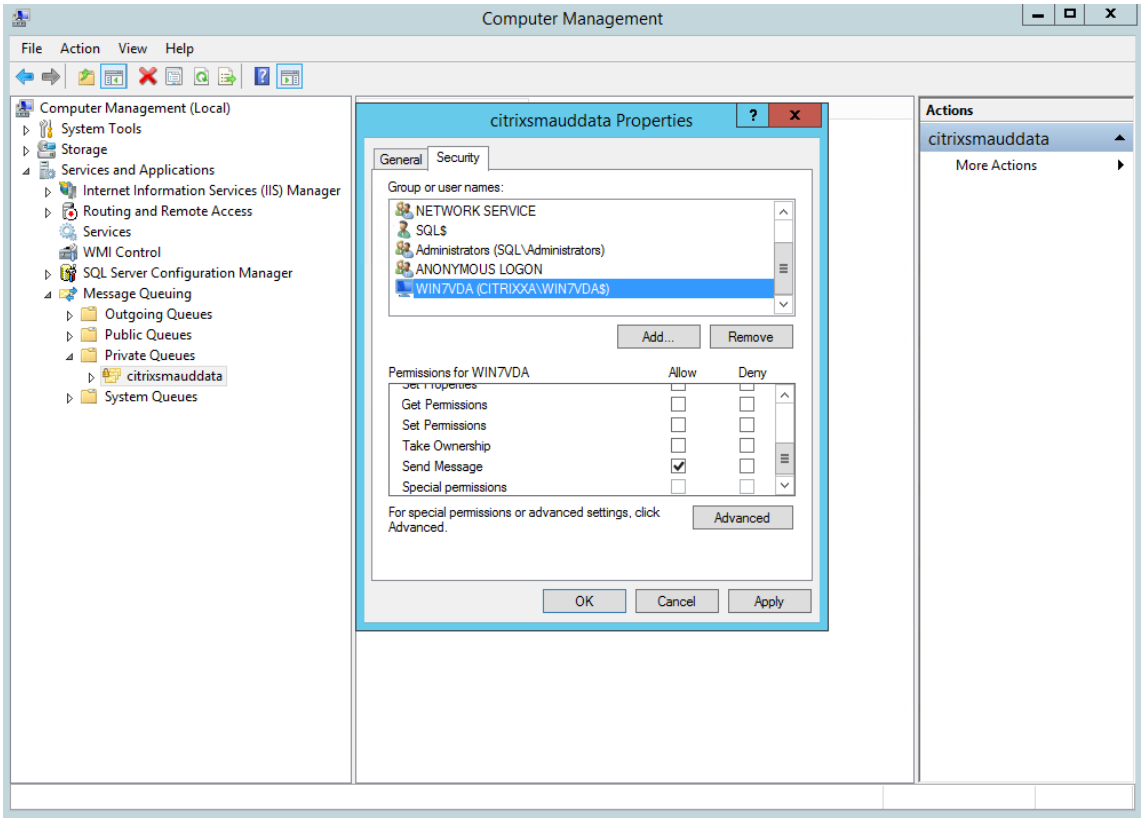
- Prozess: SsRecAgent.exe
- Dienst: CitrixSmAudAgent
- Alle Dateien im Installationsordner des Sitzungsaufzeichnungsagents
- Registrierungswerte unter HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent

- Schränken Sie über die Zugriffssteuerungsliste (ACL) für Message Queuing (MSMQ) auf dem Sitzungsaufzeichnungsserver VDA- und VDI-Maschinen ein, die MSMQ-Daten an den Sitzungsaufzeichnungsserver senden können, und blockieren Sie das Senden von Daten an den Sitzungsaufzeichnungsserver durch unbefugte Maschinen.

1. Installieren Sie das Serverfeature Directory Service Integration auf jeder Sitzungsaufzeichnungsserver- und VDA- oder VDI-Maschine, auf der die Sitzungsaufzeichnung aktiviert ist. Starten Sie dann den Message Queuing-Dienst neu.
2. Öffnen Sie auf jedem Sitzungsaufzeichnungsserver über das **Startmenü** von Windows **Verwaltungstools** > **Computerverwaltung**.
3. Öffnen Sie **Dienste und Anwendungen** > **Message Queuing** > **Private Warteschlangen**.
4. Klicken Sie auf die private Warteschlange **citrixsmauddata**, um die Seite **Eigenschaften** zu öffnen, und wählen Sie die Registerkarte **Sicherheit**.



5. Fügen Sie die Computer bzw. Sicherheitsgruppen der VDAs, die MSMQ-Daten an diesen Server senden, hinzu und erteilen Sie diesen die Berechtigung zum **Senden von Nachrichten**.



- Schützen Sie das Ereignisprotokoll des Sitzungsaufzeichnungsservers und des Sitzungsaufzeichnungsagents. Citrix empfiehlt die Verwendung einer Remoteprotokollierungslösung eines Drittanbieters oder eines entsprechenden Windows-Features zum Schutz des Ereignisprotokolls oder dessen Umleitung auf einen Remoteserver.
- Stellen Sie sicher, dass die Server mit den Sitzungsaufzeichnungskomponenten physisch geschützt werden. Schließen Sie diese Computer falls möglich in einem sicheren Raum ein, zu dem nur autorisierte Person direkten Zugang haben.
- Isolieren Sie die Server mit den Sitzungsaufzeichnungskomponenten in einem separaten Subnetz oder einer separaten Domäne.
- Installieren Sie eine Firewall zwischen dem Sitzungsaufzeichnungsserver und den anderen Servern, um die aufgezeichneten Sitzungsdaten vor Benutzern zu schützen, die auf andere Server zugreifen.
- Halten Sie den Verwaltungsserver und die SQL-Datenbank für die Sitzungsaufzeichnung durch Installation der aktuellen Sicherheitsupdates von Microsoft auf dem neuesten Stand.
- Verhindern Sie, dass Personen ohne Administratorberechtigung sich beim Verwaltungscomputer anmelden.
- Schränken Sie genau ein, welche Benutzer die Aufzeichnungsrichtlinien ändern und Sitzungsaufzeichnungen anzeigen können.

- Installieren Sie digitale Zertifikate, verwenden Sie die Funktion zur Dateisignatur der Sitzungsaufzeichnung und richten Sie die TLS-Kommunikation in IIS ein.
- Richten Sie MSMQ ein und legen Sie als Transportprotokoll HTTPS fest. Legen Sie zu diesem Zweck das MSMQ-Transportprotokoll in **Sitzungsaufzeichnungsagent - Eigenschaften** auf HTTPS fest. Weitere Informationen finden Sie unter Problembehandlung bei MSMQ.
- Verwenden Sie TLS 1.1 oder TLS 1.2 (empfohlen) und deaktivieren Sie die Verschlüsselungsverfahren SSLv2, SSLv3 und TLS 1.0 auf dem Sitzungsaufzeichnungsserver und in der Datenbank für die Sitzungsaufzeichnung. Weitere Informationen finden Sie im Microsoft-Artikel https://support.microsoft.com/default.aspx?scid=kb;en-us;187498.

  Deaktivieren Sie die RC4-Verschlüsselungssammlungen für TLS auf dem Sitzungsaufzeichnungsserver und in der Datenbank für die Sitzungsaufzeichnung:

1. Navigieren Sie mit dem Microsoft Gruppenrichtlinien-Editor zu **Computerkonfiguration** > **Administrative Vorlagen** > **Netzwerk** > **SSL-Konfigurationseinstellungen**.
2. Legen Sie die Richtlinie **Reihenfolge der SSL-Verschlüsselungssammlungen** auf **Aktiviert** fest. Standardmäßig ist diese Richtlinie auf **Nicht konfiguriert** festgelegt.
3. Entfernen Sie alle RC4-Verschlüsselungssammlungen.

- Verwenden Sie den Wiedergabeschutz. Der Wiedergabeschutz ist eine Funktion der Sitzungsaufzeichnung, mit der aufgezeichnete Dateien vor dem Download zum Sitzungsaufzeichnungsplayer verschlüsselt werden. Diese Option ist in der Standardeinstellung aktiviert und befindet sich in den **Sitzungsaufzeichnungsserver - Eigenschaften**.
- Folgen Sie den Anleitungen von NSIT für die Länge der Kryptografieschlüssel und den Kryptografiealgorithmen.
- Konfigurieren Sie TLS 1.2-Unterstützung für die Sitzungsaufzeichnung.
  - Wir empfehlen, TLS 1.2 als Kommunikationsprotokoll zu verwenden, um eine lückenlose Sicherheit für die Sitzungsaufzeichnungskomponenten sicherzustellen.
    Konfigurieren der TLS 1.2-Unterstützung für die Sitzungsaufzeichnung:
    1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an. Installieren Sie die erforderlichen SQL Server-Clientkomponenten und -Treiber und legen Sie für .NET Framework (Version 4 oder höher) starke Kryptografie fest.
    1. Installieren Sie Microsoft ODBC Driver 11 (oder eine neuere Version) for SQL Server.
    2. Wenden Sie das aktuelle Hotfix-Rollup für .NET Framework an.
    3. Installieren Sie `ADO.NET - SqlClient` gemäß Ihrer Version von .NET Framework. Weitere Informationen finden Sie unter https://support.microsoft.com/en-us/kb/3135244.
    4. Fügen Sie DWORD-Wert SchUseStrongCrypto = 1 hinzu unter HKEY_LOCAL_MACHINE\SOFTWARE\M und HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319.

5. Starten Sie die Maschine neu.
   2. Melden Sie sich bei der Maschine mit der Richtlinienkonsole für die Sitzungsaufzeichnung an. Wenden Sie das aktuelle Hotfix-Rollup für .NET Framework an und legen Sie für .NET Framework (Version 4 oder höher) starke Kryptografie fest. Die Methode zum Festlegen von starker Kryptografie ist identisch mit den Schritten 1-d und 1-e. Sie können diese Schritte auslassen, wenn Sie die Richtlinienkonsole für die Sitzungsaufzeichnung auf demselben Computer wie den Sitzungsaufzeichnungsserver installieren.

Informationen zum Konfigurieren der TLS 1.2-Unterstützung für SQL Server-Versionen vor 2016 finden Sie unter https://support.microsoft.com/en-us/kb/3135244. Zur Verwendung von TLS 1.2 konfigurieren Sie HTTPS als Kommunikationsprotokoll für die Komponenten der Sitzungsaufzeichnung.

Weitere Informationen über die Konfiguration der Sicherheitsfeatures für die Sitzungsaufzeichnung finden Sie unter Konfigurieren von Sicherheitsfunktionen für die Sitzungsaufzeichnung.

Überlegungen zur Skalierbarkeit

August 18, 2021

Die Sitzungsaufzeichnung ist ein hochskalierbares System, das zehntausende Sitzungen verarbeiten kann. Zum Installieren und Ausführen der Sitzungsaufzeichnung sind nur wenige Ressourcen erforderlich, die nicht schon für XenApp und XenDesktop gebraucht werden. Wenn Sie jedoch viele Sitzungen mit der Sitzungsaufzeichnung aufzeichnen möchten oder die Sitzungen, die Sie aufzeichnen möchten, möglicherweise große Sitzungsdateien erstellen (z. B. Anwendungen mit hohem Grafikanteil), sollten Sie die Leistung des Systems berücksichtigen, wenn Sie die Bereitstellung der Sitzungsaufzeichnung planen.

In diesem Artikel werden die Grundlagen der hohen Skalierbarkeit der Sitzungsaufzeichnung behandelt und es wird erläutert, wie Sie das System mit möglichst geringem Kostenaufwand optimal nutzen können.

Faktoren für die gute Skalierbarkeit der Sitzungsaufzeichnung

Es gibt zwei Hauptgründe für die im Vergleich zu Produkten von Mitbewerbern gute Skalierbarkeit der Sitzungsaufzeichnung:

- Kleine Dateigröße

  Mit der Sitzungsaufzeichnung erstellte Aufzeichnungsdateien sind extrem kompakt. Sie sind um ein Vielfaches kleiner als äquivalente Videoaufnahmen, die von auf Screen Scraping basieren-

den Lösungen erstellt werden. Für die Übermittlung und Speicherung von Sitzungsaufzeichnungsdateien ist der Bedarf an Netzwerkbandbreite, Festplattenspeicher und Datenträger-IOPS in der Regel mindestens zehnmal geringer als bei äquivalenten Videodateien.

Die geringe Größe von Sitzungsaufzeichnungsdateien sorgt für eine schnellere und nahtlosere Wiedergabe von Videobildern. Die Aufzeichnung ist zudem verlustfrei und weist im Gegensatz zu den meisten kompakten Videoformaten keinerlei Pixelierung auf. Text in Aufzeichnungen ist bei der Wiedergabe genauso leicht zu lesen wie in der ursprünglichen Sitzung. Zur Minimierung der Dateigrößen werden bei der Sitzungsaufzeichnung keine Keyframes innerhalb von Dateien aufgezeichnet.

- Geringer Verarbeitungsaufwand zum Generieren von Dateien

  Eine Sitzungsaufzeichnungsdatei enthält die ICA-Protokolldaten für eine Sitzung, die virtuell im nativen Format extrahiert werden. Die Datei erfasst somit den ICA-Protokolldatenstrom, der für die Kommunikation mit der Citrix Workspace-App verwendet wird. Es müssen keine teuren Transcodierer oder Encoder zur Formatumwandlung in Echtzeit ausgeführt werden. Der geringe Verarbeitungsaufwand ist auch für die VDA-Skalierbarkeit wichtig und gewährleistet eine gute Benutzererfahrung, wenn ein VDA viele Sitzungen aufzeichnet.

  Darüber hinaus werden nur die virtuellen ICA-Kanäle aufgezeichnet, die wiedergegeben werden können –eine weitere Optimierung. Beispielsweise werden der Drucker- und Clientlaufwerkzuordnungskanal nicht aufgezeichnet, da sie hohe Datenmengen erzeugen und ohne Vorteil für die Videowiedergabe sind.

Schätzung der Dateneingabe- und Verarbeitungsraten

Der Sitzungsaufzeichnungsserver ist der zentrale Sammelpunkt für Sitzungsaufzeichnungsdateien. Jede Maschine mit Multisitzungs-OS und aktivierter Sitzungsaufzeichnung sendet Sitzungsaufzeichnungsdaten an den Sitzungsaufzeichnungsserver. Die Sitzungsaufzeichnung kann große Datenmengen verarbeiten und ist burst- und fehlertolerant. Es gibt jedoch physische Limits für die Datenmenge, die einzelne Server verarbeiten können.

Berücksichtigen Sie, wie viele Daten an jeden Sitzungsaufzeichnungsserver gesendet werden und wie schnell die Server diese Daten verarbeiten und speichern können. Die Rate, mit der das System die eingehenden Daten speichern kann, muss größer als die Dateneingaberate sein.

Sie können die Dateneingaberate schätzen, wenn Sie die Anzahl der aufgezeichneten Sitzungen mit der durchschnittlichen Größe jeder Sitzungsaufzeichnung multiplizieren und durch die Länge der Sitzungsaufzeichnungen dividieren. Beispiel: An einem 8-stündigen Arbeitstag zeichnen Sie 5000 Microsoft Outlook-Sitzungen auf, deren Größe 20 MB ist. Die Dateneingaberate beträgt dann ungefähr 3,5 MBit/s (5000 Sitzungen multipliziert mit 20 MB und dividiert durch 8 Stunden, dividiert durch 3600 Sekunden pro Stunde.) Ein an ein 100-MBit/s-LAN angeschlossener Sitzungsaufzeichnungsserver mit

ausreichend Festplattenspeicher für die aufgezeichneten Daten kann basierend auf den physischen Limits durch Datenträger- und Netzwerk-IOPS in der Regel rund 5,0 MBit Daten pro Sekunde verarbeiten. Diese Rate ist die Verarbeitungsrate. In diesem Beispiel ist die Verarbeitungsrate (5,0 MBit/s) höher als die Eingaberate (3,5 MBit/s) und die Aufzeichnung der 5.000 Outlook-Sitzungen ist somit möglich.

Die pro Sitzung entstehenden Datenmengen variieren stark, je nachdem, was aufgezeichnet wird. Auch andere Faktoren wie Bildschirmauflösung, Farbtiefe und Grafikmodus haben Auswirkungen. Eine Sitzung, in der eine CAD-Anwendung mit konstant hoher Grafikaktivität ausgeführt wird, generiert wesentlich mehr Aufzeichnungsdaten als eine Sitzung, in der E-Mail in Microsoft Outlook gesendet und empfangen wird. Daher kann die Aufzeichnung einer identischen Anzahl CAD-Sitzungen eine extrem hohe Eingaberate aufweisen und die Verwendung zusätzlicher Sitzungsaufzeichnungsserver erfordern.

Bursts und Fehler

Das obige Beispiel basiert auf einem sehr einfachen und konstanten Datendurchsatz und berücksichtigt keine Bursts –kurze Zeiträume mit höherer Aktivität. Ein Burst kann beispielsweise morgens auftreten, wenn sich alle Benutzer zur gleichen Zeit anmelden, oder wenn alle Benutzer die gleiche E-Mail im Outlook-Posteingang erhalten. Die Verarbeitungsrate des Sitzungsaufzeichnungsservers von 5,0 MBit/s ist zur Bewältigung eines solchen Bursts äußerst unzureichend.

Der auf jedem VDA ausgeführte Sitzungsaufzeichnungsagent sendet aufgezeichnete Daten unter Einsatz von Microsoft Message Queuing (MSMQ) an den Speichermanager, der auf dem zentralen Sitzungsaufzeichnungsserver ausgeführt wird. Die Daten werden im Teilstreckenverfahren (store and forward) gesendet, ähnlich wie E-Mail, die vom Absender über einen Mailserver an den Empfänger gesendet wird. Wenn der Sitzungsaufzeichnungsserver oder das Netzwerk die hohe Datenrate eines Bursts nicht verarbeiten kann, werden die aufgezeichneten Sitzungsdaten vorübergehend gespeichert, bis die aufgelaufenen Datennachrichten verarbeitet sind. Datennachrichten werden, wenn das Netzwerk überlastet ist, in der Ausgangswarteschlange auf dem VDA zwischengespeichert oder aber in der Eingangswarteschlange des Sitzungsaufzeichnungsservers, wenn sie bereits das Netzwerk durchlaufen haben und der Speichermanager noch andere Nachrichten verarbeitet.

MSMQ dient auch als Fehlertoleranzmechanismus. Fällt der Sitzungsaufzeichnungsserver aus oder wird die Verbindung unterbrochen, dann werden aufgezeichnete Daten in der Ausgangswarteschlange auf den VDAs gespeichert. Nach Beseitigung des Fehlers werden alle Daten in den Warteschlangen zusammen gesendet. Die Verwendung von MSMQ ermöglicht außerdem das Offlineschalten eines Sitzungsaufzeichnungsservers für Upgrades oder Wartungszwecke, ohne dass die Aufzeichnung bestehender Sitzungen unterbrochen wird und Daten verloren gehen.

Die Haupteinschränkung von MSMQ besteht darin, dass der Speicherplatz für die temporäre Speicherung von Datennachrichten begrenzt ist. Diese Größe bestimmt, wie lange ein Burst-, Fehler- oder

Wartungsereignis dauern kann, bis Daten verloren gehen. Das Gesamtsystem kann nach Datenverlust weiter ausgeführt werden, doch fehlen in diesem Fall Datenblöcke in einzelnen Aufzeichnungen. Eine Datei mit fehlenden Daten kann zwar wiedergegeben werden, doch nur bis zu dem Punkt des ersten Datenverlusts. Beachten Sie Folgendes:

- Die Ausstattung aller Server und insbesondere des Sitzungsaufzeichnungsservers mit mehr Speicherplatz und dessen Bereitstellung für MSMQ kann die Burst- und Fehlertoleranz erhöhen.
- Es ist wichtig, die Einstellung "Nachrichtenlebensdauer"(auf der Registerkarte **Verbindungen** in den Agenteigenschaften) für jeden Sitzungsaufzeichnungsagent auf einen geeigneten Wert festzulegen. Der Standardwert von 7.200 Sekunden (zwei Stunden) bedeutet, dass aufgezeichnete Datennachrichten zwei Stunden haben, um den Speichermanager zu erreichen. Nach Ablauf dieses Zeitraums werden sie verworfen und die Aufzeichnungsdateien werden beschädigt. Wenn mehr Speicherplatz verfügbar ist (oder weniger Sitzungen aufgezeichnet werden), können Sie diesen Wert erhöhen. Der maximale Wert beträgt 365 Tage.

Die andere Einschränkung bei MSMQ besteht darin, dass es bei einem Auflaufen von Daten in der Warteschlange zu zusätzlichen IOPS für das Lesen und Schreiben von Datennachrichten kommt. Unter normalen Bedingungen empfängt und verarbeitet der Speichermanager Daten direkt aus dem Netzwerk, ohne dass Datennachrichten auf den Datenträger geschrieben werden. Das Speichern der Daten erfordert einen Schreibvorgang auf dem Datenträger, der die Sitzungsaufzeichnungsdatei anfügt. Bei einem Auflaufen von Daten verdreifachen sich die Datenträger-IOPS: Jede Nachricht muss auf den Datenträger geschrieben, von diesem gelesen und in eine Datei geschrieben werden. Da der Speichermanager sehr IOPS-gebunden ist, sinkt die Verarbeitungsrate des Sitzungsaufzeichnungsservers, bis die aufgelaufenen Nachrichten verarbeitet sind. Zur Minderung der Auswirkungen dieser zusätzlichen IOPS wird Folgendes empfohlen:

- Stellen Sie sicher, dass MSMQ Nachrichten auf einem anderen Datenträger speichert als dem, auf dem die Aufzeichnungsdateien gespeichert werden. Obwohl sich der IOPS-Wert verdreifacht, sinkt die reale Verarbeitungsrate nicht im gleichen Maß.
- Sorgen Sie dafür, dass geplante Ausfälle nur zu Nebenzeiten stattfinden. Befolgen Sie, soweit Ihr Budget dies erlaubt, anerkannte Verfahren zum Erstellen hoch verfügbarer Server. Dazu gehören der Einsatz von UPS, duale Netzwerkkarten, redundante Switches und per Hot-Swap austauschbare Arbeitsspeicher und Datenträger.

Planung mit Kapazitätsreserve

Die Datenrate der Sitzungsaufzeichnung ist in der Regel uneinheitlich, es sind Bursts und Fehler möglich und die Verarbeitung aufgelaufener Nachrichten erzeugt einen hohen IOPS-Wert. Die Sitzungsaufzeichnungsserver sollten daher über reichlich Kapazitätsreserven verfügen. Das Hinzufügen weiterer Server oder die Aufrüstung vorhandener Server (Erläuterungen hierzu weiter unten)

kann die Kapazität erhöhen. Als allgemeine Faustregel sollte ein Sitzungsaufzeichnungsserver bei maximal 50 % Gesamtkapazität ausgeführt werden. Kann ein Server 5,0 MBit/s verarbeiten, sollten Sie ihn nur mit 2,5 MBit/s ausführen. Statt der Aufzeichnung von 5.000 Outlook-Sitzungen, die 3,5 Mbit/s auf einem Sitzungsaufzeichnungsserver generieren, lassen Sie 3.500 Sitzungen aufzeichnen, die nur etwa 2,5 MBit/s generieren.

Datenrückstau und Livewiedergabe

Bei der Livewiedergabe wird eine Sitzungsaufzeichnung noch während der laufenden Sitzung zur Wiedergabe geöffnet. Bei der Livewiedergabe wechselt der für die Sitzung zuständige Sitzungsaufzeichnungsagent in den Streamingmodus und die Aufzeichnungsdaten werden direkt und ohne interne Pufferung an den Speichermanager gesendet. Da die Aufnahmedatei ständig aktualisiert wird, erhält der Player weiterhin die neuesten Daten aus der Livesitzung. Die Daten werden vom Agent allerdings über MSMQ an den Speichermanager gesendet, weshalb die o. g. Warteschlangenregeln gelten. In diesem Szenario kann ein Problem auftreten. Bei einem Datenrückstau in MSMQ werden die neuen Aufzeichnungsdaten für die Livewiedergabe wie alle anderen Datennachrichten in die Warteschlange gestellt. Die Datei kann zwar weiterhin wiedergegeben werden, doch die Anzeige der neuesten Liveaufzeichnungen verzögert sich. Ist die Livewiedergabe ein wichtiges Feature, sorgen Sie durch Kapazitätsreserven und Fehlertoleranz dafür, dass die Wahrscheinlichkeit eines Datenrückstaus gering ist.

Skalierbarkeit von XenApp und XenDesktop

Die Sitzungsaufzeichnung verringert nie die Sitzungsleistung und hält bei einem Datenrückstau nie eine Sitzung an. Der Fokus des Sitzungsaufzeichnungssystems richtet sich auf die Aufrechterhaltung der Benutzererfahrung und der Einzelserver-Skalierbarkeit. Bei einer irreversiblen Überlastung werden aufgezeichnete Sitzungsdaten verworfen. Umfangreiche Skalierbarkeitstests von Citrix haben ergeben, dass die Aufzeichnung von ICA-Sitzungen nur geringe Auswirkungen auf die Leistung und Skalierbarkeit von XenApp und XenDesktop-Servern hat. Der Grad der Auswirkungen hängt von der Plattform, dem verfügbaren Arbeitsspeicher und der Art der aufgezeichneten Sitzungen ab. Bei der nachfolgend aufgeführten Konfiguration ist mit einer Verringerung der Einzelserver-Leistung zwischen 1 % und 5 % rechnen. Anders gesagt: Wenn ein Server ohne Sitzungsaufzeichnung 100 Benutzer hosten kann, kann er bei installierter Sitzungsaufzeichnung 95 bis 99 Benutzer hosten.

- 64-Bit-Server mit 8 GB RAM und einem VDA mit Multisitzungs-OS
- In allen Sitzungen werden Office-Anwendungen wie Outlook oder Excel ausgeführt.
- Die Anwendungen werden aktiv und dauerhaft genutzt.
- Alle Sitzungen werden gemäß den Richtlinien für die Sitzungsaufzeichnung aufgezeichnet.

Werden weniger Sitzungen aufgezeichnet oder ist die Sitzungsaktivität eher sporadisch, sind die Auswirkungen geringer. In vielen Fällen sind die Skalierbarkeitsauswirkungen vernachlässigbar und die Benutzerdichte pro Server bleibt gleich. Wie bereits erwähnt, sind die geringen Auswirkung auf die einfachen Verarbeitungsanforderungen der auf den VDAs installierten Sitzungsaufzeichnungskomponenten zurückzuführen. Aufzeichnungsdaten werden einfach aus dem ICA-Sitzungsstack extrahiert und unverändert über MSMQ an den Sitzungsaufzeichnungsserver gesendet. Es ist keine teure Datencodierung erforderlich.

Selbst wenn keine Sitzungen aufgezeichnet werden, besteht ein geringfügiger Mehraufwand für die Sitzungsaufzeichnung. Die Auswirkungen sind zwar gering, doch wenn Sie sicher sind, dass von einem Server nie Sitzungen aufgezeichnet werde, können Sie die Aufzeichnung dort deaktivieren. Hierfür können Sie beispielsweise Sitzungsaufzeichnung entfernen. Weniger invasiv ist das Deaktivieren des Kontrollkästchens **Sitzungsaufzeichnung für diese VDA-Maschine aktivieren** auf der Registerkarte **Sitzungsaufzeichnung** in den Eigenschaften des Sitzungsaufzeichnungsagents. Wird die Sitzungsaufzeichnung in Zukunft benötigt, aktivieren Sie das Kontrollkästchen.

Durchsatzmessung

Es gibt verschiedene Möglichkeiten, den Durchsatz der Sitzungsaufzeichnungsdaten vom VDA zum Sitzungsaufzeichnungsserver zu messen. Einer der einfachsten und effektivsten Methoden besteht in der Messung der Größe der Sitzungsaufzeichnungsdateien sowie der Geschwindigkeit, mit der Speicherplatz auf dem Sitzungsaufzeichnungsserver belegt wird. Die Menge auf die Festplatte geschriebener Daten spiegelt fast genau die Menge des generierten Netzwerkdatenverkehrs wider. Die Windows-Leistungsüberwachung (perfmon.exe) bietet eine Reihe von Standardsystemindikatoren, die zusätzlich den Leistungsindikatoren der Sitzungsaufzeichnung geprüft werden können. Die Indikatoren gestatten die Durchsatzmessung und die Identifizierung von Engpässen und Systemproblemen. In der folgenden Tabelle werden die nützlichsten Leistungsindikatoren beschrieben.

Leistungsobjekt	Indikatorname	Beschreibung
Citrix Sitzungsaufzeichnungsagent	Anzahl aktiver Aufzeichnungen	Gibt die Anzahl der Sitzungen an, die aktuell auf einem VDA aufgezeichnet werden.

Leistungsobjekt	Indikatorname	Beschreibung
Citrix Sitzungsaufzeichnungsagent	Vom Sitzungsaufzeichnungstreiber gelesene Bytes	Die Anzahl der von den für das Erfassen von Sitzungsdaten verantwortlichen Kernel-Komponenten gelesenen Bytes. Nützlich zur Ermittlung der Datenmenge, die ein VDA für alle auf dem betreffenden Server aufgezeichneten Sitzungen generiert.
Speichermanager der Citrix Sitzungsaufzeichnung	Anzahl aktiver Aufzeichnungen	Wie beim Leistungsindikator des Citrix Sitzungsaufzeichnungsagents doch im Hinblick auf den Sitzungsaufzeichnungsserver. Gibt die Gesamtzahl der Sitzungen an, die derzeit für alle Server aufgezeichnet werden.
Speichermanager der Citrix Sitzungsaufzeichnung	Message bytes/sec	Durchsatz aller aufgezeichneten Sitzungen. Kann verwendet werden, um die Datenverarbeitungsrate des Speichermanagers zu bestimmen. Bei einem MSMQ-Nachrichtenrückstand wird der Speichermanager mit voller Geschwindigkeit ausgeführt. Anhand dieses Werts kann die maximale Verarbeitungsrate des Speichermanagers angegeben werden.

Leistungsobjekt	Indikatorname	Beschreibung
LogicalDisk	Disk Write Bytes/sec	Kann zur Messung der Datenträger-Schreibleistung verwendet werden. Dies ist wichtig zur Erzielung einer hohen Skalierbarkeit für den Sitzungsaufzeichnungsserver. Auch die Leistung einzelner Laufwerke kann gemessen werden.
MSMQ-Warteschlange	Bytes in Queue	Anhand dieses Leistungsindikators kann die Menge der in der CitrixSmAudData-Warteschlange aufgelaufenen Daten ermittelt werden. Steigt dieser Wert im Laufe der Zeit an, so ist die Rate der vom Netzwerk empfangenen Aufzeichnungsdaten größer als die Datenverarbeitungsrate des Speichermanagers. Dieser Zähler ist nützlich, um die Auswirkungen von Bursts und Fehlern zu beobachten.
MSMQ-Warteschlange	Message in Queue	Ähnlich wie “Bytes in Queue”, jedoch wird die Anzahl der Nachrichten wiedergegeben.

Leistungsobjekt	Indikatorname	Beschreibung
Netzwerkschnittstelle	Bytes Total/sec	Kann an beiden Seiten der Verbindung gemessen werden, um zu ermitteln, wie viele Daten beim Aufzeichnen von Sitzungen generiert werden. Auf dem Sitzungsaufzeichnungsserver gibt dieser Indikator die Rate des Empfangs eingehender Daten an. Dies ist im Unterschied zu dem Leistungsindikator "Message bytes/sec"des Speichermanagers der Citrix Sitzungsaufzeichnung, der die Verarbeitungsrate der Daten wiedergibt. Wenn die Netzwerkrate größer als dieser Wert ist, laufen Nachrichten in der Warteschlange auf.
Prozessor	% Processor Time	Eine Überwachung dieses Indikators lohnt sich, obwohl die CPU als wahrscheinlicher Engpass eher nicht in Frage kommt.

Hardware des Sitzungsaufzeichnungsservers

Sie können die Kapazität Ihrer Bereitstellung durch sorgfältige Auswahl der Hardware für den Sitzungsaufzeichnungsserver erhöhen. Sie können vertikal skalieren (durch Erhöhung der Kapazität der einzelnen Server) oder horizontal (durch Hinzufügen weiterer Server). In beiden Fällen geht es darum, die Kosten möglichst gering zu halten.

Vertikales Skalieren

Für einzelne Sitzungsaufzeichnungsserver folgen Sie den folgenden bewährten Methoden, um die optimale Leistung zum verfügbaren Budget sicherzustellen. Das System ist IOPS-abhängig. Dies

gewährleistet einen hohen Durchsatz von Aufzeichnungsdaten aus dem Netzwerk auf den Datenträger. Daher ist es wichtig, in geeignete Netzwerk- und Datenträgerhardware zu investieren. Für einen leistungsstarken Sitzungsaufzeichnungsserver wird ein Dual- oder Dual-Core-Prozessor empfohlen. Eine höhere Spezifikation bringt keinen nennenswerten Vorteil. Es wird ein 64-Bit-Prozessor empfohlen, doch auch ein x86-Prozessor ist geeignet. 4 GB RAM werden empfohlen, mehr bringt auch hier wenig Nutzen.

Horizontales Skalieren

Selbst bei einer optimalen vertikalen Skalierung gibt es Leistungs- und Skalierbarkeitsgrenzen, die ein einzelner Sitzungsaufzeichnungsserver erreichen kann, wenn eine große Anzahl von Sitzungen aufgezeichnet wird. Unter Umständen sind zusätzliche Server zur Bewältigung der Last erforderlich. Sie können weitere Sitzungsaufzeichnungsserver auf anderen Maschinen installieren, damit die Sitzungsaufzeichnungsserver als Lastausgleichspool fungieren. Bei dieser Art der Bereitstellung teilen sich die Sitzungsaufzeichnungsserver den Speicher und die Datenbank. Um die Last aufzuteilen, verweisen Sie die Sitzungsaufzeichnungsagents auf den Load Balancer, der für die Verteilung der Arbeitslast verantwortlich ist.

Netzwerkkapazität

Ein Netzwerk mit 100 MBit/s ist für die Verbindung eines Sitzungsaufzeichnungsservers geeignet. Eine Gigabit-Ethernet-Verbindung kann die Leistung verbessern, führt jedoch nicht zu einer 10 Mal besseren Leistung als eine Verbindung mit 100 MBit/s. In der Praxis ist der Durchsatzgewinn deutlich geringer.

Stellen Sie sicher, dass Netzwerkswitches, die von der Sitzungsaufzeichnung verwendet werden, nicht mit Anwendungen von Drittherstellern gemeinsam verwendet werden, die ggf. um die verfügbare Netzwerkbandbreite konkurrieren. Netzwerkswitches sollten nur vom Sitzungsaufzeichnungsserver verwendet werden. Wenn sich das Netzwerk als Engpass erweist, bietet ein Netzwerkupgrade eine relativ kostengünstige Möglichkeit zur Erhöhung der Systemleistung.

Speicher

Investitionen in Datenträger- und Speicherhardware sind der wichtigste Faktor für die Serverskalierbarkeit. Je schneller Daten auf den Datenträger geschrieben werden, desto höher ist die Leistung des Gesamtsystems. Berücksichtigen Sie bei der Auswahl einer Speicherlösung die Schreibleistung stärker als die Leseleistung.

Speichern Sie Daten auf lokalen Festplatten, die entweder von einem lokalen Festplattencontroller als als RAID oder als SAN gesteuert werden.

> **Hinweis:**
>
> Das Speichern von Daten in einem NAS mit dateibasiertem Protokoll wie SMB, CIFS oder NFS hat schwerwiegende Auswirkungen auf Leistung und Sicherheit. Verwenden Sie eine solche Konfiguration nie in einer Produktionsbereitstellung der Sitzungsaufzeichnung.

Bei einer Konfiguration mit lokalen Festplatten sollten Sie einen Festplattencontroller mit integriertem Cache verwenden. Caching ermöglicht dem Controller die Verwendung des Aufzug-Algorithmus beim Zurückschreiben, was die Bewegung des Festplattenkopfs minimiert und sicherstellt, dass Schreibvorgänge ohne Warten auf den Abschluss des physischen Festplattenvorgangs ausgeführt werden. Dies kann die Schreibleistung bei minimalen Mehrkosten erheblich verbessern. Beim Caching besteht jedoch das Problem eines möglichen Datenverlusts nach Stromausfall. Zur Gewährleistung der Integrität von Daten und Dateisystem sollten Sie eine batteriegetriebene Backuplösung für den Festplattencontroller mit Cache in Betracht ziehen, die den Cache bei einem Stromausfall aufrecht erhält und dafür sorgt, dass die Daten bei Wiederherstellung der Stromversorgung auf die Festplatte geschrieben werden können.

Erwägen Sie die Verwendung einer geeigneten RAID-Speicherlösung. Je nach Leistungs- und Redundanzanforderungen stehen viele RAID-Level zur Verfügung. In der folgenden Tabelle werden die einzelnen RAID-Level und ihre Eignung für die Sitzungsaufzeichnung angegeben.

RAID-Level	Typ	Mindestanzahl Datenträger	Beschreibung
RAID 0	Mit Striping, ohne Parität	2	Bietet eine hohe Leistung, aber keine Redundanz. Der Verlust eines Datenträgers zerstört das Array. Es ist eine kostengünstige Lösung für die Speicherung von Sitzungsaufzeichnungsdateien, wenn ein Datenverlust nur geringe Auswirkungen hat. Die Leistung kann durch Hinzufügen weiterer Datenträger mühelos erhöht werden.

RAID-Level	Typ	Mindestanzahl Datenträger	Beschreibung
RAID 1	Gespiegelt, ohne Parität	2	Keine größere Leistung als mit einen Datenträger und daher eine relativ kostspielige Lösung. Verwenden Sie diese Lösung nur, wenn eine hohe Redundanz erforderlich ist.
RAID 3	Mit Striping und dedizierter Parität	3	Bietet hohe Schreibleistung mit ähnlichen Redundanzeigenschaften wie RAID 5. RAID 3 wird für die Videoproduktion und Livestreaming empfohlen. Da es sich bei der Sitzungsaufzeichnung um eine Anwendung dieser Art handelt, wird RAID 3 am ehesten empfohlen, es ist jedoch nicht üblich.

RAID-Level	Typ	Mindestanzahl Datenträger	Beschreibung
RAID 5	Mit Striping und verteilter Parität	3	Bietet eine hohe Leseleistung mit Redundanz, jedoch auf Kosten einer geringeren Schreibleistung. RAID 5 ist die am häufigsten die allgemeine Verwendung eingesetzte Lösung. Aufgrund der langsamen Schreibleistung wird RAID 5 jedoch nicht für die Sitzungsaufzeichnung empfohlen. Bei RAID 3 sind die Kosten ähnlich, die Schreibleistung ist aber deutlich besser.
RAID 10	Gespiegelt, mit Striping	4	Bietet Leistungsmerkmale wie RAID 0 mit Redundanz wie RAID 1. Eine teure Lösung, die für die Sitzungsaufzeichnung nicht empfohlen wird.

RAID 0 und RAID 3 sind die empfohlenen RAID-Level. RAID 1 und RAID 5 sind gängige Standards, werden aber für die Sitzungsaufzeichnung nicht empfohlen. RAID 10 bietet einige Leistungsvorteile, doch die Kosten stehen in keinem Vergleich dazu.

Wählen Sie den Typ und die Spezifikation der Laufwerke. IDE/ATA-Laufwerke und externe USB- oder Firewire-Laufwerke sind nicht für die Verwendung für die Sitzungsaufzeichnung geeignet. Die beiden Hauptalternativen sind SATA und SCSI. SATA-Laufwerke bieten im Vergleich zu SCSI-Laufwerken

relativ hohe Übertragungsraten zu geringeren Kosten pro MB. SCSI-Laufwerke bieten jedoch eine bessere Leistung und sind bei Serverbereitstellungen gängiger. Server-RAID-Lösungen unterstützen meist SCSI-Laufwerke, es gibt jetzt aber auch einige SATA-RAID-Produkte. Berücksichtigen Sie bei der Auswahl von Datenträgern die Festplatten-Geschwindigkeit und andere Leistungsmerkmale.

Da die Aufzeichnung von Tausenden von Sitzungen pro Tag erhebliche Mengen an Speicherplatz belegen kann, müssen Sie zwischen Gesamtkapazität und Leistung wählen. Die Aufzeichnung von 5.000 Outlook-Sitzungen des o. g. Beispiels belegt an einem 8-Stunden-Arbeitstag etwa 100 GB Speicherplatz. Zur Speicherung der Aufzeichnungen von 10 Tagen (d. h. 50.000 Sitzungsaufzeichnungsdateien) benötigen Sie 1.000 GB (1 TB). Durch einen kürzeren Aufbewahrungszeitraum vor der Archivierung oder dem Löschen von Aufzeichnungen kann Festplattenspeicher eingespart werden. Steht 1 TB Festplattenspeicher zur Verfügung, ist eine siebentägige Aufbewahrungsfrist sinnvoll, die sicherstellt, dass rund 700 GB Festplattenspeicher belegt werden und 300 GB als Puffer für einen hohen Betrieb zur Verfügung stehen. In der Sitzungsaufzeichnung wird das Archivieren und Löschen von Dateien mit dem ICLDB-Hilfsprogramm unterstützt. Die Mindestaufbewahrungsdauer beträgt zwei Tage. Sie können einen Hintergrundtask planen, der täglich einmal außerhalb der Spitzenzeiten ausgeführt wird. Weitere Informationen zu ICLDB-Befehlen und Archivierung finden Sie unter Verwalten der Datensätze in der Datenbank.

Die Alternative zu lokalen Laufwerken und Controllern ist die Verwendung einer SAN-Speicherlösung mit Datenträgerzugriff auf Blockebene. Auf dem Sitzungsaufzeichnungsserver wird das Datenträgerarray als lokales Laufwerk angezeigt. SANs sind teurer, doch da das Datenträgerarray gemeinsam genutzt wird, ist ihre Verwaltung einfacher und zentral. Es gibt zwei SAN-Haupttypen: Fibre Channel und iSCSI. iSCSI – im Wesentlichen SCSI über TCP/IP – gewinnt seit der Einführung von Gigabit-Ethernet an Beliebtheit gegenüber Fibre Channel.

Datenbankskalierbarkeit

Die Datenbank für die Sitzungsaufzeichnung erfordert Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012 oder Microsoft SQL Server 2008 R2. Die an die Datenbank gesendete Datenmenge ist gering, da dort nur die Metadaten über die aufgezeichneten Sitzungen gespeichert werden. Die Sitzungsaufzeichnungsdateien werden auf einem separaten Datenträger gespeichert. Normalerweise benötigt jede aufgezeichnete Sitzung nur 1 KB in der Datenbank, es sei denn, Sie fügen durchsuchbare Ereignisse mit der Sitzungsaufzeichnungs-Ereignis-API in die Sitzung ein.

Bei den Express-Editionen von Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, und Microsoft SQL Server 2008 R2 ist die Größe der Datenbank auf 10 GB beschränkt. Bei 1 KB pro aufgezeichneter Sitzung kann die Datenbank ungefähr 4.000.000 Sitzungen katalogisieren. Andere Editionen von Microsoft SQL Server haben keine Beschränkungen hinsichtlich Datenbankgröße und werden nur durch den verfügbaren Speicherplatz auf dem Datenträger beschränkt. Wenn die Zahl

der Sitzungen in der Datenbank ansteigt, wird die Leistung der Datenbank und die Geschwindigkeit der Suchen nur geringfügig beeinträchtigt.

Wenn Sie keine Anpassungen über die Sitzungsaufzeichnungs-Ereignis-API machen, generiert jede aufgezeichnete Sitzung vier Datenbanktransaktionen: Zwei beim Start der Aufzeichnung, eine bei der Benutzeranmeldung bei der aufgezeichneten Sitzung und eine am Ende der Aufzeichnung. Beim Anpassen der Sitzungen mit der Sitzungsaufzeichnungs-Ereignis-API erstellt jedes durchsuchbare Ereignis, das aufgezeichnet wurde, eine Transaktion. Da selbst bei der einfachsten Datenbankbereitstellung mehrere Hundert Transaktionen pro Sekunde gehandhabt werden können, wird die Verarbeitungslast für die Datenbank nie überstrapaziert. Die Auswirkung ist so gering, dass die Datenbank für die Sitzungsaufzeichnung normalerweise auf demselben SQL-Server wie andere Datenbanken ausgeführt werden kann, u. a. der XenApp- oder XenDesktop-Datenbank des Datenspeichers.

Wenn Sie in der Bereitstellung der Sitzungsaufzeichnung viele Millionen aufgezeichneter Sitzungen in der Datenbank katalogisieren müssen, halten Sie die Microsoft-Richtlinien zur Skalierbarkeit von SQL Server ein.

Installieren, Aktualisieren und Deinstallieren der Sitzungsaufzeichnung

August 18, 2021

In diesem Kapitel wird beschrieben, wie die Sitzungsaufzeichnung mit dem Installationsprogramm für XenApp/XenDesktop installiert wird. Der Bericht besteht aus den folgenden Abschnitten:

Installationscheckliste

Ab Version 7.14 können Sie die Komponenten der Sitzungsaufzeichnung mit dem Installationsprogramm für XenApp/XenDesktop installieren.

Stellen Sie vor der Installation sicher, dass Sie die in dieser Liste aufgeführten Schritte abgeschlossen haben:

☒	Schritt
	Wählen Sie die Computer aus, auf denen Sie die Komponenten der Sitzungsaufzeichnung installieren möchten, und stellen Sie sicher, dass jeder Computer die Hardware- und Softwareanforderungen für die zu installierenden Komponenten erfüllt. Rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die XenApp- und XenDesktop-Downloadseite auf und laden Sie die Produkt-ISO-Datei herunter. Entpacken Sie die ISO-Datei oder brennen Sie sie auf DVD. Installieren Sie die relevanten Zertifikate in der Umgebung zur Kommunikation zwischen den Komponenten der Sitzungsaufzeichnung per TLS. Installieren Sie die für die Komponenten der Sitzungsaufzeichnung benötigten Hotfixes. Die Hotfixes sind unter Citrix Support verfügbar. Konfigurieren Sie Director zum Erstellen und Aktivieren von Sitzungsaufzeichnungsrichtlinien. Weitere Informationen finden Sie unter Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers.

Hinweis:

- Citrix empfiehlt, die veröffentlichten Anwendungen in separate Bereitstellungsgruppen basierend auf den Aufzeichnungsrichtlinien aufzuteilen, da die Sitzungsfreigabe veröffentlichter Anwendungen einen Konflikt mit aktiven Richtlinien verursachen kann, wenn sie in derselben Bereitstellungsgruppe sind. Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet.
- Wenn Sie beabsichtigen, Maschinenerstellungsdienste (MCS) oder Provisioning Services zu verwenden, bereiten Sie eine eindeutige QMID vor. Wenn Sie dies nicht tun, kann dies zum Verlust von Aufzeichnungsdaten führen.
- Für SQL Server muss TCP/IP aktiviert sein, der SQL Server-Browserdienst muss ausgeführt und die Windows-Authentifizierung muss verwendet werden.

- Zur Verwendung von HTTPS konfigurieren Sie Serverzertifikate für TLS/HTTPS.
- Vergewissern Sie sich unter **Lokale Benutzer und Gruppen** > **Gruppen** > **Benutzer** Schreibberechtigung für den Ordner C:\windows\temp festgelegt ist.

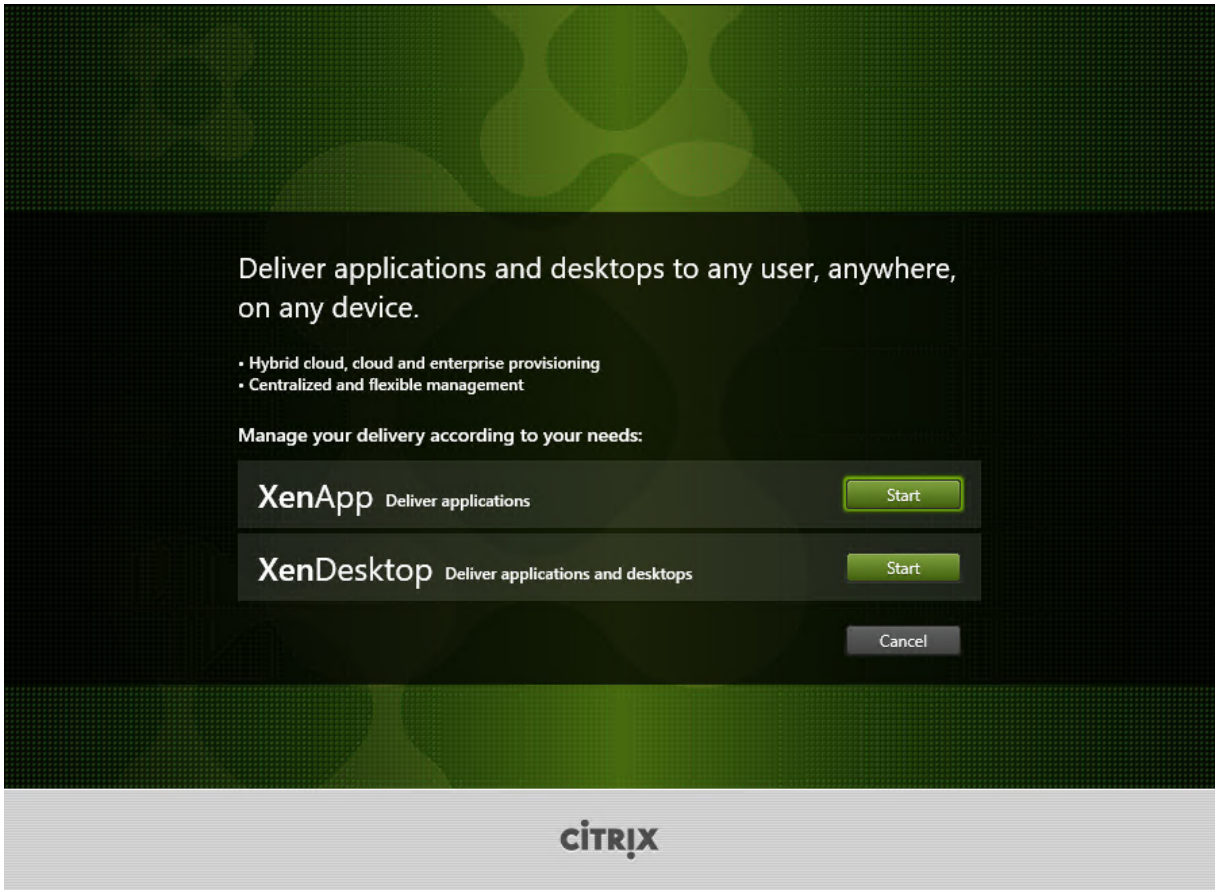
Installieren der Verwaltungskomponenten der Sitzungsaufzeichnung

Citrix empfiehlt die Installation von Sitzungsaufzeichnungsverwaltung, Sitzungsaufzeichnungsagent und Sitzungsaufzeichnungsplayer auf separaten Servern. Die Verwaltungskomponenten der Sitzungsaufzeichnung umfassen die Datenbank für die Sitzungsaufzeichnung, den Sitzungsaufzeichnungsserver und die Richtlinienkonsole für die Sitzungsaufzeichnung. Sie können festlegen, welche dieser Komponenten auf einem Server installiert werden.

Schritt 1: Herunterladen der Produktsoftware und Starten des Assistenten

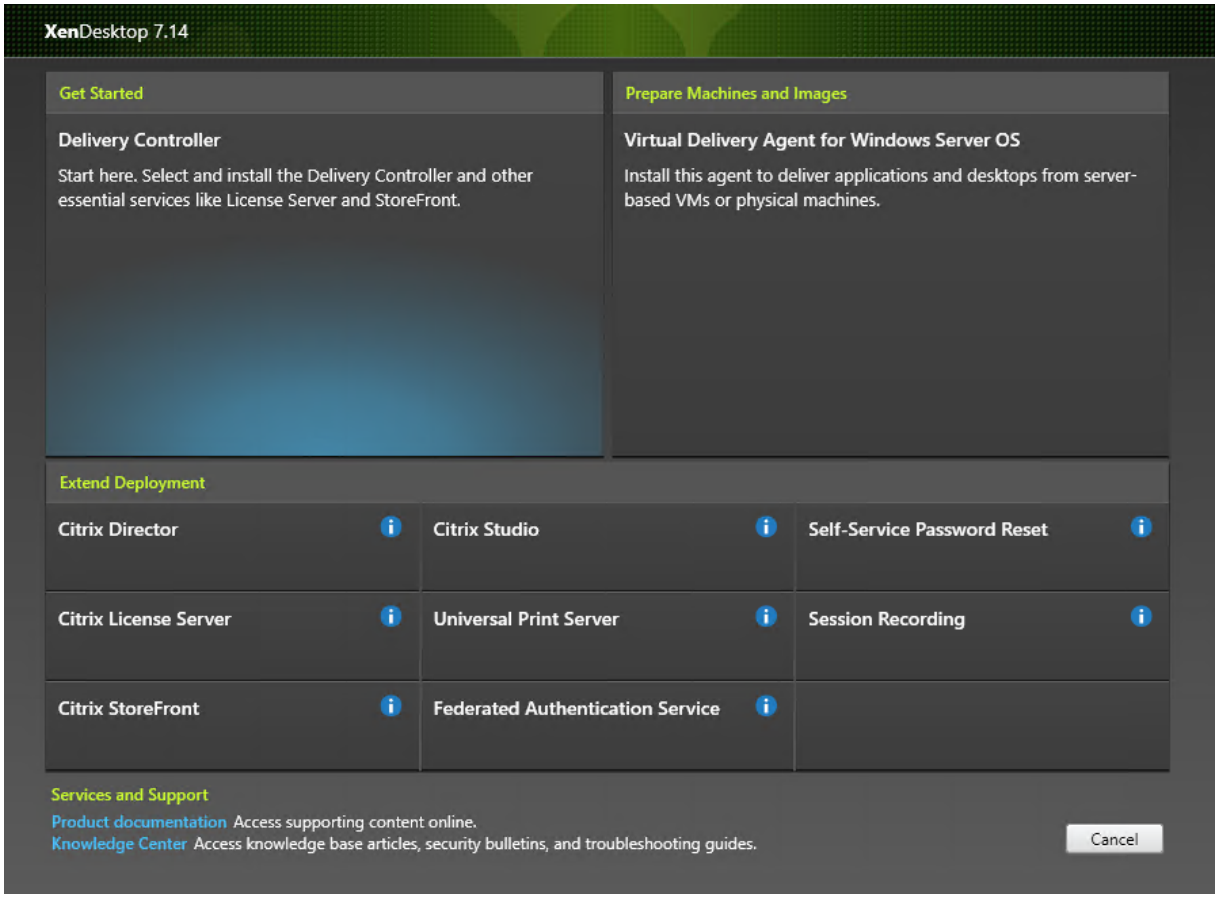
1. Wenn Sie die Produkt-ISO-Datei noch nicht heruntergeladen haben, rufen Sie unter Angabe Ihrer Citrix Anmeldeinformationen die XenApp- und XenDesktop-Downloadseite auf und laden Sie sie herunter. Entpacken Sie die ISO-Datei oder brennen Sie sie auf DVD.
2. Melden Sie sich mit einem lokalen Administratorkonto bei der Maschine an, auf der Sie die Verwaltungskomponenten der Sitzungsaufzeichnung installieren. Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit. Wenn das Installationsprogramm nicht automatisch gestartet wird, doppelklicken Sie auf die Anwendung **AutoSelect** oder das bereitgestellte Laufwerk.
   Der Installationsassistent wird gestartet.

Schritt 2: Auswählen des zu installierenden Produkts



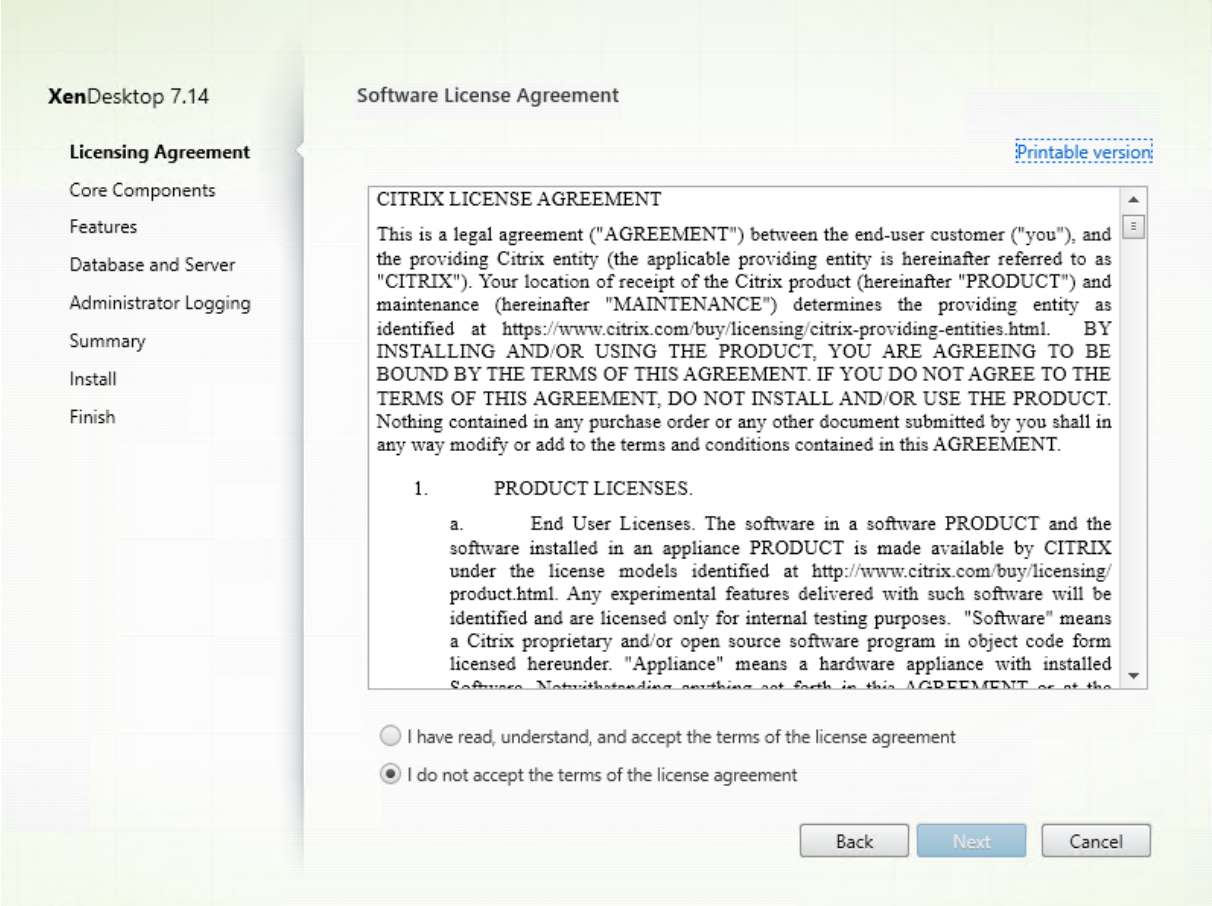
Klicken Sie auf **Start** neben dem zu installierenden Produkt: **XenApp** oder **XenDesktop**.

Schritt 3: Auswählen der Sitzungsaufzeichnung



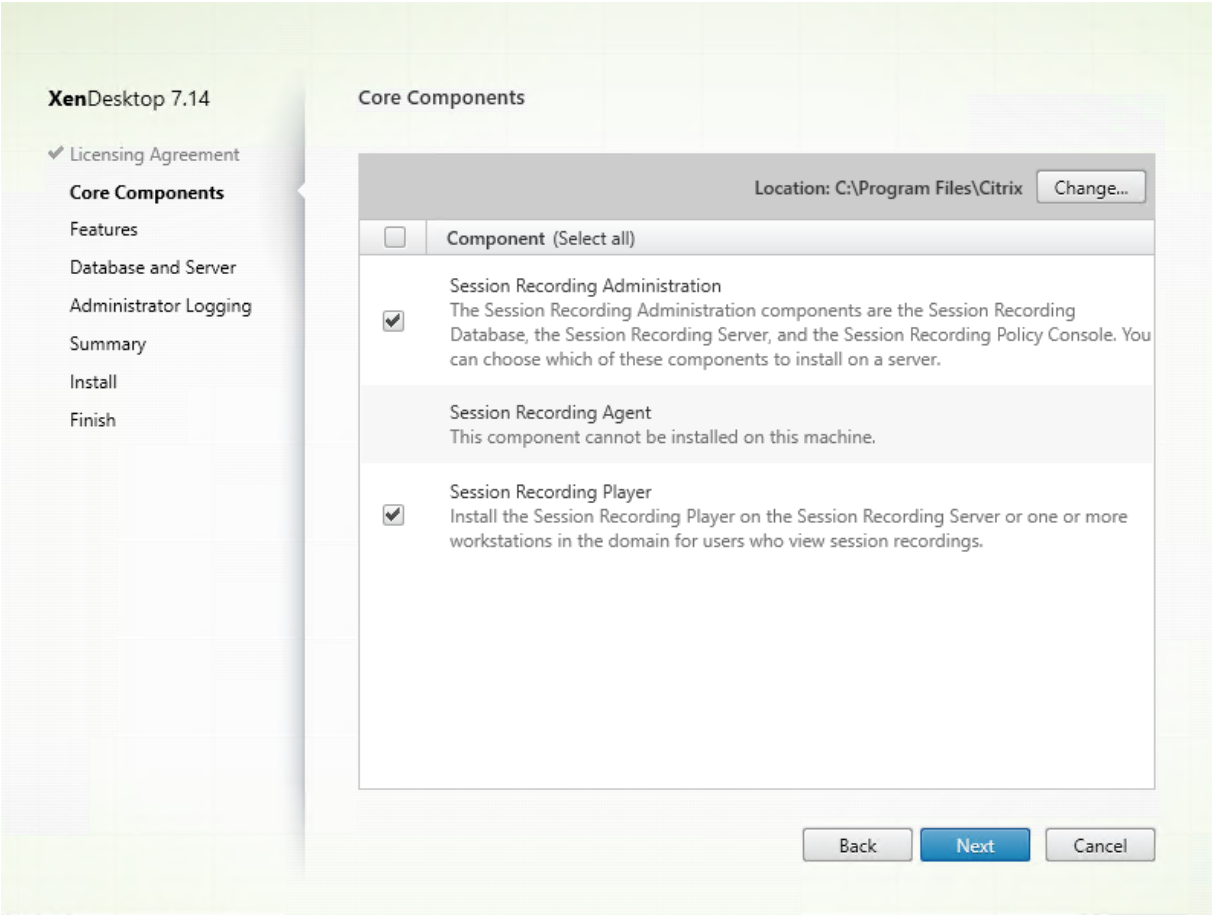
Wählen Sie den Eintrag **Sitzungsaufzeichnung**.

Schritt 4: Lesen und Akzeptieren der Lizenzvereinbarung



Lesen Sie die **Lizenzvereinbarung**, akzeptieren Sie sie und klicken Sie auf **Weiter**.

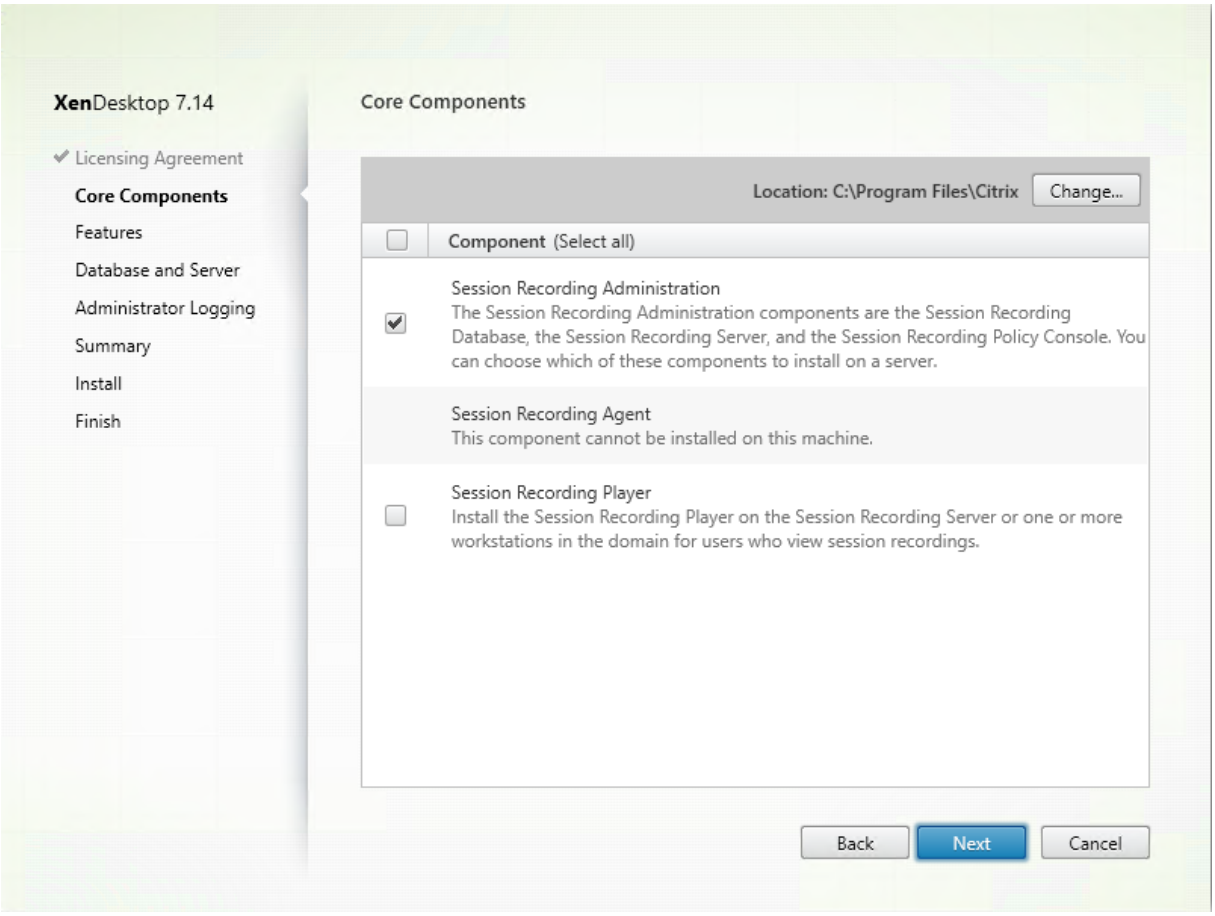
Schritt 5: Auswählen der Komponenten und des Speicherorts für die Installation



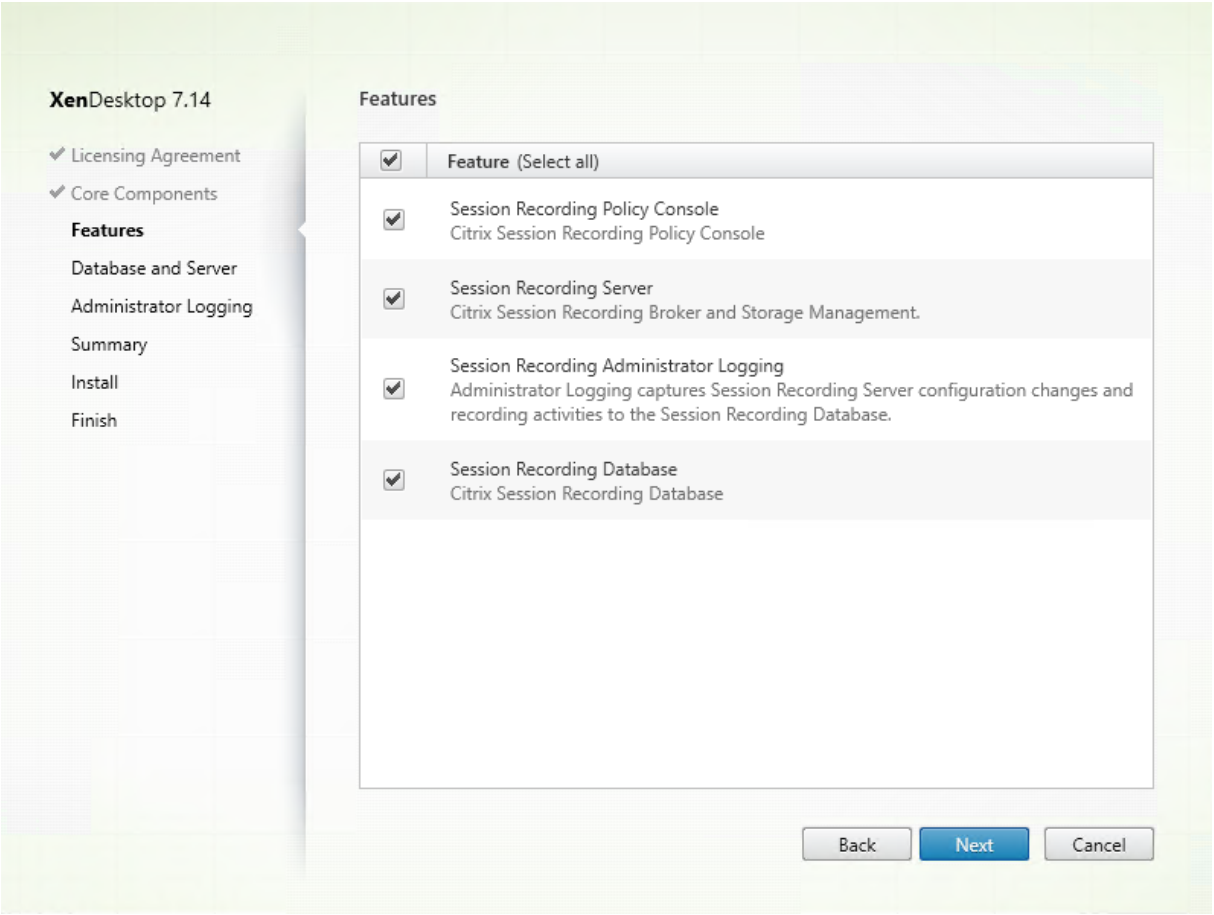
Treffen Sie auf der Seite **Kernkomponenten** folgende Auswahl:

- **Speicherort:** Standardmäßig werden die Komponenten in C:\Programme\Citrix installiert. Der Standardspeicherort eignet sich für die meisten Installationen. Sie können einen benutzerdefinierten Installationsspeicherort angeben.
- **Komponente**: In der Standardeinstellung sind alle Kontrollkästchen neben Komponenten, die installiert werden können, ausgewählt. Das Installationsprogramm erkennt, ob ein Desktopbetriebssystem oder ein Serverbetriebssystem ausgeführt wird. Es gestattet die Installation der Komponenten der Sitzungsaufzeichnungsverwaltung nur unter einem Serverbetriebssystem und verhindert die Installation des Sitzungsaufzeichnungsagents auf einem Computer, auf dem kein VDA installiert ist. Auf einem Computer ohne VDA ist die Option **Sitzungsaufzeichnungagent** nicht verfügbar.

Wählen Sie **Sitzungsaufzeichnungsverwaltung** und klicken Sie auf **Weiter**.



Schritt 6: Auswählen der zu installierenden Features



Auf der Seite **Features**:

- In der Standardeinstellung sind alle Kontrollkästchen neben Features, die installiert werden können, ausgewählt. Die Installation dieser Features auf einem einzelnen Server ist für eine Machbarkeitsstudie geeignet. Für große Produktionsumgebungen empfiehlt Citrix die Installation der Richtlinienkonsole für die Sitzungsaufzeichnung auf einem Server und die Installation von Sitzungsaufzeichnungsserver, Administratorprotokollierung der Sitzungsaufzeichnung und Datenbank für die Sitzungsaufzeichnung auf einem zweiten Server. Die Administratorprotokollierung ist ein optionales Teilfeature des Sitzungsaufzeichnungsservers. Sie müssen den Sitzungsaufzeichnungsserver auswählen, bevor Sie die Administratorprotokollierung auswählen können.
- Zum Hinzufügen eines Features auf einem Server nach Installation eines Features müssen Sie das MSI-Paket verwenden. Das Installationsprogramm kann nicht erneut ausgeführt werden.

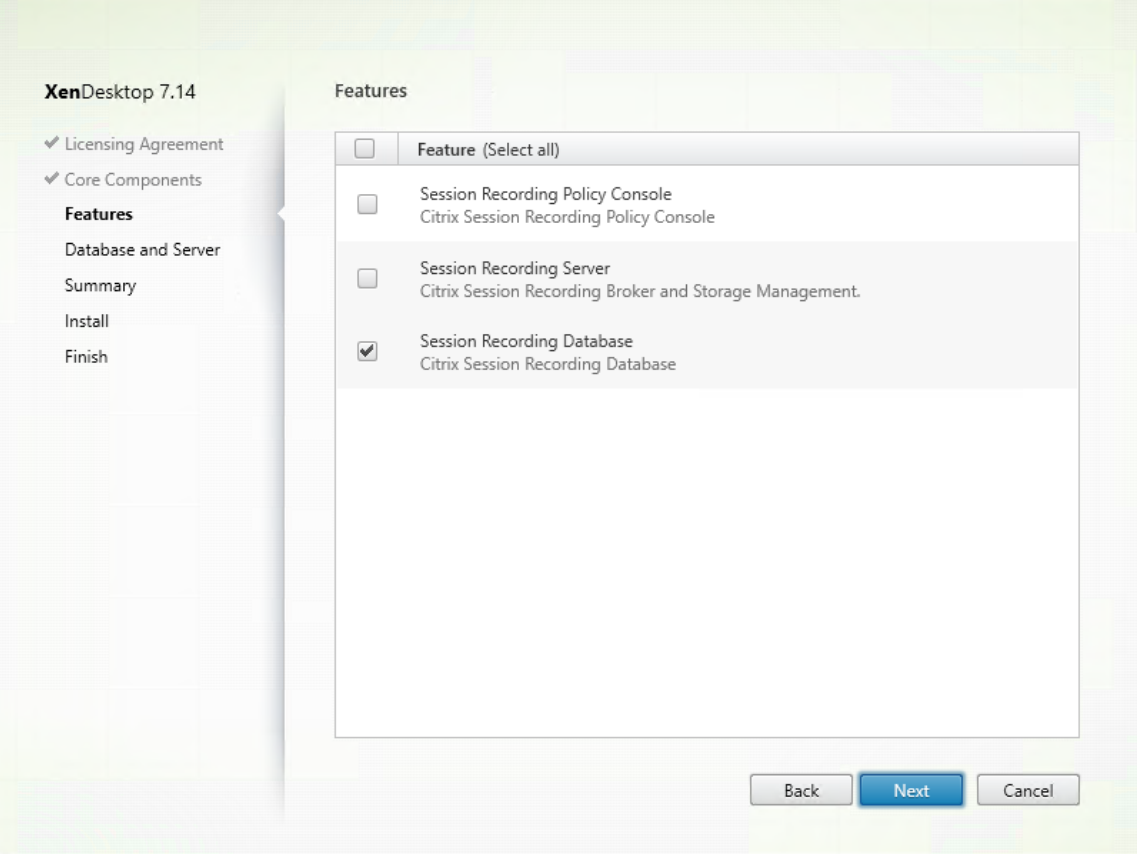
Wählen Sie die gewünschten Features und klicken Sie auf **Weiter**.

Schritt 6.1: Installieren der Datenbank für die Sitzungsaufzeichnung **Hinweis:** Die Datenbank für die Sitzungsaufzeichnung ist eigentlich keine Datenbank. Sie ist für das Erstellen und Konfigurieren der erforderlichen Datenbanken in der Microsoft SQL Server-Instanz während der Installation zuständig. Die Sitzungsaufzeichnung unterstützt drei Lösungen für die hohe Verfügbarkeit der Datenbank basierend auf Microsoft SQL Server. Weitere Informationen finden Sie unter Installieren der Sitzungsaufzeichnung mit hoher Datenbankverfügbarkeit.

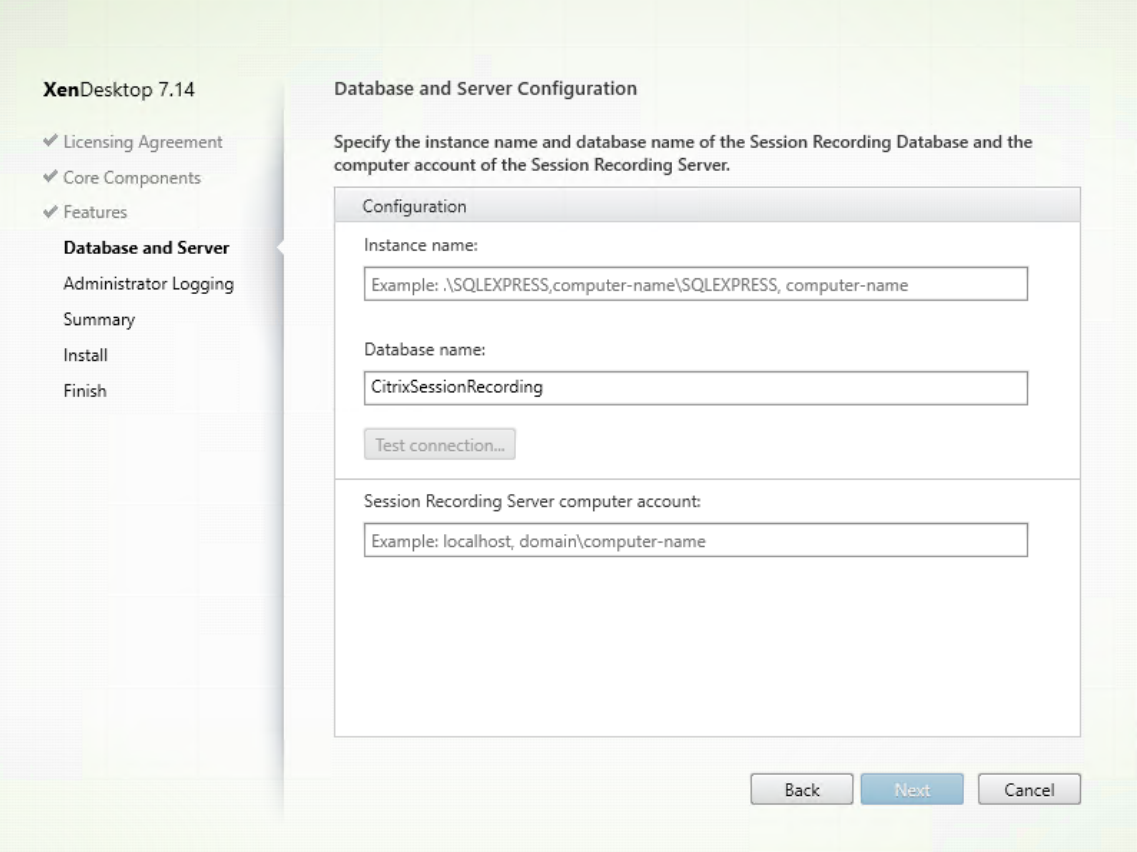
Es gibt drei typische Bereitstellungen der Datenbank für die Sitzungsaufzeichnung und von Microsoft SQL Server:

- Bereitstellung 1: Installation des Sitzungsaufzeichnungsservers und der Datenbank für die Sitzungsaufzeichnung auf derselben Maschine und Installation von Microsoft SQL Server auf einer Remotemaschine (**empfohlen**)
- Bereitstellung 2: Installation des Sitzungsaufzeichnungsservers, der Datenbank für die Sitzungsaufzeichnung und von Microsoft SQL Server auf derselben Maschine
- Bereitstellung 3: Installation des Sitzungsaufzeichnungsservers auf einer Maschine und Installation der Datenbank für die Sitzungsaufzeichnung sowie von Microsoft SQL Server auf einer anderen Maschine (**nicht empfohlen**)

1. Wählen Sie auf der Seite **Features** die Option **Datenbank für die Sitzungsaufzeichnung** und klicken Sie auf **Weiter**.



2. Geben Sie auf der Seite **Datenbank- und Server** den Instanznamen und Datenbanknamen der Datenbank für die Sitzungsaufzeichnung und das Computerkonto des Sitzungsaufzeichnungsservers an. Klicken Sie auf **Weiter**.



Führen Sie auf der Seite **Datenbank- und Serverkonfiguration** folgende Schritte aus:

- **Instanzname**: Wenn die Datenbankinstanz keine benannte Instanz ist, die Sie beim Setup der Instanz konfiguriert haben, können Sie nur den Computernamen des SQL Server-Computers verwenden. Wenn Sie die Instanz benannt haben, verwenden Sie Computername\Instanzname als Datenbankinstanznamen. Um den verwendeten Servernamen zu ermitteln, führen Sie **select @@servername** auf dem SQL Server aus. Der zurückgegebene Name ist der Datenbankinstanzname. Wenn Ihr SQL Server so konfiguriert ist, dass er auf einem benutzerdefinierten Port (außer dem Standardport 1433) abhört, legen Sie den benutzerdefinierten Listenerport fest, indem Sie ein Komma an den Instanznamen anhängen. Beispiel: Geben Sie **DXSBC-SRD-1,2433** in das Textfeld **Instanzname** ein, wobei 2433 nach dem Komma den benutzerdefinierten Listenerport angibt.
- **Datenbankname:** Geben Sie einen benutzerdefinierten Datenbanknamen in das Textfeld **Datenbankname** ein oder übernehmen Sie den Standardnamen. Klicken Sie auf **Verbindung testen** zum Testen der Verbindung mit der SQL Server-Instanz und der Gültigkeit des Datenbanknamens.

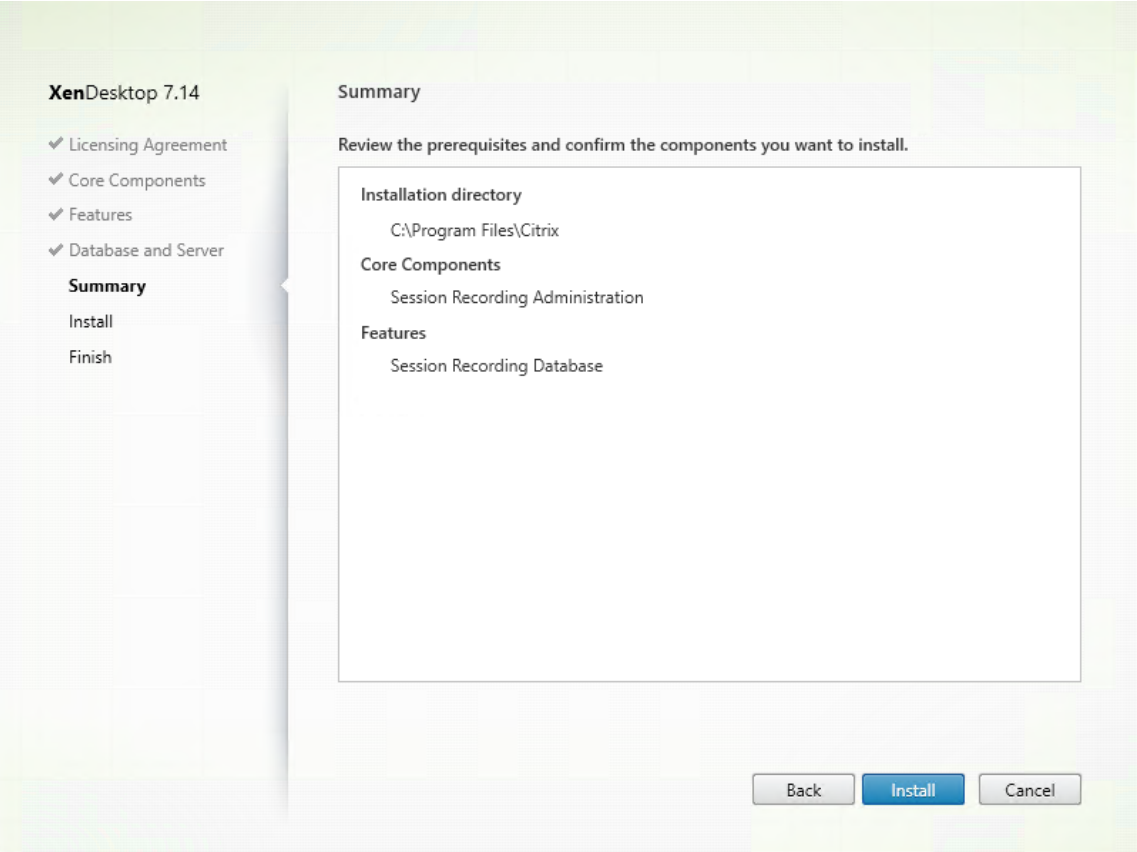
> **Wichtig:**
>
> Ein benutzerdefinierter Datenbankname darf nur Buchstaben (A-Z, a-z) und Ziffern (0-9) enthalten und nicht länger als 123 Zeichen sein.

- Sie müssen die Serverrollenberechtigungen **securityadmin** und **dbcreator** für die Datenbank haben. Wenn Sie diese Berechtigungen nicht haben, gibt es folgende Möglichkeiten:
  - Bitten Sie den Datenbankadministrator darum, Berechtigungen für die Installation zuzuweisen. Nach Abschluss der Installation werden die Serverrollenberechtigungen **securityadmin** und **dbcreator** nicht mehr benötigt und können entfernt werden.
  - Verwenden Sie das Paket SessionRecordingAdministrationx64.msi (in der entpackten ISO-Datei unter …\x64\Session Recording). Während der MSI-Installation wird ein Dialogfeld angezeigt, in dem die Anmeldeinformationen eines Datenbankadministrators mit den Serverrollenberechtigungen **securityadmin** und **dbcreator** eingegeben werden müssen. Geben Sie die richtigen Anmeldeinformationen ein und klicken Sie auf **OK**, um mit der Installation fortzufahren.

    Bei der Installation wird die neue Datenbank für die Sitzungsaufzeichnung erstellt und das Maschinenkonto des Sitzungsaufzeichnungsservers als **db_owner** hinzugefügt.
- **Computerkonto des Sitzungsaufzeichnungsservers**:
  - **Bereitstellung 1 und 2:** Geben Sie im Feld **Computerkonto des Sitzungsaufzeichnungsservers** die Zeichenfolge **localhost** ein.
  - **Bereitstellung 3**: Geben Sie den Namen des Computers, der den Sitzungsaufzeichnungsserver hostet, im Format "Domäne\Computername"ein. Das Computerkonto des Sitzungsaufzeichnungsservers wird als Benutzerkonto für den Zugriff auf die Datenbank für die Sitzungsaufzeichnung verwendet.

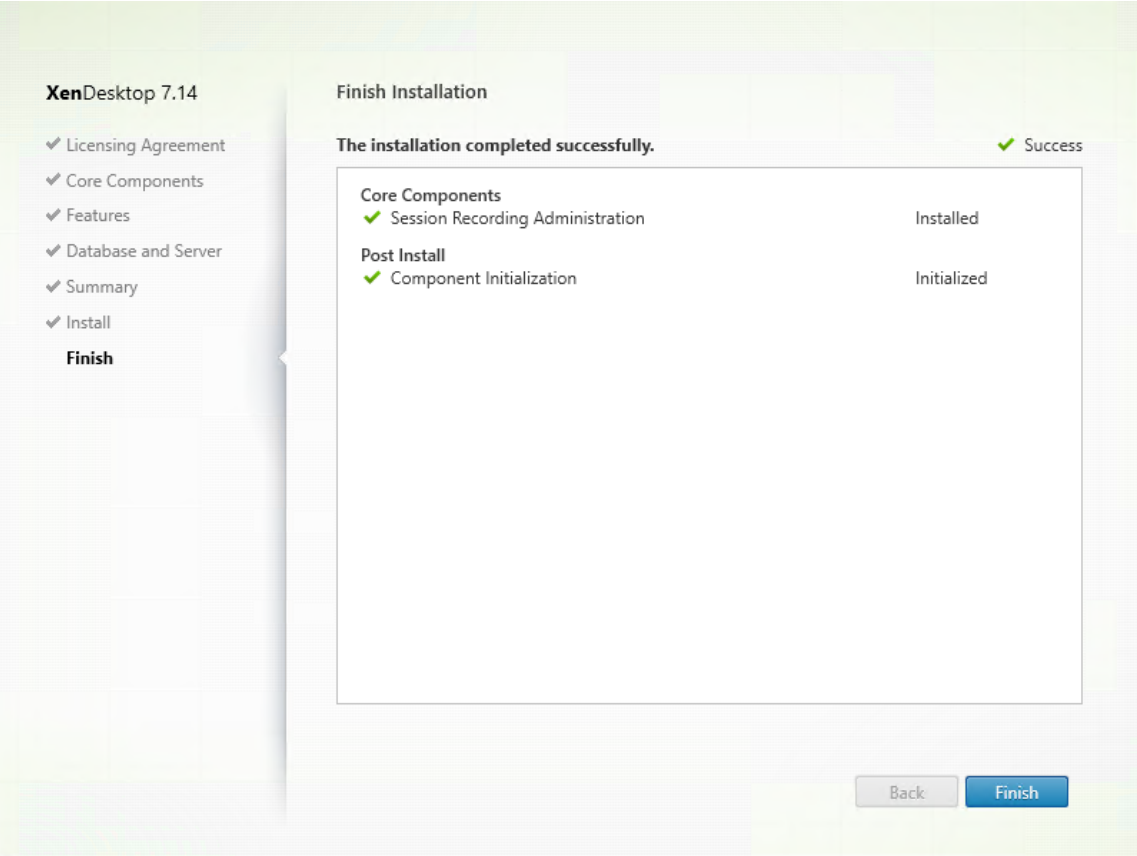
  Hinweis: Die Installation der Komponenten der Sitzungsaufzeichnungsverwaltung kann mit dem Fehlercode 1603 fehlschlagen, wenn für **Computerkonto des Sitzungsaufzeichnungsservers** ein Domänenname festgelegt ist. Geben Sie als Workaround im Feld **Computerkonto des Sitzungsaufzeichnungsservers** die Zeichenfolge **localhost** oder einen Namen im Format "NetBIOS-Domänennamen\Maschinenname"ein.

3. Überprüfen Sie die Voraussetzungen und bestätigen Sie die Installation.



Die Seite **Zusammenfassung** enthält die Installationsoptionen. Sie können mit der Schaltfläche **Zurück** zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern. Klicken Sie alternativ auf **Installieren**, um die Installation zu starten.

4. Schließen Sie die Installation ab.

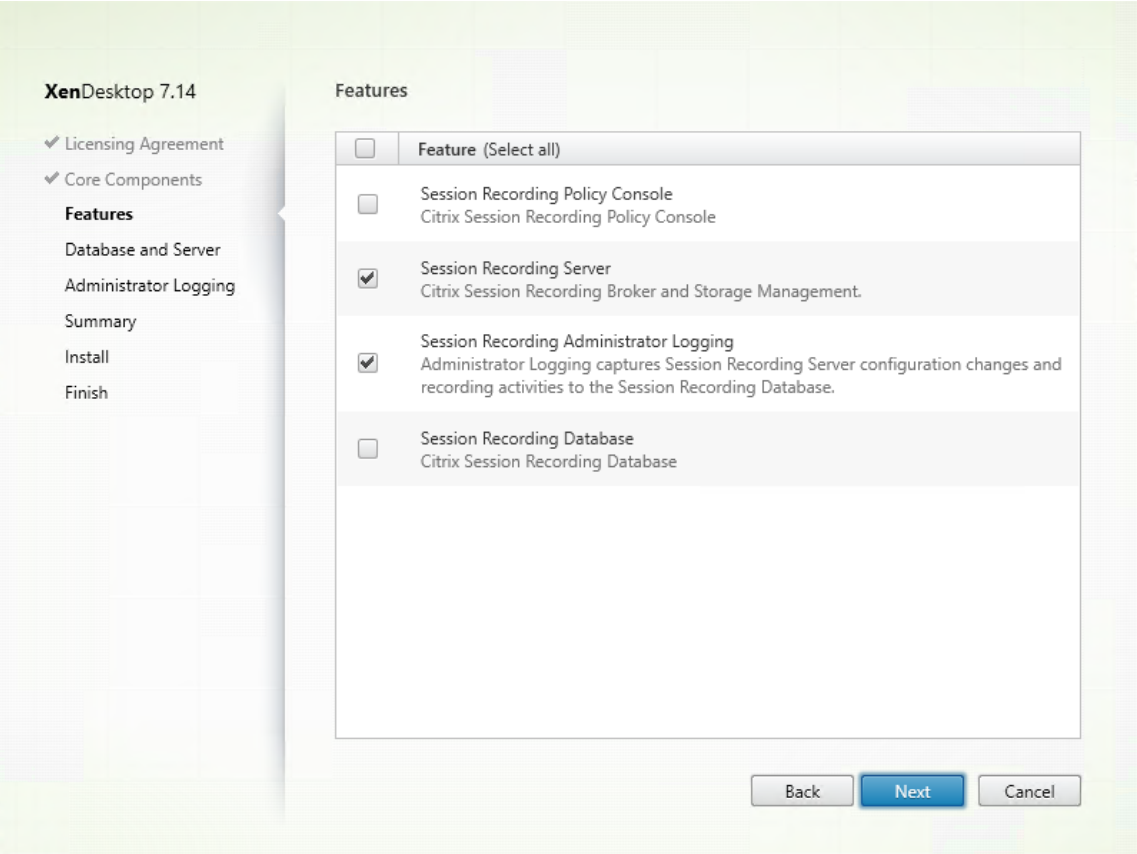


Die Seite **Fertigstellen der Installation** enthält grüne Häkchen für alle Voraussetzungen und Komponenten, die installiert und initialisiert werden konnten.

Klicken Sie auf **Fertig stellen**, um die Installation der Datenbank für die Sitzungsaufzeichnung abzuschließen.

Schritt 6.2: Installieren des Sitzungsaufzeichnungsservers

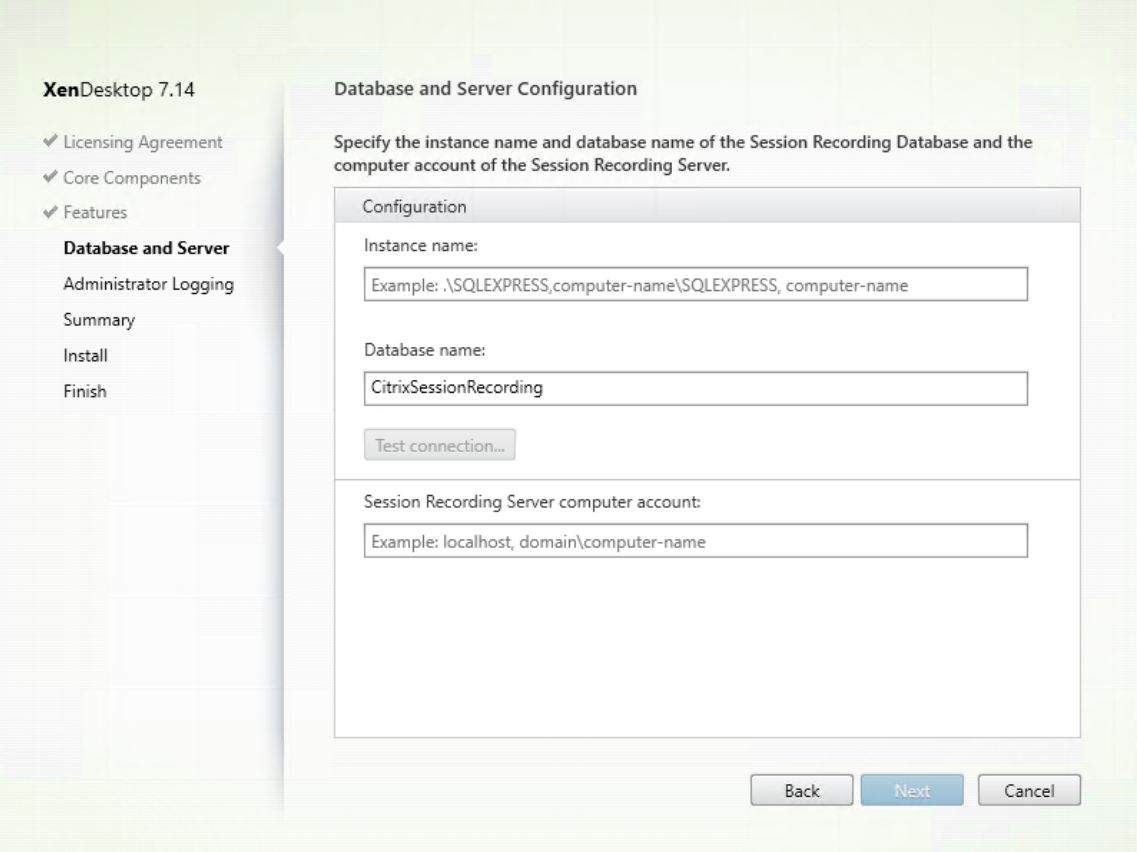
1. Wählen Sie auf der Seite **Features** die Optionen **Sitzungsaufzeichnungsserver** und **Administratorprotokollierung der Sitzungsaufzeichnung**. Klicken Sie auf **Weiter**.



Hinweis:

- Die Administratorprotokollierung ist ein optionales Teilfeature des Sitzungsaufzeichnungsservers. Sie müssen den Sitzungsaufzeichnungsserver auswählen, bevor Sie die Administratorprotokollierung auswählen können.
- Citrix empfiehlt, dass Sie die Administratorprotokollierung zusammen mit dem Sitzungsaufzeichnungsserver installieren. Wenn Sie die Administratorprotokollierung nicht aktivieren möchten, können Sie sie auf einer nachfolgenden Seite deaktivieren. Wenn Sie das Feature nicht gleich zu Beginn installieren, es jedoch später hinzufügen möchten, können Sie dies nur manuell mit dem Paket SessionRecordingAdministrationx64.msi tun.

2. Führen Sie auf der Seite **Datenbank- und Serverkonfiguration** folgende Schritte aus:



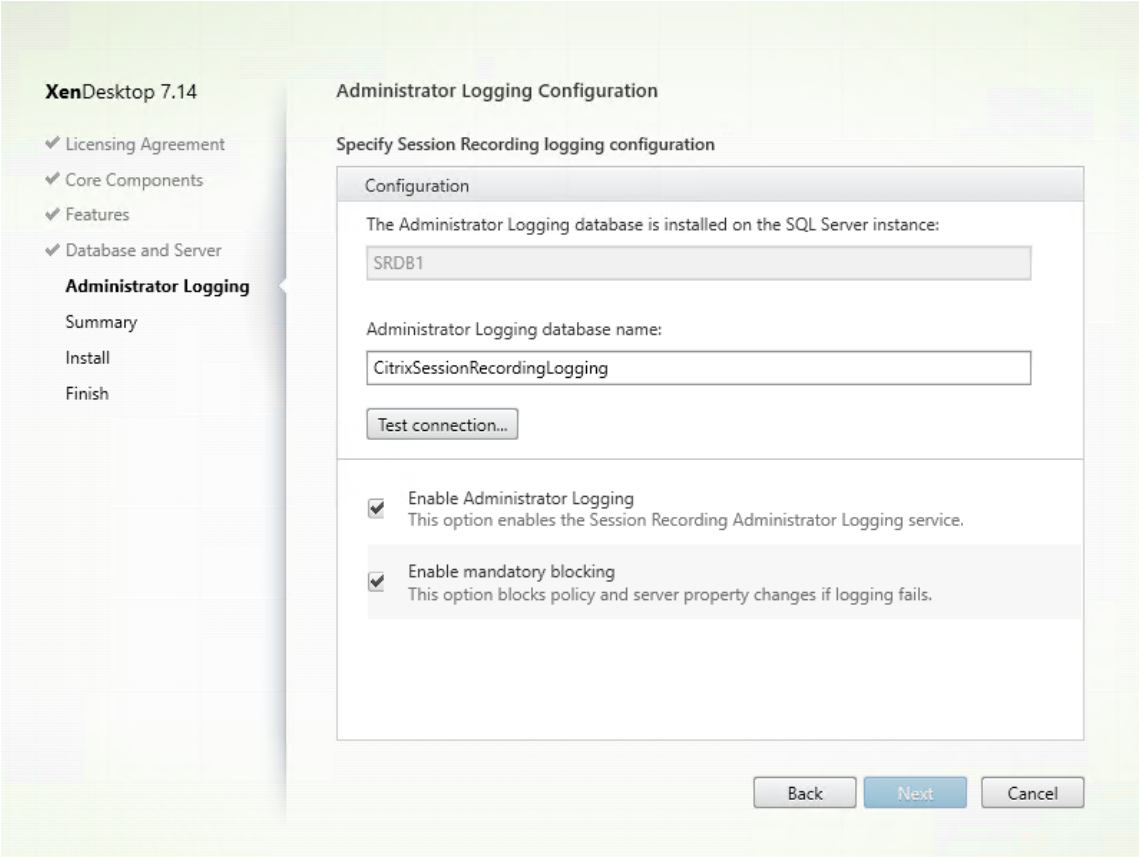
Führen Sie auf der Seite **Datenbank- und Serverkonfiguration** folgende Schritte aus:

- **Instanzname**: Geben Sie den Namen des SQL Servers im Textfeld **Instanzname** ein. Wenn Sie eine benannte Instanz verwenden, machen Sie die Angabe im Format "Computername\Instanzname", andernfalls geben Sie nur einen Computernamen ein. Wenn Ihr SQL Server so konfiguriert ist, dass er auf einem benutzerdefinierten Port (außer dem Standardport 1433) abhört, legen Sie den benutzerdefinierten Listenerport fest, indem Sie ein Komma an den Instanznamen anhängen. Beispiel: Geben Sie **DXSBC-SRD-1,2433** in das Textfeld **Instanzname** ein, wobei 2433 nach dem Komma den benutzerdefinierten Listenerport angibt.
- **Datenbankname:** Geben Sie einen benutzerdefinierten Datenbanknamen in das Textfeld **Datenbankname** ein oder übernehmen Sie den Standardnamen **CitrixSessionRecording**.
- Sie müssen die Serverrollenberechtigungen **securityadmin** und **dbcreator** für die Datenbank haben. Wenn Sie diese Berechtigungen nicht haben, gibt es folgende Möglichkeiten:
  - Bitten Sie den Datenbankadministrator darum, Berechtigungen für die Installation zuzuweisen. Nach Abschluss der Installation werden die Serverrollenberechtigungen **securityadmin** und **dbcreator** nicht mehr benötigt und können entfernt werden.
  - Verwenden Sie das Paket SessionRecordingAdministrationx64.msi. Während der MSI-Installation wird ein Dialogfeld angezeigt, in dem die Anmeldeinformationen eines

Datenbankadministrators mit den Serverrollenberechtigungen **securityadmin** und **dbcreator** eingegeben werden müssen. Geben Sie die richtigen Anmeldeinformationen ein und klicken Sie auf **OK**, um mit der Installation fortzufahren.

- Klicken Sie nach Eingabe der korrekten Namen für Instanz und Datenbank auf **Verbindung testen**, um die Verbindung zur Datenbank für die Sitzungsaufzeichnung zu testen.
- Geben Sie das Computerkonto für die Sitzungsaufzeichnung ein und klicken Sie auf **Weiter**.

3. Geben Sie auf der Seite **Konfiguration der Administratorprotokollierung** die Konfigurationen für die Administratorprotokollierung an.



Treffen Sie auf der Seite **Administratorprotokollierung - Konfiguration** folgende Auswahl:

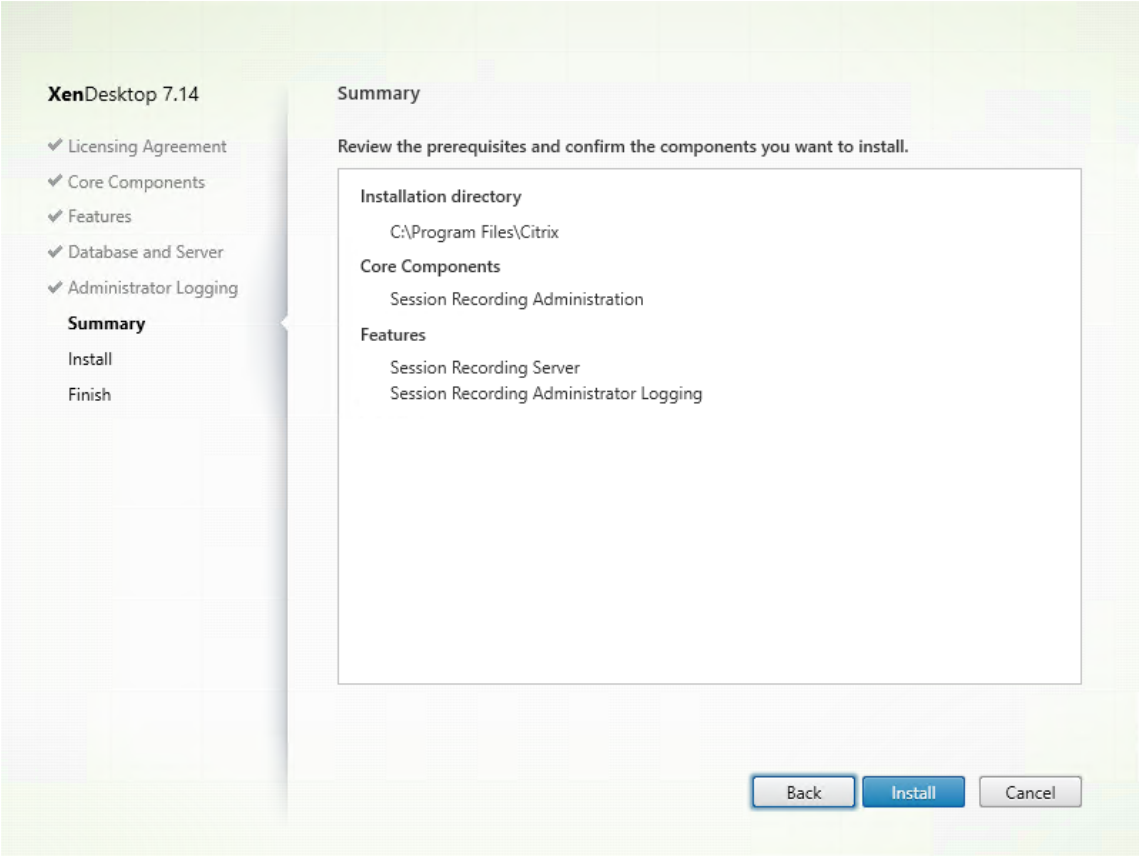
- **Datenbank für Administratorprotokollierung installieren auf SQL Server-Instanz:** Dieses Feld kann nicht bearbeitet werden. Der Name der SQL Server-Instanz der Datenbank für die Administratorprotokollierung wird automatisch aus dem Instanznamen abgerufen, den Sie auf der Seite **Datenbank und Server** eingegeben haben.
- **Datenbankname für die Administratorprotokollierung:** Wenn Sie die Administratorprotokollierung der Sitzungsaufzeichnung installieren möchten, geben Sie auf der nächsten Seite einen benutzerdefinierten Namen für die Datenbank der Administratorprotokollierung im Textfeld ein oder übernehmen Sie den angegebenen Standarddatenbankna-

men **CitrixSessionRecordingLogging**.
Hinweis: Der Name der Datenbank für die Administratorprotokollierung muss sich vom Namen der Datenbank für die Sitzungsaufzeichnung, der im Textfeld **Datenbankname** auf der vorherigen Seite **Datenbank und Server - Konfiguration** festgelegt wurde, unterscheiden.

- Nach der Eingabe des Namens klicken Sie auf **Verbindung testen**, um die Verbindung mit der Datenbank zu testen.
- **Administratorprotokollierung aktivieren:** Die Administratorprotokollierung ist standardmäßig aktiviert. Sie können sie deaktivieren, indem Sie das Kontrollkästchen deaktivieren.
- **Obligatorische Blockierung aktivieren:** Die obligatorische Blockierung ist standardmäßig aktiviert. Die normalen Funktionen werden möglicherweise blockiert, wenn die Protokollierung fehlschlägt. Sie können sie deaktivieren, indem Sie das Kontrollkästchen deaktivieren.

Klicken Sie auf **Weiter**, um die Installation fortzusetzen.

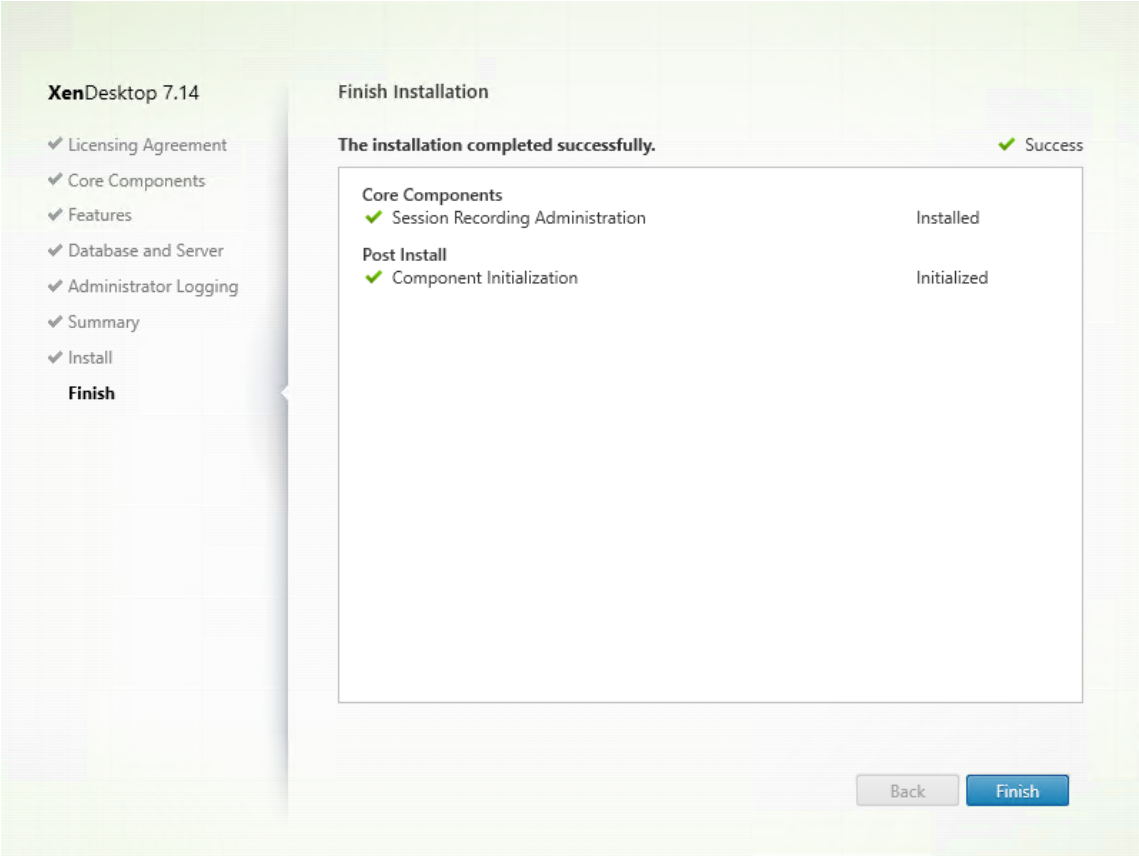
4. Überprüfen Sie die Voraussetzungen und bestätigen Sie die Installation.



Die Seite **Zusammenfassung** enthält die Installationsoptionen. Sie können mit der Schaltfläche **Zurück** zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern. Klicken Sie

alternativ auf **Installieren**, um die Installation zu starten.

5. Schließen Sie die Installation ab.



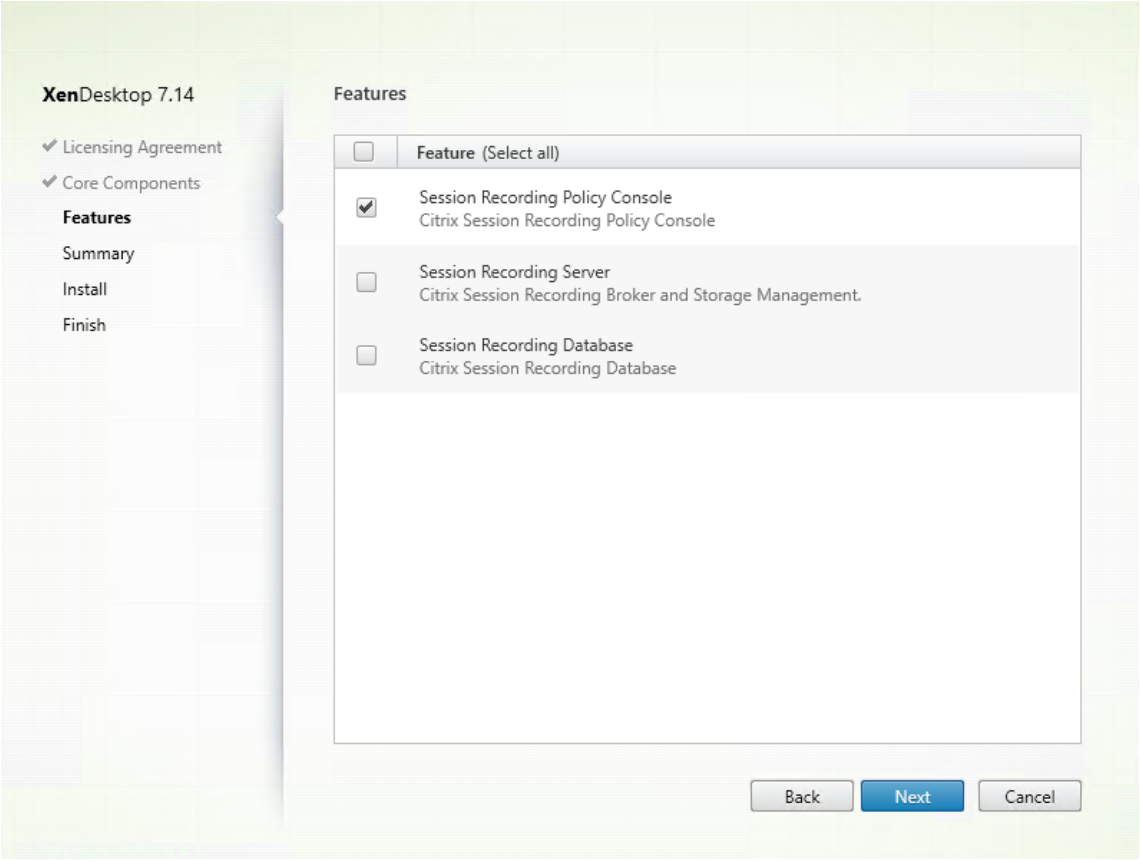
Die Seite **Fertigstellen der Installation** enthält grüne Häkchen für alle Voraussetzungen und Komponenten, die installiert und initialisiert werden konnten.

Klicken Sie auf **Fertig stellen**, um die Installation der Datenbank für den Sitzungsaufzeichnungsserver abzuschließen.

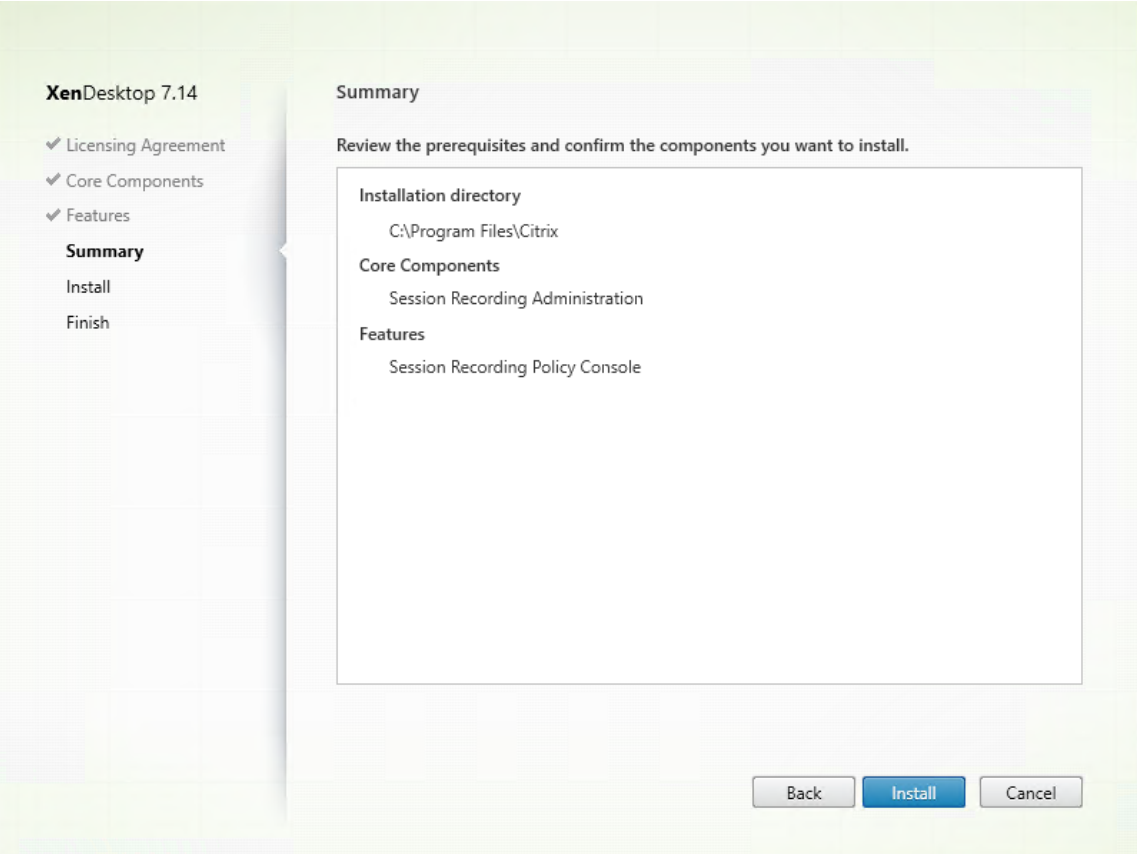
Hinweis: Standardmäßig verwendet der Sitzungsaufzeichnungsserver HTTPS/TLS für die sichere Kommunikation. Wenn TLS nicht in der Standard-IIS-Site des Sitzungsaufzeichnungsservers konfiguriert ist, verwenden Sie HTTP. Hierfür löschen Sie die SSL-Auswahl in der IIS-Verwaltungskonsole, indem Sie die Site des Sitzungsaufzeichnungsbrokers aufrufen, die SSL-Einstellungen öffnen und das Kontrollkästchen **SSL erforderlich** deaktivieren.

Schritt 6.3: Installieren der Richtlinienkonsole für die Sitzungsaufzeichnung

1. Wählen Sie auf der Seite **Features** die Option **Richtlinienkonsole für die Sitzungsaufzeichnung** und klicken Sie auf **Weiter**.

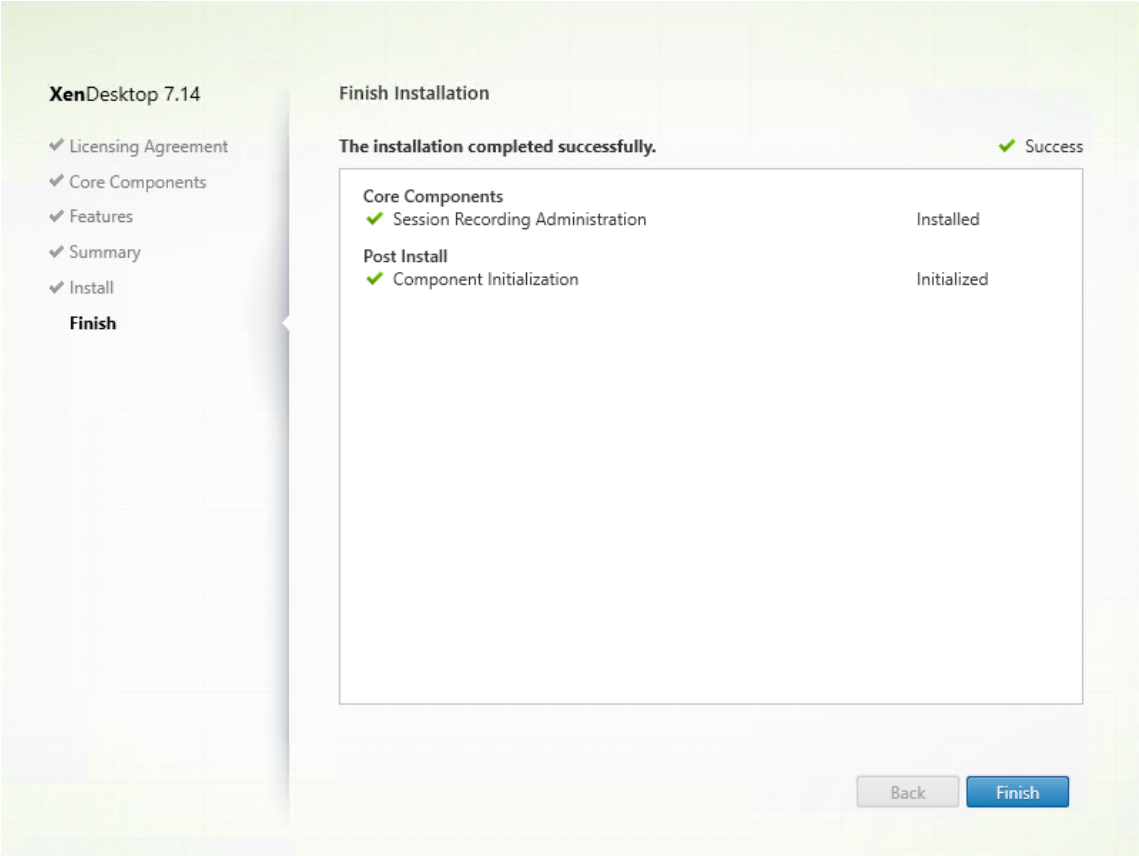


2. Überprüfen Sie die Voraussetzungen und bestätigen Sie die Installation.



Die Seite **Zusammenfassung** enthält die Installationsoptionen. Sie können mit der Schaltfläche **Zurück** zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern. Klicken Sie alternativ auf **Installieren**, um die Installation zu starten.

3. Schließen Sie die Installation ab.



Die Seite **Fertigstellen der Installation** enthält grüne Häkchen für alle Voraussetzungen und Komponenten, die installiert und initialisiert werden konnten.

Klicken Sie auf **Fertig stellen**, um die Installation der Richtlinienkonsole für die Sitzungsaufzeichnung abzuschließen.

Schritt 7: Installieren von Broker_PowerShellSnapIn_x64.msi

Wichtig: Um die Richtlinienkonsole für die Sitzungsaufzeichnung zu verwenden, muss das Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) installiert sein. Das Snap-In kann nicht automatisch über das Installationsprogramm installiert werden. Navigieren Sie zu dem Snap-In auf dem ISO-Image für XenApp-XenDesktop (\layout\image-full\x64\Citrix Desktop Delivery Controller) und folgen Sie den Anweisungen, um es manuell zu installieren. Anderenfalls kann es zu Fehlern kommen.

Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers

Sie können mit der Director-Konsole die Sitzungsaufzeichnungsrichtlinien erstellen und aktivieren.

1. Zur Verwendung einer HTTPS-Verbindung installieren Sie das Zertifikat zum Vertrauen des Sitzungsaufzeichnungsservers im Ordner mit den vertrauenswürdigen Stammzertifikaten des Director-Servers.
2. Zum Konfigurieren des Director-Servers für die Verwendung des Sitzungsaufzeichnungsservers führen Sie den Befehl **C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording** aus.
3. Geben Sie die IP-Adresse bzw. den FQDN des Sitzungsaufzeichnungsservers, die Portnummer und den Verbindungstyp (HTTP/HTTPS) für die Verbindung zwischen Sitzungsaufzeichnungsagent und Sitzungsaufzeichnungsbroker auf dem Director-Server ein.

Installieren des Sitzungsaufzeichnungsagent

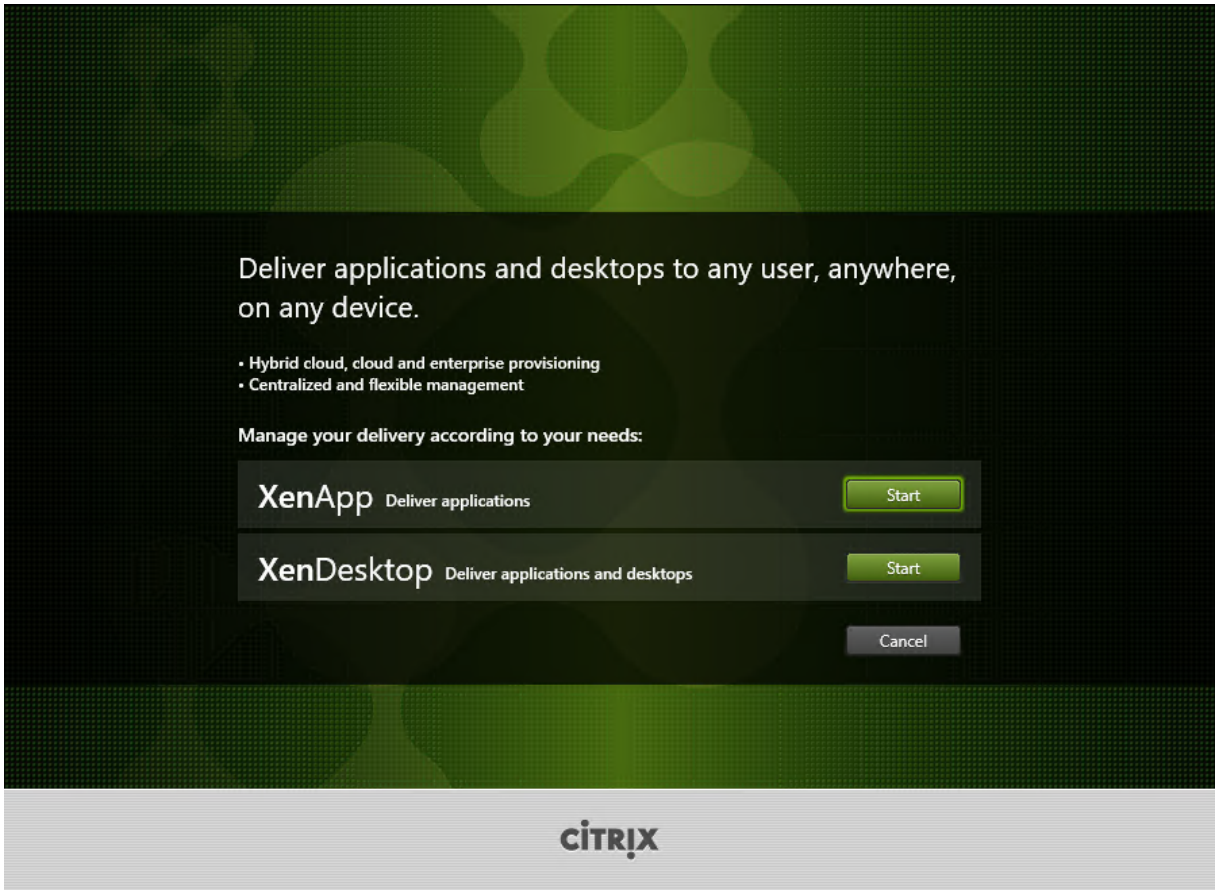
Sie müssen den Sitzungsaufzeichnungsagent auf der Serverbetriebssystem-VDA bzw. -VDI-Maschine installieren, auf der Sie Sitzungen aufzeichnen möchten.

Schritt 1: Herunterladen der Produktsoftware und Starten des Assistenten

Melden Sie sich mit einem lokalen Administratorkonto bei der Maschine an, auf der Sie den Sitzungsaufzeichnungsagent installieren. Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit. Wenn das Installationsprogramm nicht automatisch gestartet wird, doppelklicken Sie auf die Anwendung **AutoSelect** oder das bereitgestellte Laufwerk.

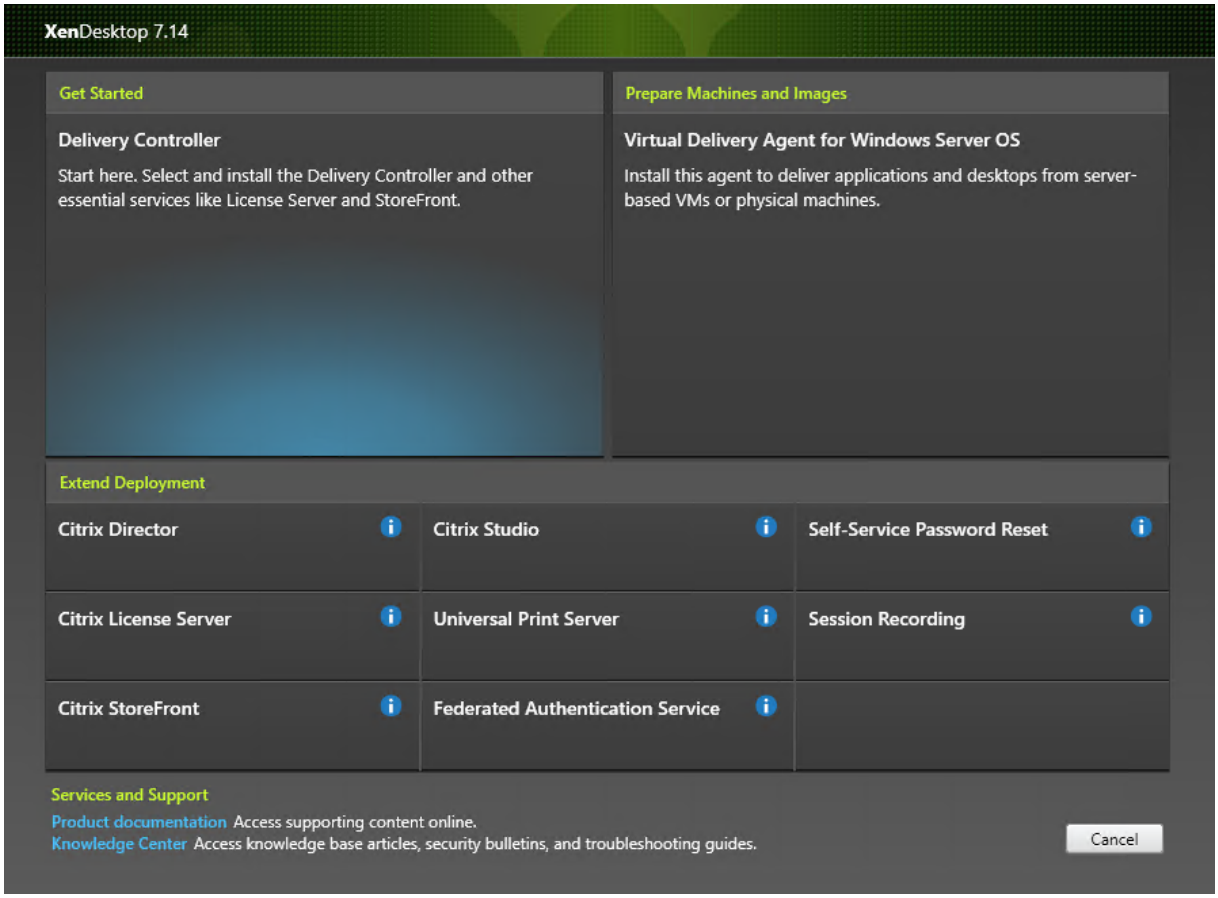
Der Installationsassistent wird gestartet.

Schritt 2: Auswählen des zu installierenden Produkts



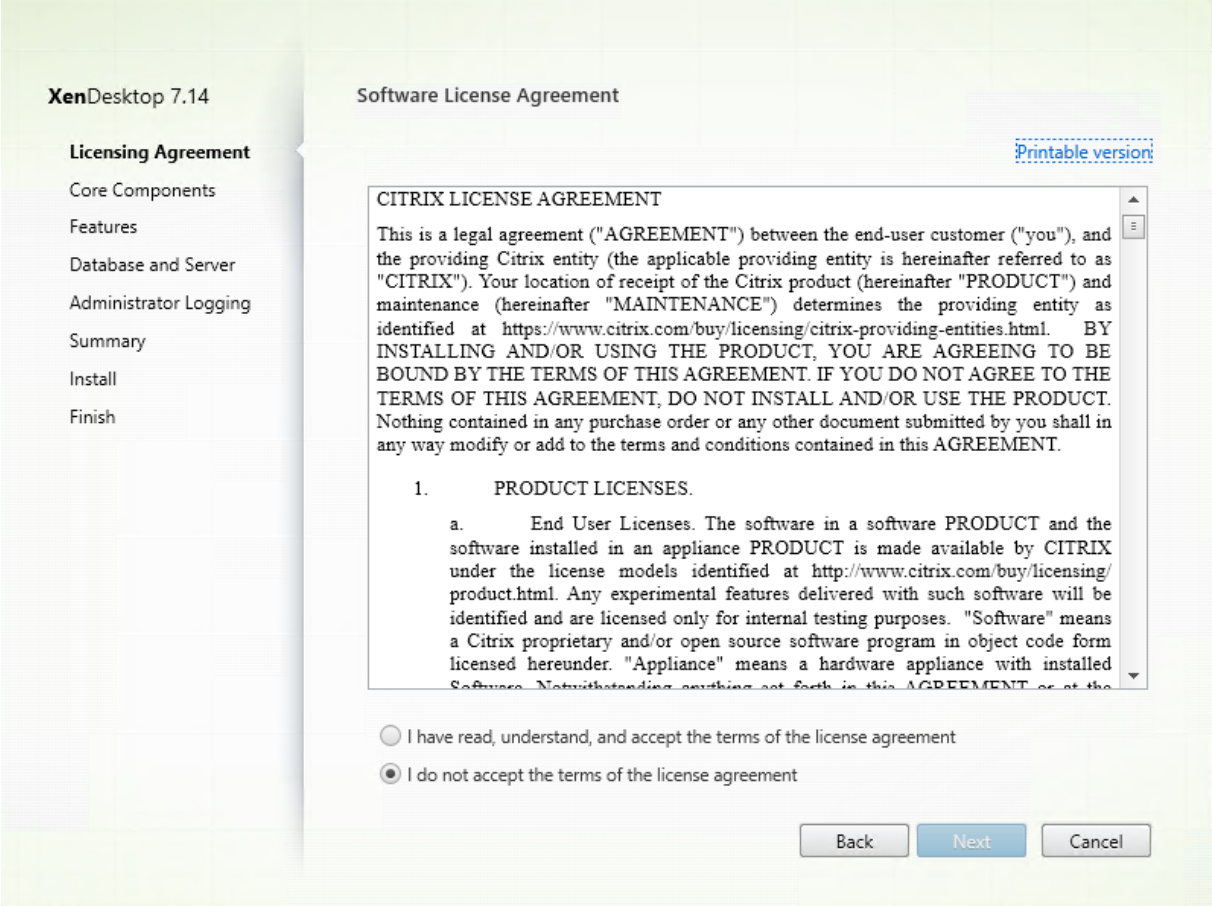
Klicken Sie auf **Start** neben dem zu installierenden Produkt: **XenApp** oder **XenDesktop**.

Schritt 3: Auswählen der Sitzungsaufzeichnung



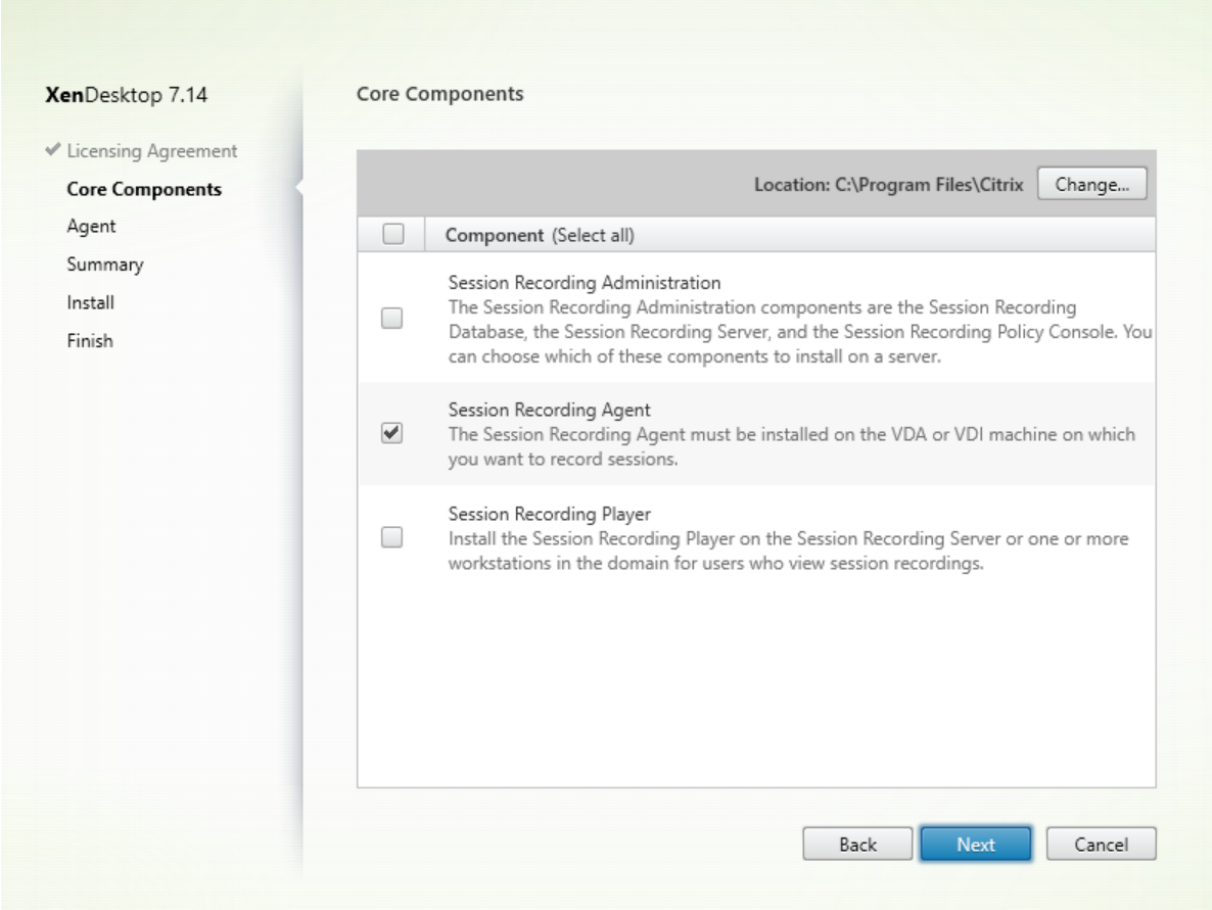
Wählen Sie den Eintrag **Sitzungsaufzeichnung**.

Schritt 4: Lesen und Akzeptieren der Lizenzvereinbarung



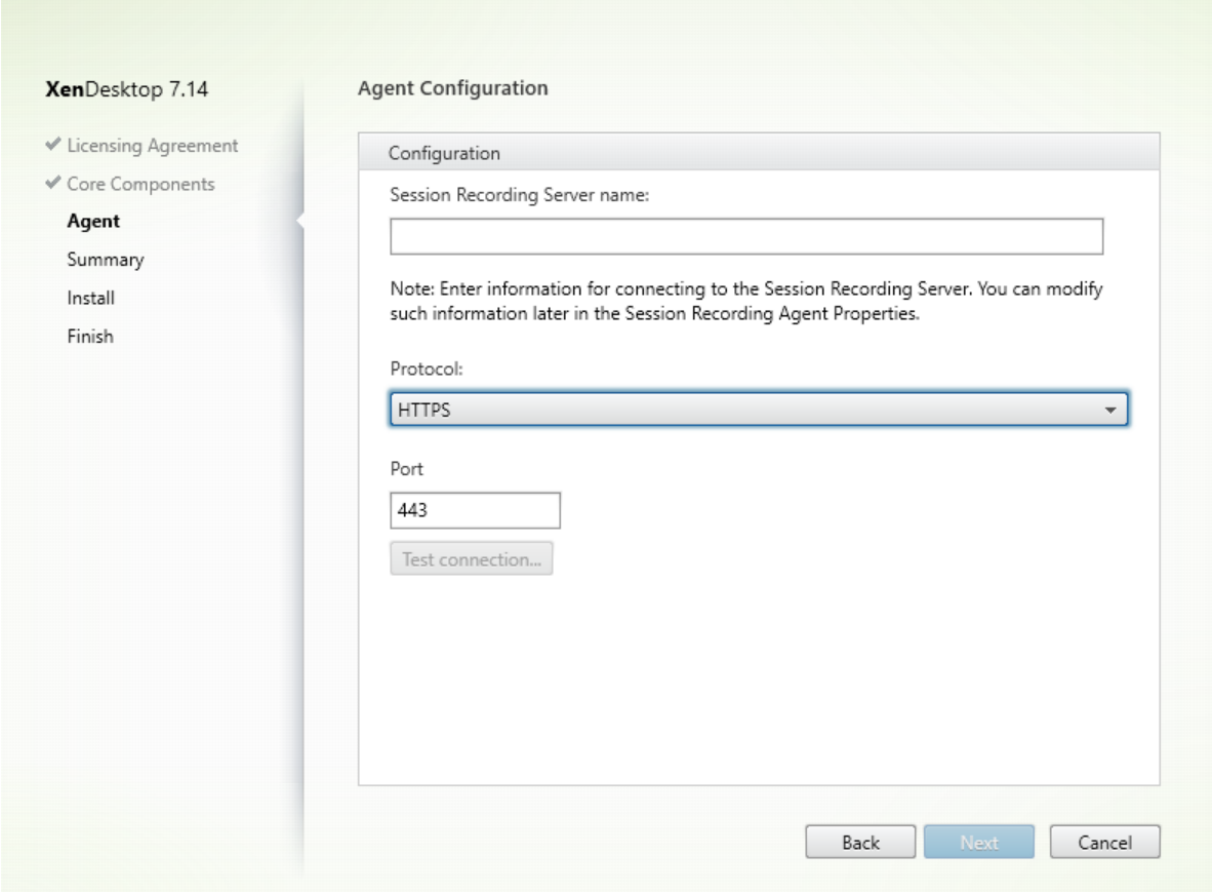
Lesen Sie die **Lizenzvereinbarung**, akzeptieren Sie sie und klicken Sie auf **Weiter**.

Schritt 5: Auswählen der Komponente und des Speicherorts für die Installation



Wählen Sie **Sitzungsaufzeichnungsagent** und klicken Sie auf **Weiter**.

Schritt 6: Angeben der Agentkonfiguration

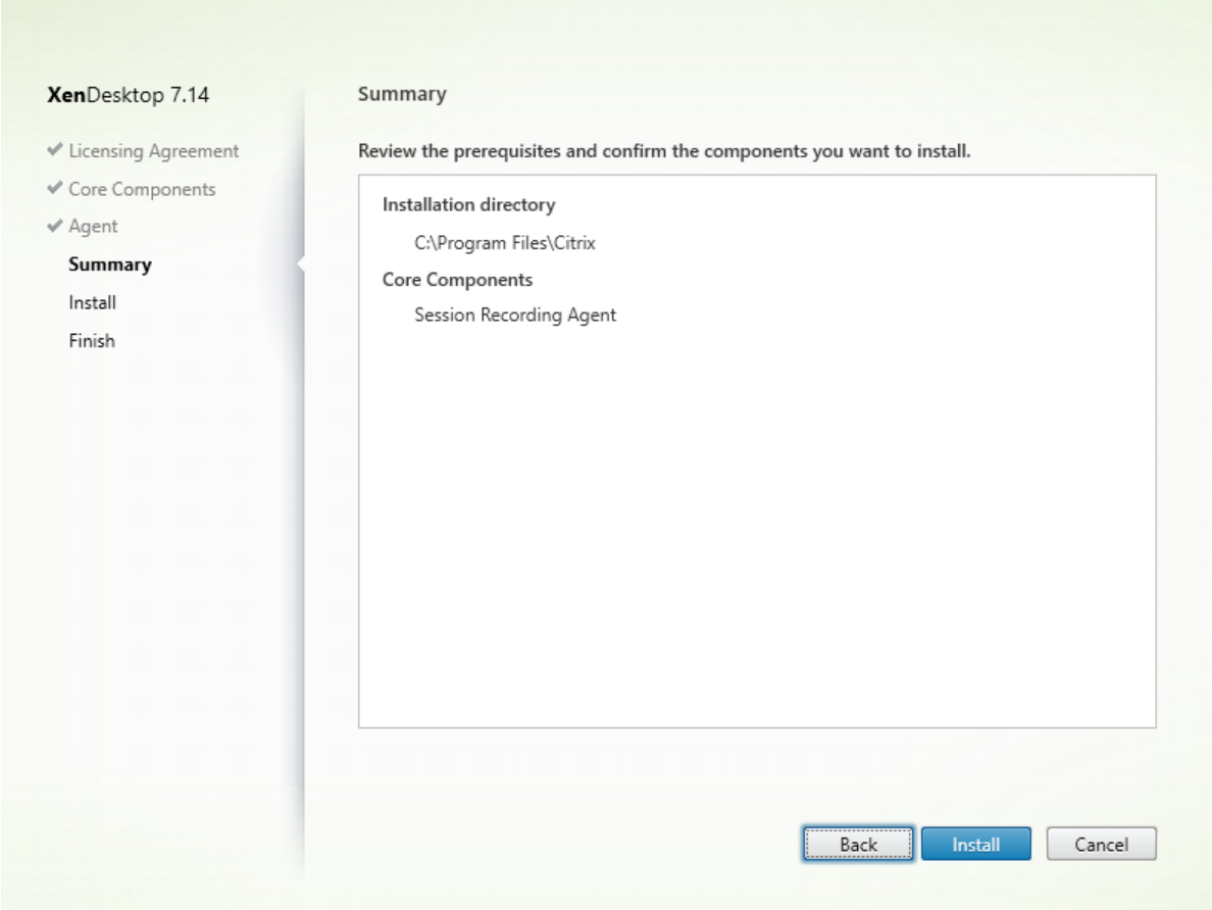


Seite **Agentkonfiguration**:

- Wenn Sie den Sitzungsaufzeichnungsserver zuvor installiert haben, geben Sie den Namen des Computers ein, auf dem Sie den Server installiert haben, sowie das Protokoll und die Portinformationen für die Verbindung zum Sitzungsaufzeichnungsserver. Wenn Sie die Sitzungsaufzeichnung noch nicht installiert haben, können Sie diese Informationen später unter **Sitzungsaufzeichnungsagent - Eigenschaften** ändern.

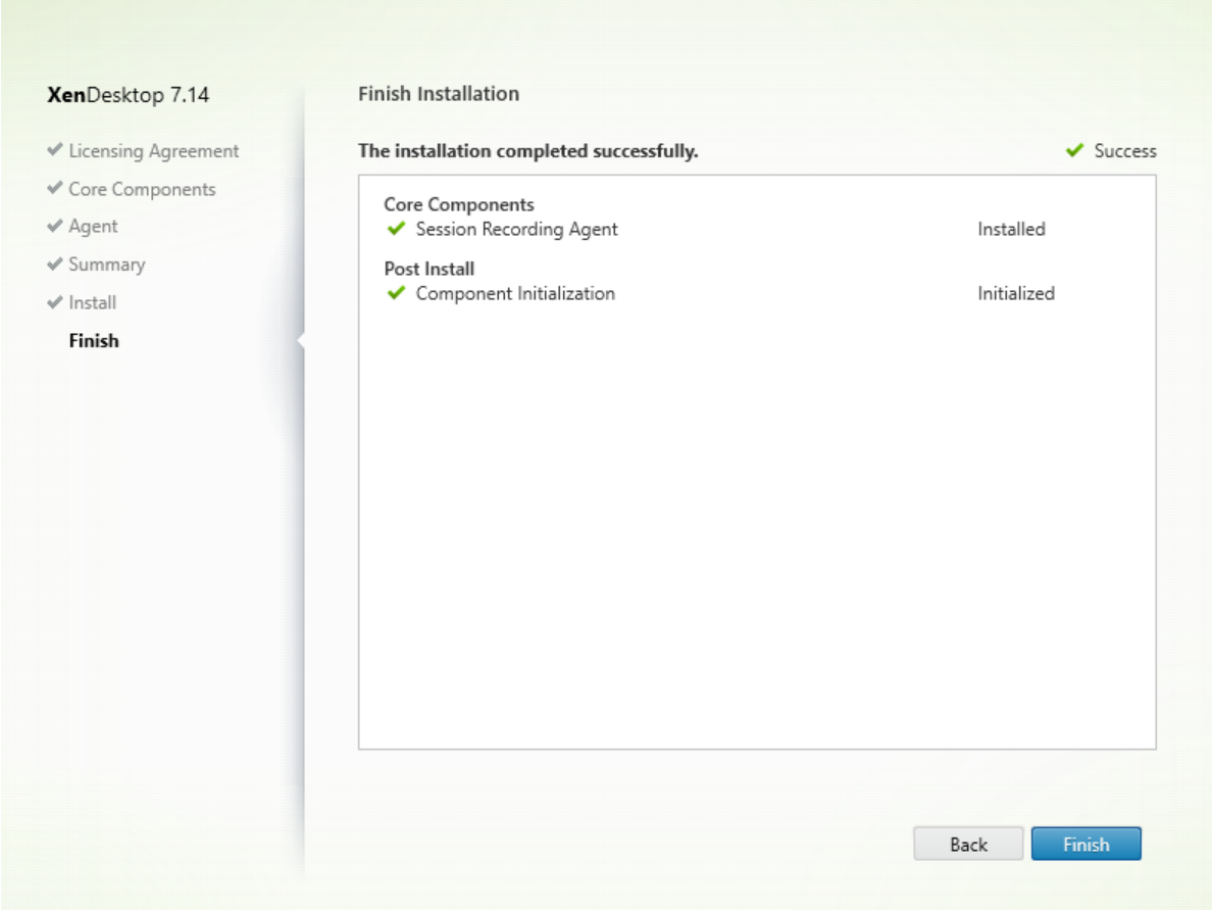
Hinweis: Es gibt eine Einschränkung bei der Funktion des Installationsprogramms zum Verbindungstest. Das Szenario "HTTPS erfordert TLS 1.2"wird nicht unterstützt. Bei Verwendung des Installationsprogramms in diesem Szenario schlägt der Verbindungstest fehl, Sie können den Fehler jedoch ignorieren und auf **Weiter** klicken, um mit der Installation fortzufahren. Die normale Funktionsweise wird nicht beeinflusst.

Schritt 7: Überprüfen der Voraussetzungen und Bestätigen der Installation



Die Seite **Zusammenfassung** enthält die Installationsoptionen. Sie können mit der Schaltfläche **Zurück** zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern. Klicken Sie alternativ auf **Installieren**, um die Installation zu starten.

Schritt 8: Vollständige Installation



Die Seite **Fertigstellen der Installation** enthält grüne Häkchen für alle Voraussetzungen und Komponenten, die installiert und initialisiert werden konnten.

Klicken Sie auf **Fertig stellen**, um die Installation des Sitzungsaufzeichnungsagents abzuschließen.

Hinweis: Wenn von Maschinenerstellungsdienste (MCS) oder Provisioning Services (PVS) mehrere VDAs mit dem konfigurierten Masterimage und Microsoft Message Queuing (MSMQ) erstellt werden, erhalten die VDAs unter bestimmten Bedingungen ggf. die gleiche QMID. Dies kann u. a. zu folgenden Problemen führen:

- Sitzungen werden nicht aufgezeichnet, selbst wenn eine Aufzeichnungsvereinbarung akzeptiert wurde.
- Der Sitzungaufzeichnungsserver empfängt möglicherweise keine Sitzungsabmeldungssignale, sodass Sitzungen permanent den Status “Live”beibehalten.

Erstellen Sie als Workaround eine eindeutige QMID für jeden VDA (abhängig von der Bereitstellungsmethode).

Keine zusätzliche Aktion ist erforderlich, wenn Desktopbetriebssystem-VDAs mit Sitzungsaufzeich-

nungsagent mit PVS 7.7 oder höher oder mit MCS 7.9 oder höher im statischen Desktopmodus erstellt werden und beispielsweise festgelegt wurde, dass alle Änderungen mit einer separaten Personal vDisk oder einem lokalen Datenträger des VDAs persistent gemacht werden.

Bei Serverbetriebssystem-VDAs, die mit MCS oder PVS erstellt wurden, und Desktopbetriebssystem-VDAs, die so konfiguriert wurden, dass alle Änderungen bei Abmeldung des Benutzers verworfen werden, verwenden Sie das Skript GenRandomQMID.ps1 zum Ändern der QMID beim Systemstart. Ändern Sie die Energieverwaltungsstrategie, um sicherzustellen, dass vor Anmeldeversuchen der Benutzer genug VDAs ausgeführt werden.

Führen Sie zum Verwenden des Skripts GenRandomQMID.ps1 folgende Schritte aus:

1. Stellen Sie sicher, dass die Ausführungsrichtlinie in PowerShell auf **RemoteSigned** oder **Unrestricted** festgelegt ist.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

2. Erstellen Sie einen geplanten Task und legen Sie als Auslöser “Bei Systemstart fest”und für die Ausführung auf dem Computer mit dem PVS- oder MCS-Masterimage das Konto SYSTEM.

3. Fügen Sie den Befehl als Starttask hinzu.

   ```
   powershell .exe -file C:\\GenRandomQMID.ps1
   ```

Zusammenfassung des GenRandomQMID.ps1-Skripts:

1. Entfernen Sie die aktuelle QMID aus der Registrierung.
2. Fügen Sie HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters den Wert “SysPrep = 1”hinzu.
3. Anhalten zugehöriger Dienste, einschließlich CitrixSmAudAgent und MSMQ
4. Zum Generieren einer zufälligen QMID starten Sie die zuvor angehaltenen Dienste.

```
# Remove old QMId from registry and set SysPrep flag for MSMQ
Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\
    MachineCache -Name QMId -Force
Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "
    SysPrep" -Type DWord -Value 1
# Get dependent services
\$depServices = Get-Service -name MSMQ -dependentservices | Select -
    Property Name
# Restart MSMQ to get a new QMId
Restart-Service -force MSMQ
# Start dependent services
if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        \$startMode = Get-WmiObject win32\_service -filter \"NAME = '\$
            \($depService.Name)'\" | Select -Property StartMode
        if ($startMode.StartMode -eq "Auto") {
```



```
15
16              Start-Service $depService.Name
17          }
18
19
20  }
21
22  }
```

Installieren des Sitzungsaufzeichnungsplayers

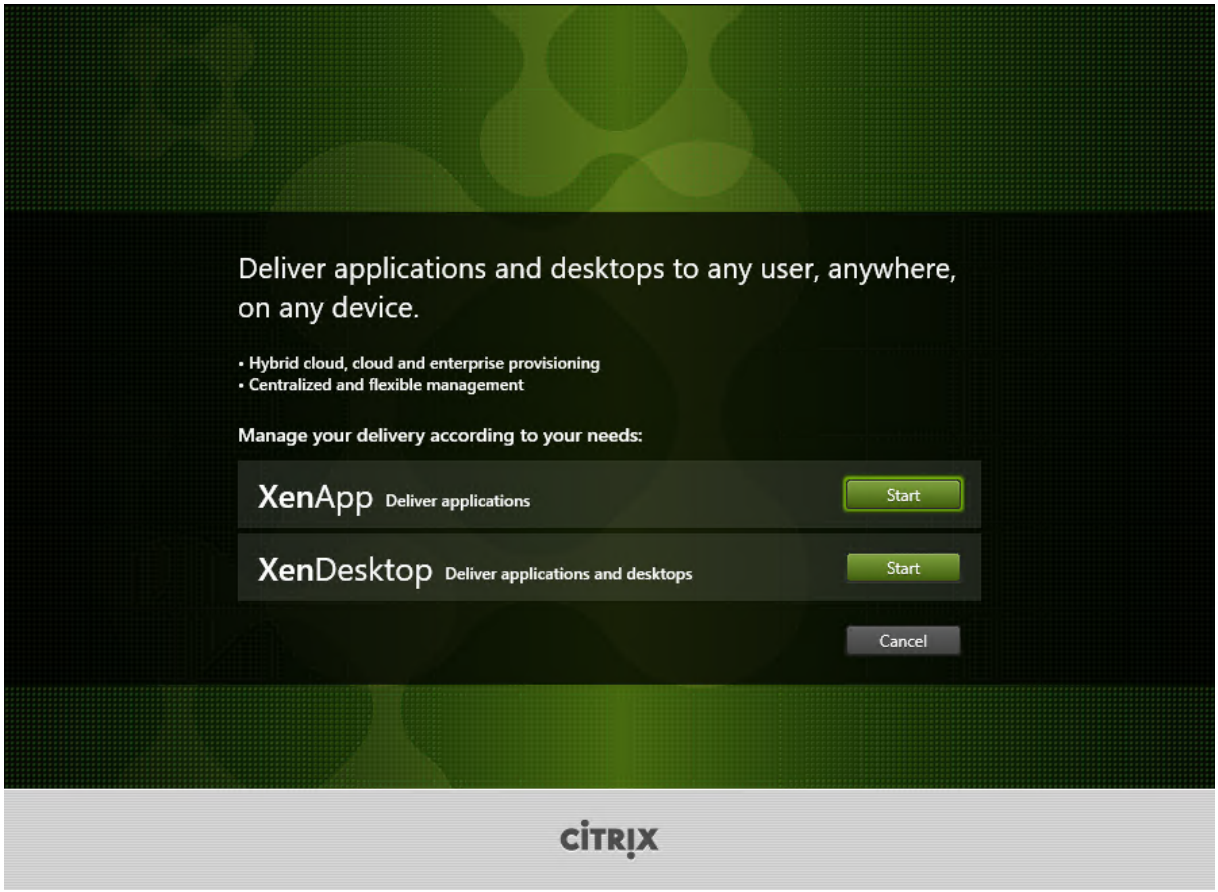
Installieren Sie den Sitzungsaufzeichnungsplayer auf dem Sitzungsaufzeichnungsserver oder auf mindestens einer Arbeitsstation in der Domäne für Benutzer, die Sitzungsaufzeichnungen anzeigen.

Schritt 1: Herunterladen der Produktsoftware und Starten des Assistenten

Melden Sie sich mit einem lokalen Administratorkonto bei der Maschine an, auf der Sie den Sitzungsaufzeichnungsplayer installieren. Legen Sie die DVD in das Laufwerk ein oder stellen Sie die ISO-Datei bereit. Wenn das Installationsprogramm nicht automatisch gestartet wird, doppelklicken Sie auf die Anwendung **AutoSelect** oder das bereitgestellte Laufwerk.

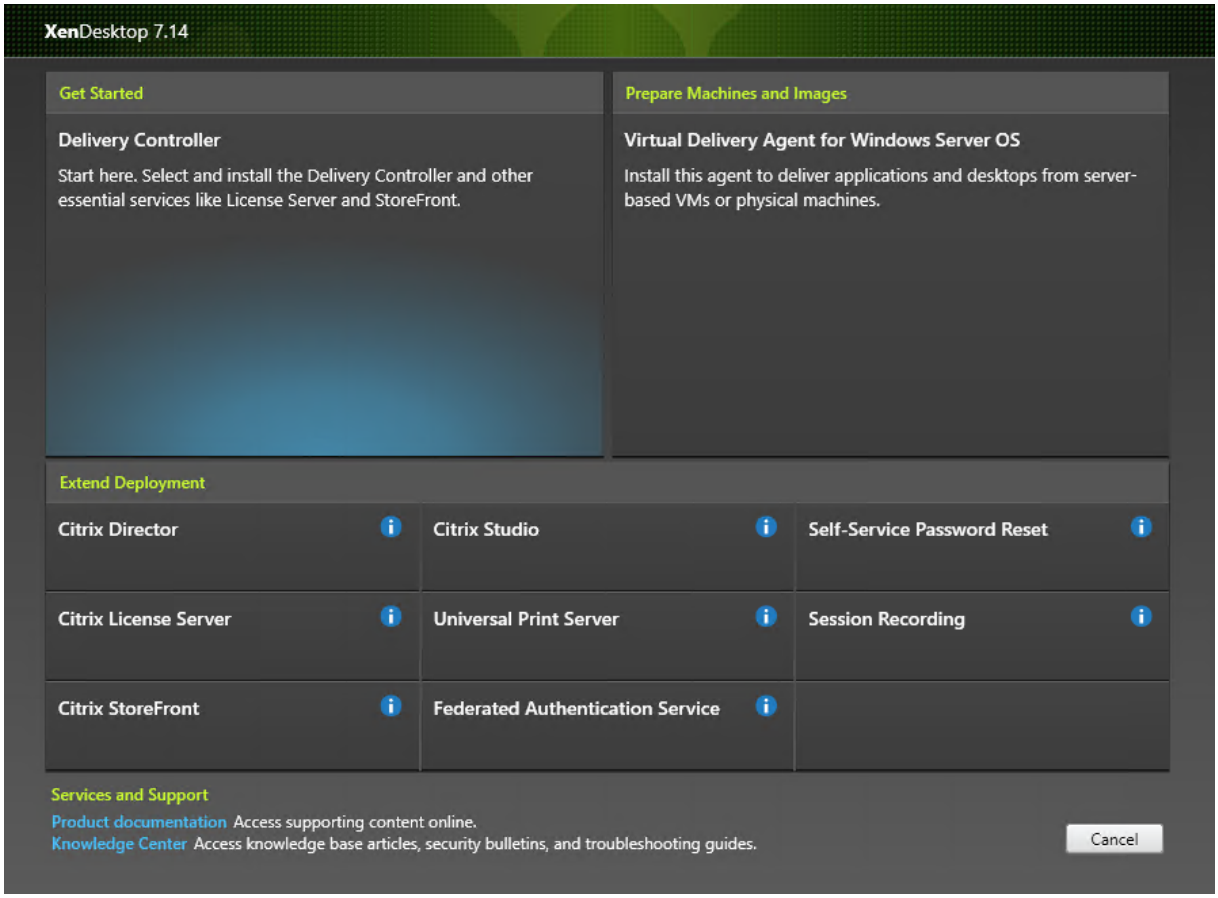
Der Installationsassistent wird gestartet.

Schritt 2: Auswählen des zu installierenden Produkts



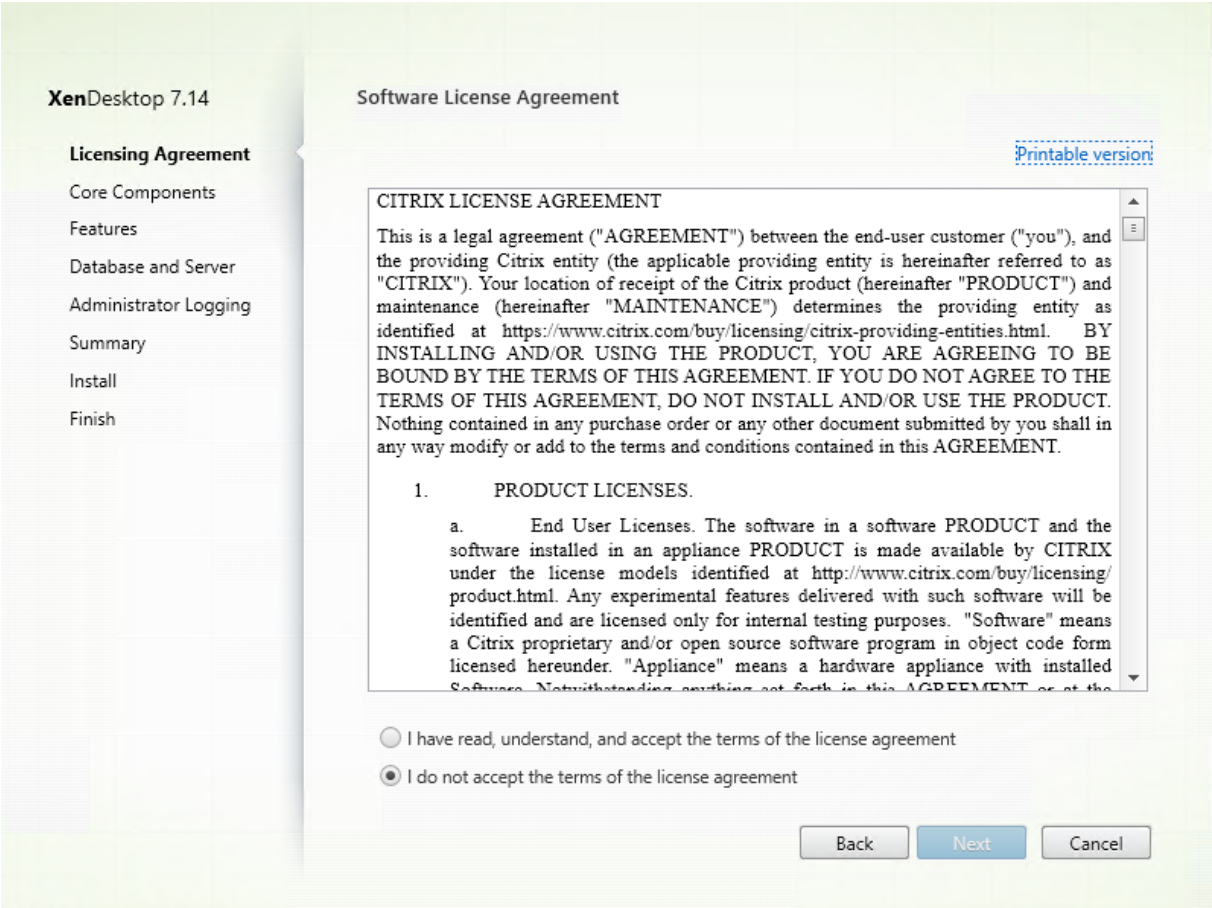
Klicken Sie auf **Start** neben dem zu installierenden Produkt: **XenApp** oder **XenDesktop**.

Schritt 3: Auswählen der Sitzungsaufzeichnung



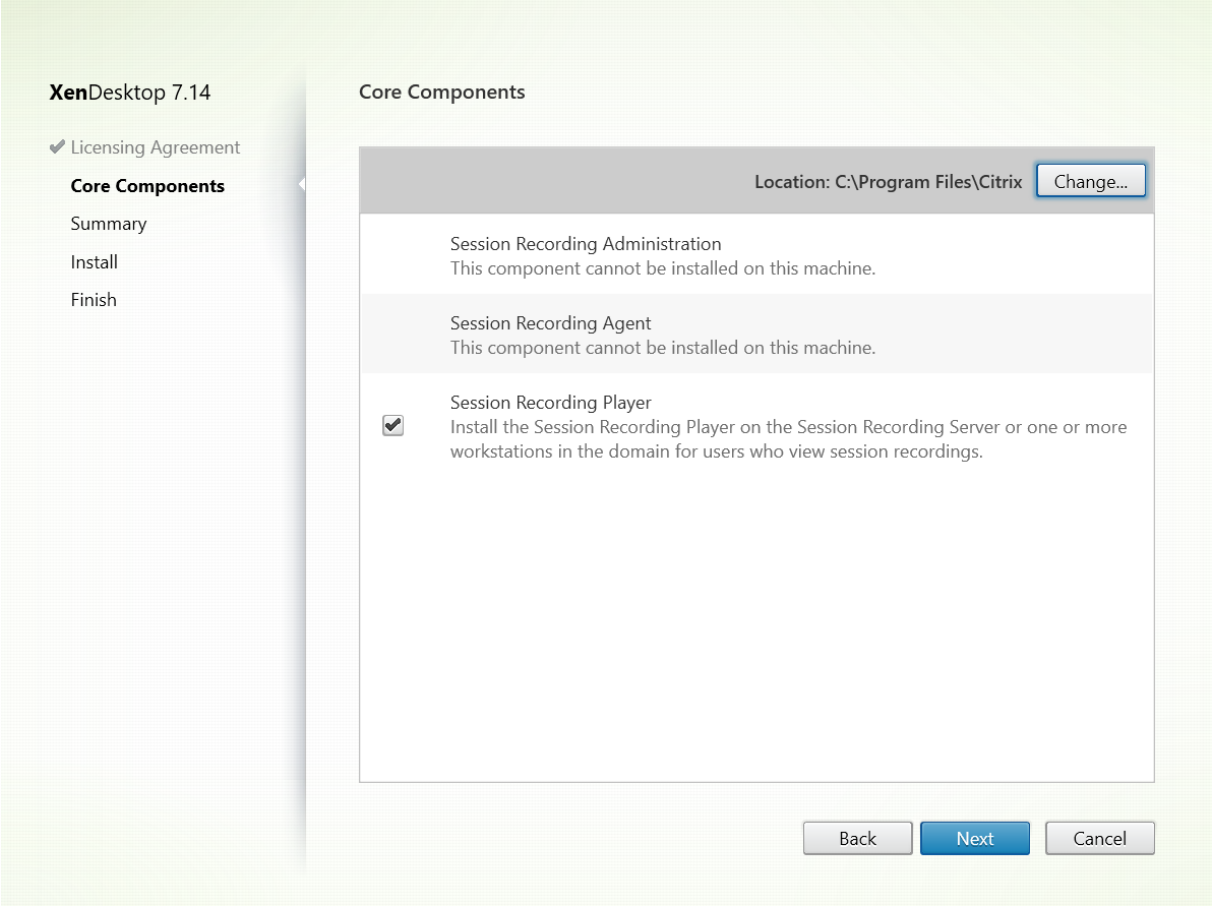
Wählen Sie den Eintrag **Sitzungsaufzeichnung**.

Schritt 4: Lesen und Akzeptieren der Lizenzvereinbarung



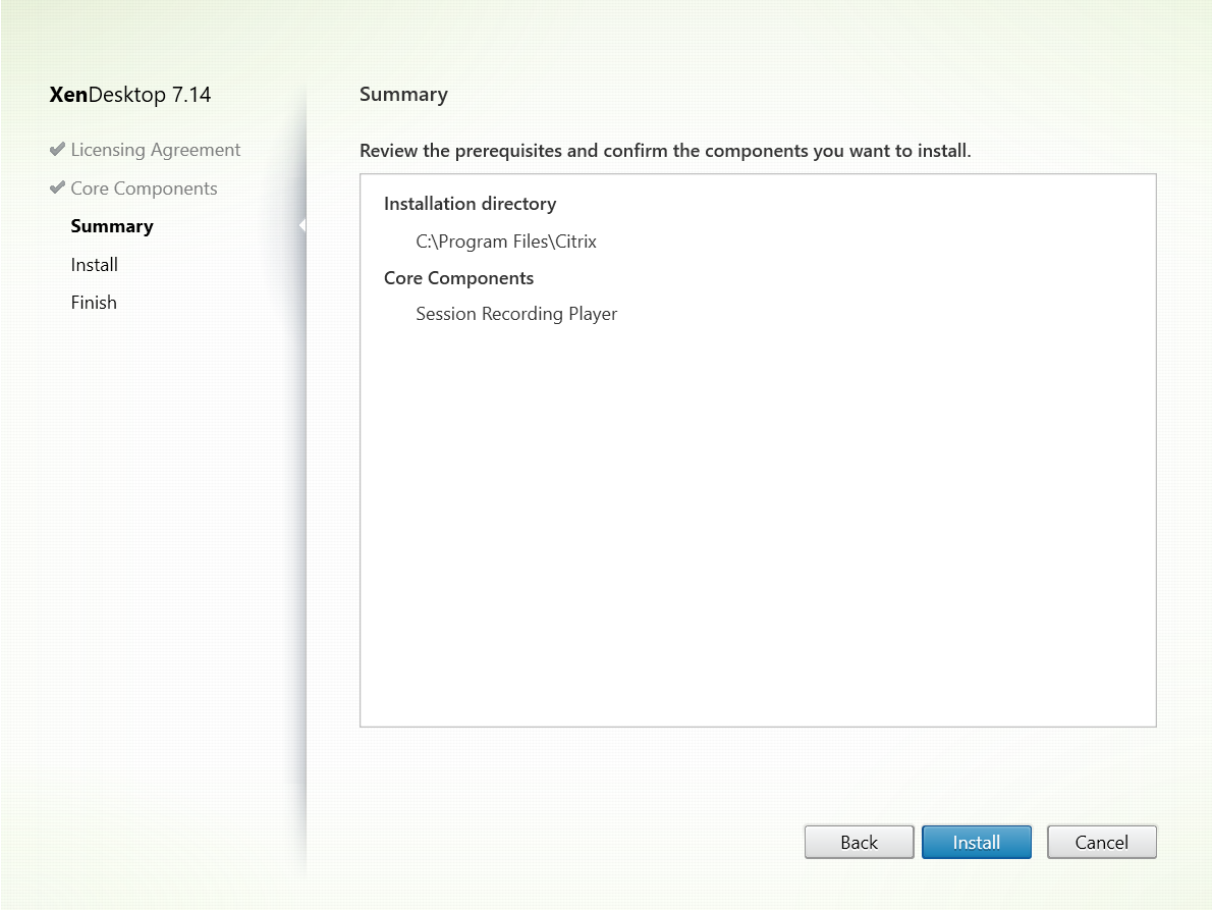
Lesen Sie die **Lizenzvereinbarung**, akzeptieren Sie sie und klicken Sie auf **Weiter**.

Schritt 5: Auswählen der Komponente und des Speicherorts für die Installation



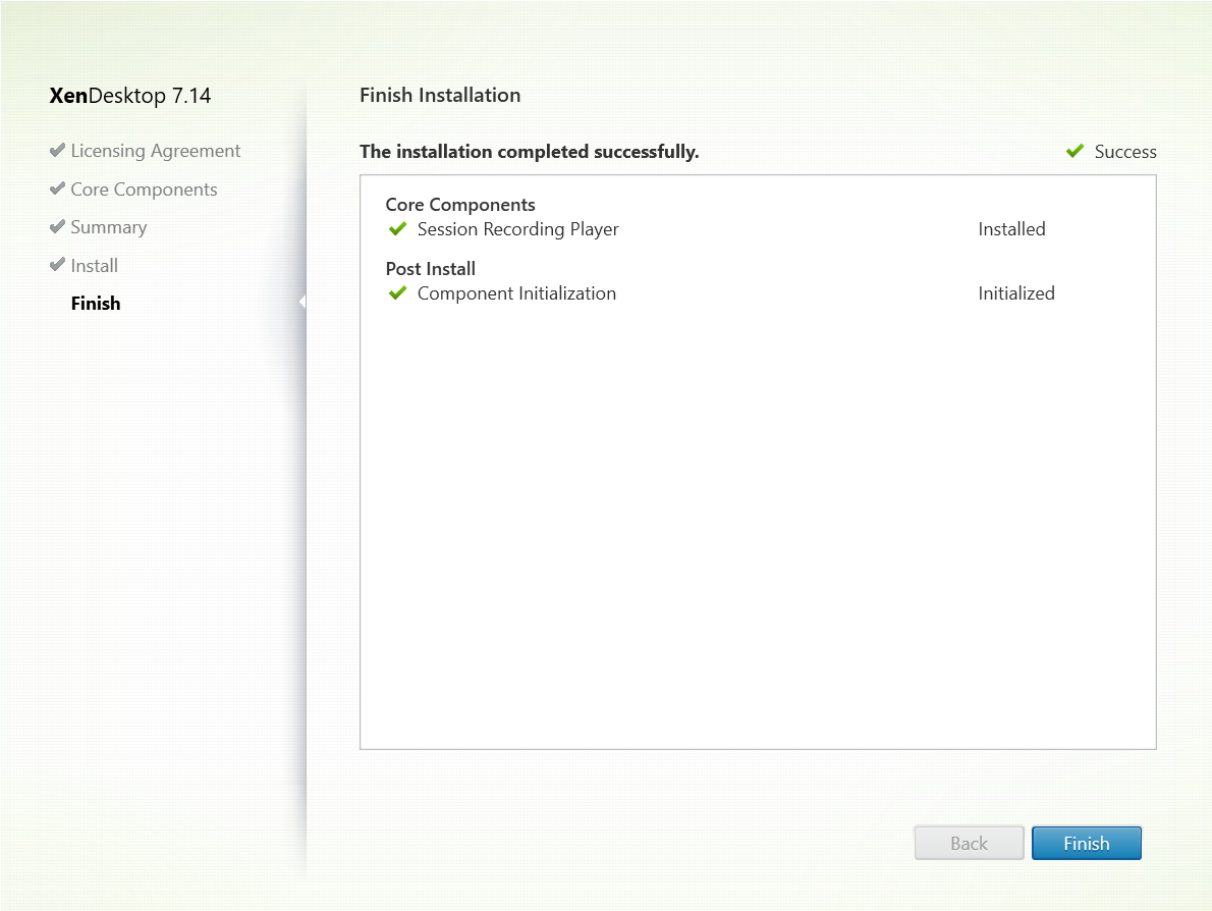
Wählen Sie **Sitzungsaufzeichnungsverwaltung** und klicken Sie auf **Weiter**.

Schritt 6: Überprüfen der Voraussetzungen und Bestätigen der Installation



Die Seite **Zusammenfassung** enthält die Installationsoptionen. Sie können mit der Schaltfläche **Zurück** zu vorherigen Seiten zurückkehren und Ihre Auswahl ändern. Klicken Sie alternativ auf **Installieren**, um die Installation zu starten.

Schritt 7: Abschließen der Installation



Die Seite **Fertigstellen der Installation** enthält grüne Häkchen für alle Voraussetzungen und Komponenten, die installiert und initialisiert werden konnten.

Klicken Sie auf **Fertig stellen**, um die Installation des Sitzungsaufzeichnungsplayers abzuschließen.

Automatisieren von Installationen

Zur Installation des Sitzungsaufzeichnungsagents auf mehreren Servern können Sie ein Skript erstellen, das eine Installation ohne Benutzereingriffe ausführt.

Mit dem folgenden Befehl installieren Sie den Sitzungsaufzeichnungsagent und erstellen eine Protokolldatei, in der die Installationsinformationen aufgezeichnet werden.

64-Bit-Systeme:

msiexec /i SessionRecordingAgentx64.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

Hinweis: Die SessionRecordingAgentx64.msi-Datei im XenApp-/XenDesktop-ISO-Image ist unter \layout\image-full\x64\Session Recording.

32-Bit-Systeme:

msiexec /i SessionRecordingAgent.msi /q /l*vx *yourinstallationlog* SESSIONRECORDINGSERVERNAME=yourservername SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol SESSIONRECORDINGBROKERPORT=yourbrokerport

Hinweis: Die SessionRecordingAgent.msi-Datei im XenApp-/XenDesktop-ISO-Image ist unter \layout\image-full\x86\Session Recording.

Wobei:

yourservername ist der NetBIOS-Name oder FQDN des Computers, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird. Wenn Sie keinen Namen eingeben, wird der Standardwert **localhost** verwendet.

yourbrokerport ist eine Ganzzahl, die den Port angibt, über den der Sitzungsaufzeichnungsagent mit dem Sitzungsaufzeichnungsbroker kommuniziert. Erfolgt keine Angabe, wird standardmäßig HTTPS verwendet.

yourbrokerport entspricht der Nummer des Ports, über den der Sitzungsaufzeichnungsagent mit dem Sitzungsaufzeichnungsbroker kommuniziert. Wenn Sie keine Eingabe machen, wird als Standardwert Null verwendet, d. h. der Sitzungsaufzeichnungsagent verwendet den Standardport für das ausgewählte Protokoll: 80 für HTTP oder 443 für HTTPS.

/l*v gibt eine ausführliche Protokollierung an.

yourinstallationlog ist der Speicherort der Installationsprotokolldatei.

/q gibt den stillen Modus an.

Upgrade der Sitzungsaufzeichnung

Sie können bestimmte Bereitstellungen aktualisieren, ohne zunächst neue Maschinen oder Sites erstellen zu müssen. Sie können ein Upgrade von Version 7.6 (oder einer höheren Version) der Sitzungsaufzeichnung auf das aktuelle Release durchführen.

Hinweise:

- Wenn Sie ein Upgrade der Sitzungsaufzeichnungsverwaltung von Version 7.6 auf 7.13 oder höher durchführen und unter "Sitzungsaufzeichnungsverwaltung"zum Hinzufügen der Administratorprotokollierung **Ändern** wählen, wird der SQL Server-Instanzname auf der Seite **Konfiguration der Administratorprotokollierung** nicht angezeigt. Die folgende Fehlermeldung

wird angezeigt, wenn Sie auf **Weiter** klicken: `Database connection test failed. Please enter correct Database instance name`. Fügen Sie als Workaround dem folgenden Ordner der SmartAuditor Server-Registrierung die Leseberechtigung für localhost-Benutzer hinzu: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.

- Das Upgrade der Datenbank für die Sitzungsaufzeichnung kann fehlschlagen, wenn nur diese Komponente auf einer Maschine installiert ist. Überprüfen Sie in diesem Fall, ob die folgenden Registrierungseinträge unter HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\SmartAuditor\Data vorhanden sind. Wenn dies nicht der Fall ist, fügen Sie die Einträge vor dem Upgrade manuell hinzu.

Schlüsselname	Schlüsseltyp	Schlüsselwert
SmAudDatabaseInstance	Zeichenfolge	Instanzname der Datenbank für die Sitzungsaufzeichnung
DatabaseName	Zeichenfolge	Datenbankname der Datenbank für die Sitzungsaufzeichnung

Anforderungen, Vorbereitung und Einschränkungen

Hinweis: Sie können kein Upgrade von einer Technology Preview-Version ausführen.

- Sie müssen über die grafische Oberfläche oder die Befehlszeile des Installationsprogramms für die Sitzungsaufzeichnung ein Upgrade von deren Komponenten auf der Maschine ausführen, auf der die Komponenten installiert sind.
- Vor Beginn des Upgrades machen Sie ein Backup der Datenbank "CitrixSessionRecording"auf der SQL Server-Instanz, damit Sie sie im Falle eines Problems nach dem Datenbankupgrade wiederherstellen können.
- Auf den Maschinen, auf denen Sie die Komponenten der Sitzungsaufzeichnung aktualisieren, müssen Sie sowohl Domänenbenutzer als auch lokaler Administrator sein.
- Sind Server und Datenbank der Sitzungsaufzeichnung nicht auf dem gleichen Server installiert, benötigen Sie die Datenbankrollenberechtigung für das Upgrade der Datenbank für die Sitzungsaufzeichnung. Alternativen:
  - Bitten Sie den Datenbankadministrator die Rollenberechtigungen **securityadmin** und **dbcreator** für das Upgrade zuzuweisen. Nach Abschluss des Upgrades werden die Serverrollenberechtigungen **securityadmin** und **dbcreator** nicht mehr benötigt und können entfernt werden.
  - Verwenden Sie das Paket SessionRecordingAdministrationx64.msi für das Upgrade. Wenn der aktuelle Benutzer nicht der Datenbankadministrator ist, wird während des Upgrades

ein Dialogfeld angezeigt, in dem die Anmeldeinformationen eines Datenbankadministrators mit den Serverrollenberechtigungen **securityadmin** und **dbcreator** eingegeben werden müssen. Geben Sie die richtigen Anmeldeinformationen ein und klicken Sie auf **OK** um mit dem Upgrade fortzufahren.

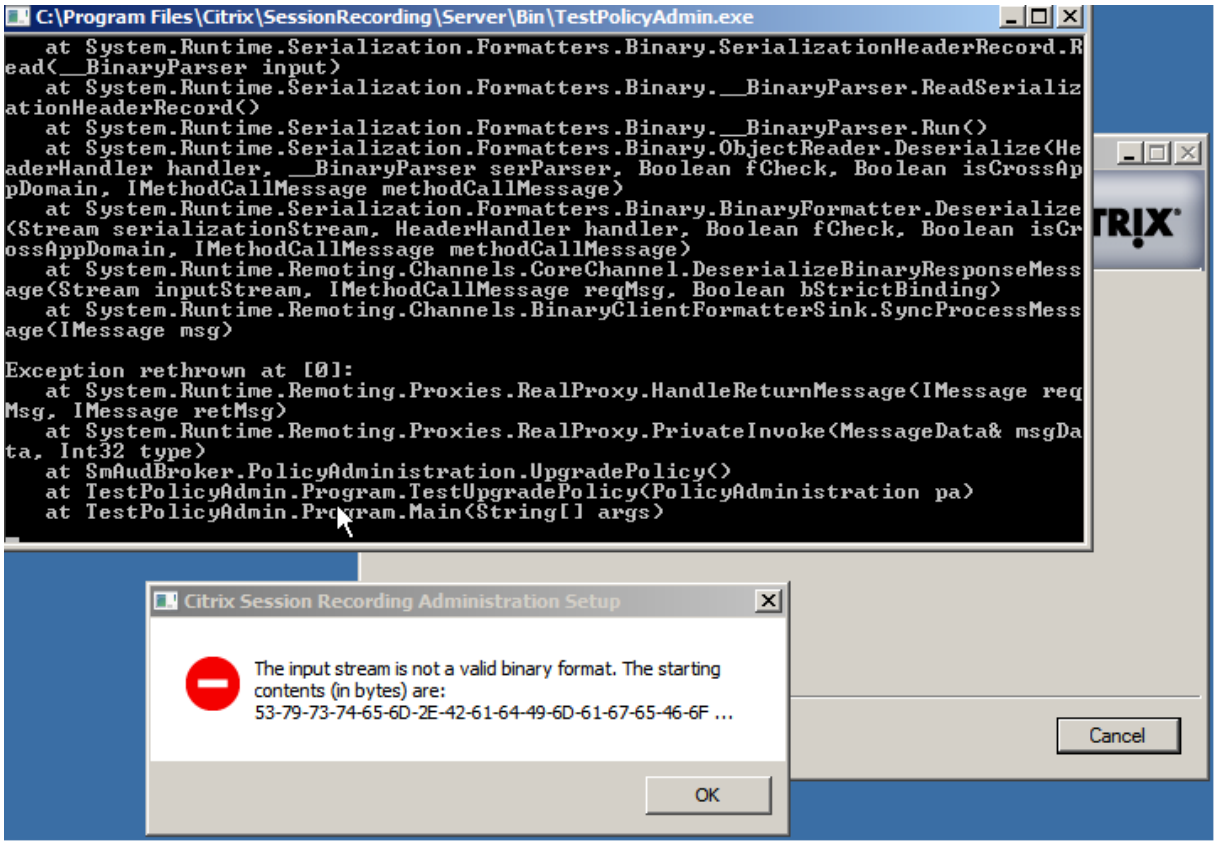
- Wenn Sie nicht alle Sitzungsaufzeichnungsagents zur gleichen Zeit aktualisieren möchten, können Sie Version 7.6.0 (oder höher) für das aktuelle Release des Sitzungsaufzeichnungsservers verwenden. Allerdings stehen dann einige neue Features und Fehlerbehebungen ggf. nicht zur Verfügung.
- Sitzungen, die während des Upgrades des Sitzungsaufzeichnungsservers gestartet werden, werden nicht aufgezeichnet.
- Die Option **Grafikanpassung** in den Eigenschaften des Sitzungsaufzeichnungsagents sind nach einer Neuinstallation oder einem Upgrade standardmäßig aktiviert, um Kompatibilität mit der Desktopgestaltungsumleitung zu gewährleisten. Sie können diese Option nach einer Neuinstallation oder einem Upgrade manuell deaktivieren.
- Die Administratorprotokollierung wird nicht installiert, wenn ein Upgrade der Sitzungsaufzeichnung von einem vorherigen Release, der dieses Feature nicht enthielt, durchgeführt wird. Zum Hinzufügen dieses neuen Features ändern Sie die Installation nach dem Upgrade.
- Laufen zu Beginn des Upgrades Sitzungen, kann deren Aufzeichnung sehr wahrscheinlich nicht ausgeführt werden.
- Lesen Sie den Abschnitt zur Upgradereihenfolge weiter unten, damit Sie mögliche Ausfälle einplanen und das Risiko senken können.

Aktualisierungsreihenfolge

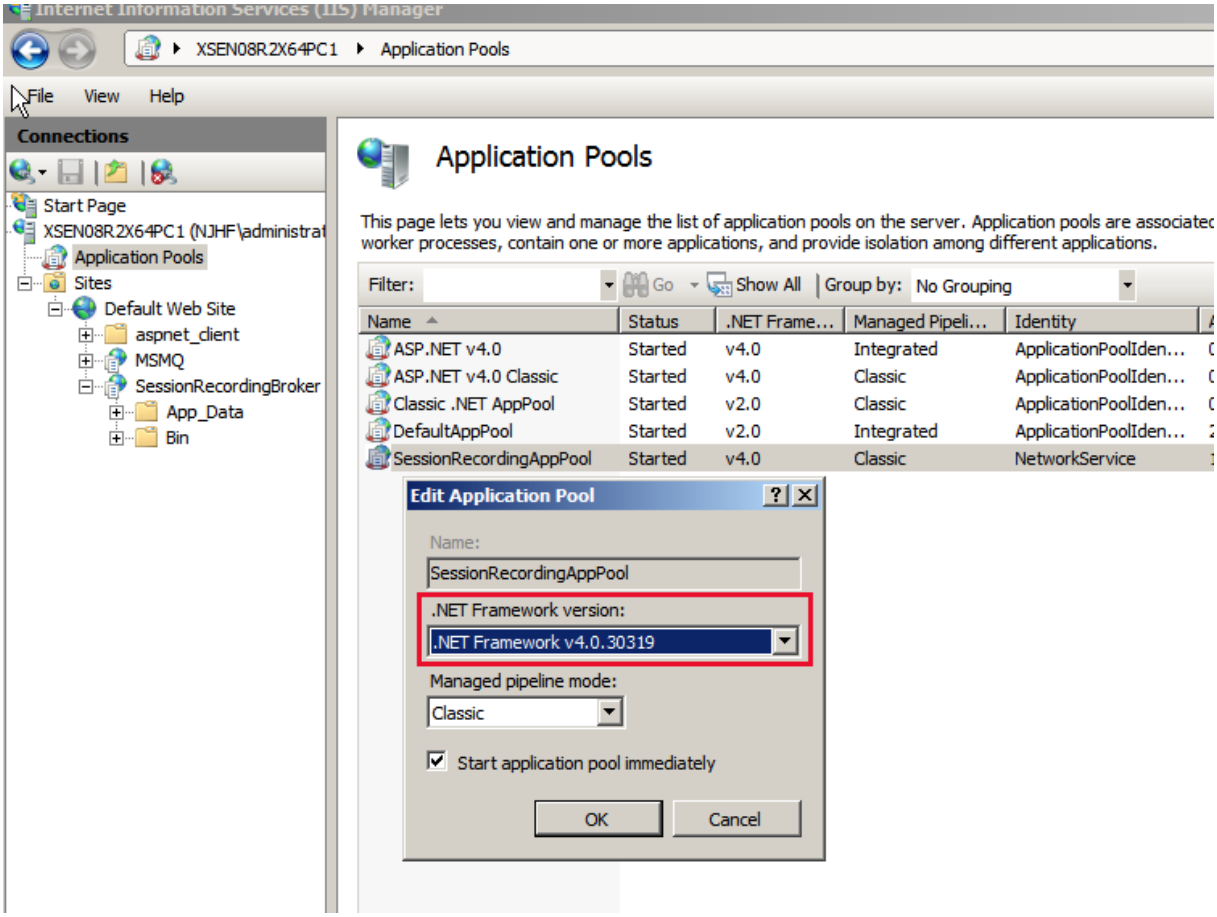
1. Sind Server und Datenbank für die Sitzungsaufzeichnung auf verschiedenen Servern installiert, beenden Sie den Speichermanager der Sitzungsaufzeichnung auf dem Sitzungsaufzeichnungsserver manuell und führen Sie zunächst das Upgrade der Datenbank durch.
2. Stellen Sie sicher, dass der Sitzungsaufzeichnungsbroker mit IIS ausgeführt wird. Führen Sie das Upgrade des Sitzungsaufzeichnungsservers durch. Sind Datenbank und Server der Sitzungsaufzeichnung auf dem gleichen Server installiert, erfolgt auch ein Upgrade der Datenbank.
3. Der Sitzungsaufzeichnungsdienst geht automatisch wieder online, sobald das Upgrade des Sitzungsaufzeichnungsservers abgeschlossen ist.
4. Führen Sie das Upgrade des Sitzungsaufzeichnungsagents (auf dem Masterimage) durch.
5. Führen Sie das Upgrade der Richtlinienkonsole für die Sitzungsaufzeichnung zusammen mit oder nach dem des Sitzungsaufzeichnungsservers durch.
6. Führen Sie das Upgrade des Sitzungsaufzeichnungsplayers durch.

Hinweis: Der folgende Fehler kann auftreten, wenn Sie ein Upgrade der Administratorkomponente

der Sitzungsaufzeichnungsverwaltung unter Windows Server 2008 R2 durchführen.



Ändern Sie in diesem Fall die “.NET Framework-Version”für “SessionRecordingAppPool”in “.NET Framework v4”in IIS, und führen Sie das Upgrade noch einmal durch.



Deinstallieren der Sitzungsaufzeichnung

Verwenden Sie zum Entfernen von Komponenten der Sitzungsaufzeichnung von einem Server oder einer Arbeitsstation die Option zum Deinstallieren von Programmen in der Windows-Systemsteuerung. Zum Entfernen der Datenbank für die Sitzungsaufzeichnung benötigen Sie die gleichen SQL Server-Rollenberechtigungen wie bei der Installation (**securityadmin** und **dbcreator**).

Aus Sicherheitsgründen wird die Datenbank der Administratorprotokollierung nach der Deinstallation der Komponenten nicht entfernt.

Konfigurieren der Sitzungsaufzeichnung

July 10, 2020

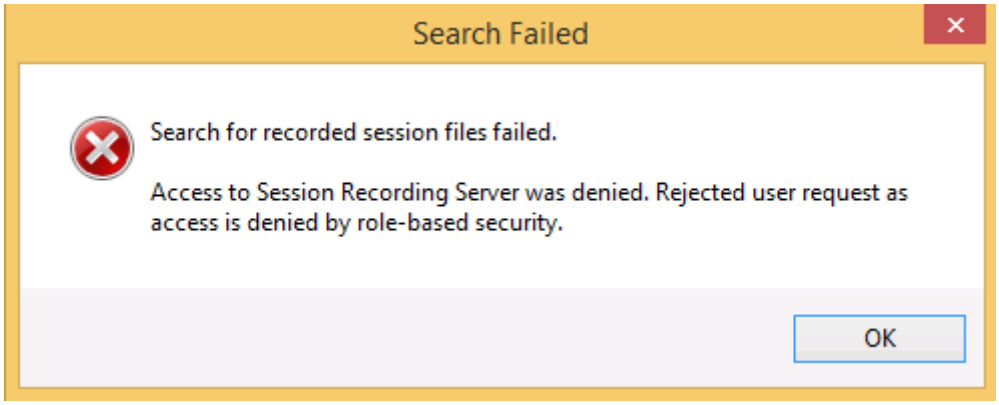
Konfigurieren der Sitzungsaufzeichnung für die Wiedergabe und Aufzeichnung von Sitzungen

Nach der Installation der Sitzungsaufzeichnungskomponenten konfigurieren Sie die Sitzungsaufzeichnung mit den folgenden Schritten für die Aufzeichnung von XenApp- bzw. XenDesktop-Sitzungen und das benutzerseitige Anzeigen der Sitzungen.

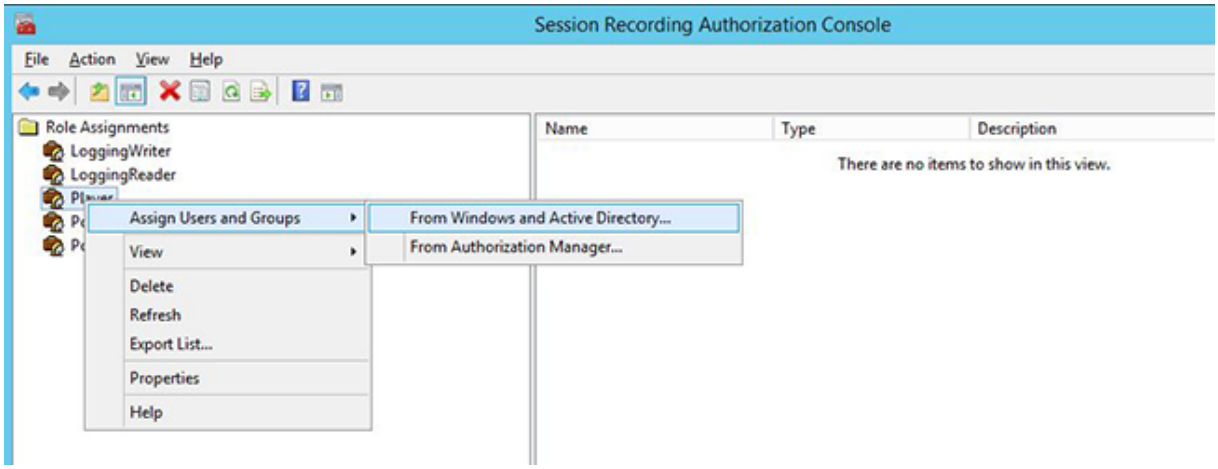
- Berechtigen von Benutzern zur Wiedergabe von Aufzeichnungen
- Berechtigen von Benutzern zur Verwaltung von Aufzeichnungsrichtlinien
- Festlegen einer aktiven Aufzeichnungsrichtlinie zum Aufzeichnen von Sitzungen
- Konfigurieren von benutzerdefinierten Richtlinien
- Konfigurieren des Sitzungsaufzeichnungsplayers für die Verbindung mit dem Sitzungsaufzeichnungsserver

Berechtigen von Benutzern zur Wiedergabe von Sitzungsaufzeichnungen

Nach der Installation der Sitzungsaufzeichnung ist zunächst kein Benutzer berechtigt, Sitzungsaufzeichnungen wiederzugeben. Sie müssen jedem Benutzer, auch dem Administrator, Berechtigungen zuweisen. Ein Benutzer ohne Berechtigung zur Wiedergabe von Sitzungsaufzeichnungen erhält die folgende Fehlermeldung bei dem Versuch, eine Sitzungsaufzeichnung wiederzugeben:



1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver als Administrator an.
2. Starten Sie die Sitzungsaufzeichnungsautorisierungskonsole.
3. Klicken Sie in der Sitzungsaufzeichnungsautorisierungskonsole auf Player.
4. Wählen Sie die Benutzer und Gruppen aus, denen Sie Berechtigungen zur Wiedergabe von Sitzungsaufzeichnungen geben möchten.



Berechtigen von Benutzern zur Verwaltung von Aufzeichnungsrichtlinien

Bei der Installation der Sitzungsaufzeichnung gewähren standardmäßig Domänenadministratoren Berechtigung zum Steuern von Aufzeichnungsrichtlinien. Sie können die Autorisierungseinstellung ändern.

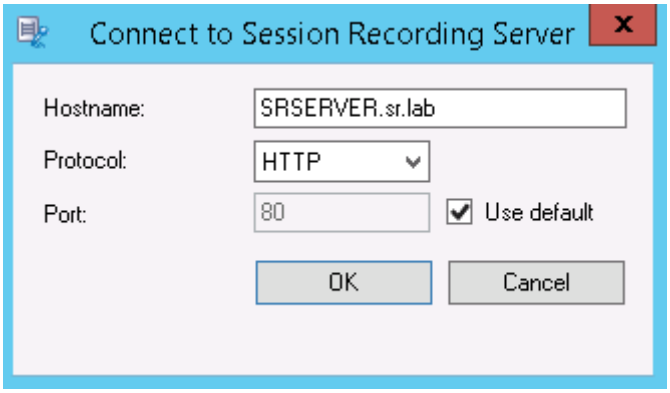
1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver als Administrator an.
2. Starten Sie die Sitzungsaufzeichnungs-Autorisierungskonsole und wählen Sie PolicyAdministrators aus.
3. Fügen Sie die Benutzer und Gruppen hinzu, die Aufzeichnungsrichtlinien verwalten sollen.

Festlegen der aktiven Aufzeichnungsrichtlinie zum Aufzeichnen von Sitzungen

Die aktive Aufzeichnungsrichtlinie legt ein Sitzungsaufzeichnungsverhalten für alle VDAs und VDIs fest, auf denen der Sitzungsaufzeichnungsagent installiert ist und die eine Verbindung mit dem Sitzungsaufzeichnungsserver herstellen. Bei der Installation der Sitzungsaufzeichnung wird als aktive Richtlinie **Nicht aufzeichnen** verwendet. Sitzungen können erst aufgezeichnet werden, wenn Sie die aktive Aufzeichnungsrichtlinie ändern.

Wichtig: Eine Richtlinie kann viele Regeln enthalten, aber es kann jeweils nur eine aktive Richtlinie ausgeführt werden.

1. Melden Sie sich bei dem Server, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Computers, auf dem der Sitzungsaufzeichnungsserver gehostet wird, das Protokoll und die Portnummer richtig sind.



4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung **Aufzeichnungsrichtlinien**, um die verfügbaren Aufzeichnungsrichtlinien anzuzeigen. Ein Häkchen gibt die aktive Richtlinie an:

    - **Nicht aufzeichnen**. Die Standardrichtlinie. Wenn Sie keine andere Richtlinie festlegen, wird keine Sitzung aufgezeichnet.
    - **Alle mit Benachrichtigung aufzeichnen**. Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Es wird für jede Aufzeichnungsinstanz ein Fenster mit einer entsprechenden Benachrichtigung angezeigt.
    - **Alle ohne Benachrichtigung aufzeichnen**. Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Es wird kein Fenster mit einer entsprechenden Benachrichtigung angezeigt.

5. Wählen Sie die Richtlinie aus, die Sie als aktiv festlegen möchten.
6. Klicken Sie im Menü auf **Aktion** > **Richtlinie aktivieren**.

Sie können in der Sitzungsaufzeichnung eigene Aufzeichnungsrichtlinien erstellen. Die erstellten Aufzeichnungsrichtlinien werden im Ordner **Aufzeichnungsrichtlinien** der Richtlinienkonsole für die Sitzungsaufzeichnung angezeigt.

Die generische Aufzeichnungsrichtlinie entspricht u. U. nicht Ihren Anforderungen. Sie können Richtlinien und Regeln basierend auf Benutzern, VDA- und VDI-Servern, Bereitstellungsgruppen und Anwendungen konfigurieren. Weitere Informationen zu benutzerdefinierten Richtlinien finden Sie unter Erstellen benutzerdefinierter Aufzeichnungsrichtlinien.

Hinweis: Die Administratorprotokollierung der Sitzungsaufzeichnung ermöglicht die Protokollierung von Änderungen an der Sitzungsaufzeichnungsrichtlinie. Weitere Informationen finden Sie unter Protokollierte Verwaltungsaktivitäten.

Konfigurieren des Sitzungsaufzeichnungsplayers

Damit der Sitzungsaufzeichnungsplayer Sitzungen wiedergeben kann, müssen Sie die Verbindung mit dem Sitzungsaufzeichnungsserver konfigurieren, auf dem die Sitzungsaufzeichnungen gespeichert

sind. Jeder Sitzungsaufzeichnungsplayer kann eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen, jedoch kann nur jeweils eine Verbindung aktiv sein. Wenn ein Sitzungsaufzeichnungsplayer eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen kann, können Benutzer den gewünschten Sitzungsaufzeichnungsserver durch Auswahl eines Kontrollkästchens auf der Registerkarte **Verbindungen** unter **Extras** > **Optionen** festlegen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Starten Sie den Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf **Extras** > **Optionen**.
4. Klicken Sie auf der Registerkarte **Verbindungen** auf **Hinzufügen**.
5. Geben Sie im Feld **Hostname** den Namen oder die IP-Adresse des Computers mit dem Sitzungsaufzeichnungsserver ein und wählen Sie das Protokoll aus. Standardmäßig verwendet die Sitzungsaufzeichnung HTTPS/SSL für die sichere Kommunikation. Wenn SSL nicht konfiguriert ist, wählen Sie HTTP.
6. Um den Sitzungsaufzeichnungsplayer so zu konfigurieren dass er eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen kann, wiederholen Sie Schritt 4 und 5 für jeden Server.
7. Aktivieren Sie das Kontrollkästchen für den Sitzungsaufzeichnungsserver, mit dem Sie eine Verbindung herstellen möchten.

Konfigurieren der Verbindung mit dem Sitzungsaufzeichnungsserver

Die Verbindung zwischen Sitzungsaufzeichnungsagent und dem Sitzungsaufzeichnungsserver wird normalerweise bei der Installation des Agents konfiguriert. Die Verbindung kann nach der Installation des Sitzungsaufzeichnungsagents in dessen Eigenschaften konfiguriert werden.

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Verbindungen**.
4. Geben Sie im Feld **Sitzungsaufzeichnungsserver** den FQDN des Sitzungsaufzeichnungsservers ein.

   > **Hinweis:**
   >
   > Um Message Queuing über HTTPS zu verwenden (Standardeinstellung ist TCP), geben Sie einen FQDN in das Feld **Sitzungsaufzeichnungsserver** ein. Andernfalls schlägt die Sitzungsaufzeichnung fehl.

5. Wählen Sie im Bereich **Nachrichtenwarteschlange des Speichermanagers** der Sitzungsaufzeichnung das Protokoll aus, das der Speichermanager der Sitzungsaufzeichnung für die Kommu-

nikation verwendet. Sie können auch die Standardportnummer ändern.

> **Hinweis:**
>
> Um Message Queuing über HTTP und HTTPS zu verwenden, installieren Sie alle von IIS empfohlenen Features.

6. Akzeptieren Sie im Feld **Lebensdauer** den Standardwert 7200 Sekunden (zwei Stunden) oder geben Sie einen neuen Wert für die Anzahl der Sekunden ein, für die jede Nachricht in der Warteschlange gespeichert wird, wenn ein Kommunikationsfehler auftritt. Nach dem Ablauf dieses Zeitraums wird die Nachricht gelöscht und die Datei kann nur bis an die Stelle wiedergegeben werden, an der die Daten verloren wurden.
7. Wählen Sie im Bereich **Sitzungsaufzeichnungsbroker** das Protokoll aus, das der Sitzungsaufzeichnungsbroker für die Kommunikation verwendet. Sie können auch die Standardportnummer ändern.
8. Starten Sie auf Aufforderung den **Sitzungsaufzeichnungsagent-Dienst** neu, um die Änderung zu übernehmen.

Gewähren von Zugriffsrechten für Benutzer

January 22, 2019

> **Wichtig:**
>
> Aus Sicherheitsgründen sollten Sie den Benutzern nur die Rechte geben, die sie zum Ausführen bestimmter Funktionen benötigen, z. B. Anzeigen aufgezeichneter Sitzungen.

Sie weisen den Benutzern in der Sitzungsaufzeichnungsautorisierungskonsole auf dem Sitzungsaufzeichnungsserver Rollen zu und gewähren den Sitzungsaufzeichnungsbenutzern Rechte. Sitzungsaufzeichnungsbenutzer haben drei Rollen:

- **Player.** Mitglieder der Rolle können aufgezeichnete XenApp-Sitzungen anzeigen. Für diese Rolle besteht keine Standardeinstellung.
- **PolicyQuery.** Die Server mit dem Sitzungsaufzeichnungsagent können Auswertungen der Aufzeichnungsrichtlinie anfordern. In der Standardeinstellung sind authentifizierte Benutzer Mitglieder dieser Rolle.
- **PolicyAdministrator.** Mitglieder dieser Rolle können Aufzeichnungsrichtlinien anzeigen, erstellen, bearbeiten, löschen und aktivieren. In der Standardeinstellung sind Administratoren des Computers, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird, Mitglieder dieser Rolle.

Die Sitzungsaufzeichnung unterstützt in Active Directory definierte Benutzer und Gruppen.

Zuweisen von Rollen zu Benutzern

1. Melden Sie sich bei dem Computer, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird, als Administrator oder Richtlinienadministrator an.
2. Starten Sie die Sitzungsaufzeichnungsautorisierungskonsole.
3. Wählen Sie die Rolle, der Sie Benutzer zuweisen möchten.
4. Wählen Sie auf der Menüleiste **Aktion** > **Windows-Benutzer und -Gruppen zuweisen**.
5. Fügen Sie die Benutzer und Gruppen hinzu.

In der Konsole vorgenommene Änderungen werden beim Update (das jede Minute erfolgt) übernommen.

Erstellen und Aktivieren von Aufzeichnungsrichtlinien

February 10, 2021

Mit der Richtlinienkonsole für die Sitzungsaufzeichnung erstellen und aktivieren Sie Richtlinien, die festlegen, wie Sitzungen aufgezeichnet werden.

> **Wichtig:**
>
> Um die Richtlinienkonsole für die Sitzungsaufzeichnung zu verwenden, muss das Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi) installiert sein. Das Snap-In kann nicht automatisch über das Installationsprogramm installiert werden. Navigieren Sie zu dem Snap-In auf dem ISO-Image für XenApp und XenDesktop (\layout\image-full\x64\Citrix Desktop Delivery Controller) und folgen Sie den Anweisungen, um es manuell zu installieren. Anderenfalls kann es zu Fehlern kommen.
>
> **Tipp:**
>
> Sie können die Registrierung bearbeiten, um den Verlust von Aufzeichnungsdateien zu verhindern, falls Ihr Sitzungsaufzeichnungsserver unerwartet ausfällt. Melden Sie sich als Administrator bei der Maschine an, auf der der Sitzungsaufzeichnungsagent installiert ist, öffnen Sie den Registrierungs-Editor und fügen Sie unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent` einen DWORD-Wert hinzu: `DefaultRecordActionOnError` =1
> .

Sie können verfügbare Systemrichtlinien nach der Installation der Sitzungsaufzeichnung aktivieren oder eigene Richtlinien erstellen und aktivieren. Die Systemrichtlinien für die Sitzungsaufzeichnung wenden eine Regel auf alle Benutzer, veröffentlichten Anwendungen und Server an. In

benutzerdefinierten Richtlinien geben Sie an, welche Benutzer, veröffentlichten Anwendungen und Server aufgezeichnet werden.

Die aktive Richtlinie legt fest, welche Sitzungen aufgezeichnet werden. Nur jeweils eine Richtlinie ist aktiv.

Systemrichtlinien

Die Sitzungsaufzeichnung enthält die folgenden Systemrichtlinien:

- **Nicht aufzeichnen**. Die Standardrichtlinie. Wenn Sie keine andere Richtlinie festlegen, wird keine Sitzung aufgezeichnet.
- **Alle mit Benachrichtigung aufzeichnen**. Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Ein Popupfenster wird angezeigt, um auf die Aufzeichnung hinzuweisen.
- **Alle ohne Benachrichtigung aufzeichnen**. Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Kein Popupfenster wird angezeigt, um auf die Aufzeichnung hinzuweisen.

Systemrichtlinien können nicht geändert oder gelöscht werden.

Aktivieren einer Richtlinie

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf **OK**.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung **Aufzeichnungsrichtlinien**.
5. Wählen Sie die Richtlinie aus, die Sie als aktive Richtlinie verwenden möchten.
6. Klicken Sie im Menü auf **Aktion** > **Richtlinie aktivieren**.

Erstellen benutzerdefinierter Aufzeichnungsrichtlinien

Wenn Sie eine eigene Richtlinie erstellen, legen Sie Regeln fest und geben an, welche Sitzungen von Benutzern und Gruppen, veröffentlichten Anwendungen und Servern aufgezeichnet werden. Ein Assistent in der Richtlinienkonsole für die Sitzungsaufzeichnung unterstützt Sie beim Erstellen der Regeln. Zum Abrufen einer Liste der veröffentlichten Anwendungen und Server ist Siteadministrator-Leseberechtigung erforderlich. Konfigurieren Sie dies auf dem Delivery Controller der Site.

Für jede erstellte Regel geben Sie eine Aufzeichnungsaktion und Regelkriterien an. Die Aufzeichnungsaktion gilt für Sitzungen, die das Regelkriterium erfüllen.

Wählen Sie für jede Regel eine Aufzeichnungsaktion aus:

- **Nicht aufzeichnen**. (Wählen Sie **Sitzungsaufzeichnung deaktivieren** im Assistenten für **Regeln**.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, nicht aufgezeichnet werden.
- **Mit Benachrichtigung aufzeichnen**. (Wählen Sie **Sitzungsaufzeichnung mit Benachrichtigung aktivieren** im Assistenten für **Regeln**.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, aufgezeichnet werden. Ein Popupfenster wird angezeigt, um auf die Aufzeichnung hinzuweisen.
- **Ohne Benachrichtigung aufzeichnen**. (Wählen Sie **Sitzungsaufzeichnung ohne Benachrichtigung aktivieren** im Assistenten für **Regeln**.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, aufgezeichnet werden. Benutzer werden nicht über die Aufzeichnung informiert.

Wählen Sie für jede Regel mindestens eines der folgenden Elemente, um ein Regelkriterium zu erstellen:

- **Benutzer oder Gruppen**. erstellt eine Liste der Benutzer oder Gruppen, für die die Aufzeichnungsaktion der Regel gilt.
- **Veröffentlichte Ressourcen**. Erstellt eine Liste der veröffentlichten Anwendungen oder Desktops, auf die die Aufzeichnungsaktion der Regel angewendet wird. Wählen Sie im Assistenten für **Regeln** die XenApp und XenDesktop-Sites aus, auf denen die Anwendungen bzw. Desktops verfügbar sind.
- **Bereitstellungsgruppen oder Maschinen**. Erstellt eine Liste der Bereitstellungsgruppen oder Maschinen, auf die die Aufzeichnungsaktion der Regel angewendet wird. Wählen Sie im Assistenten für **Regeln** den Speicherort der Bereitstellungsgruppen oder Maschinen.
- **IP-Adresse oder IP-Bereich**. Erstellt eine Liste von IP-Adressen oder IP-Adressbereichen, für die die Aufzeichnungsaktion der Regel gilt. Fügen Sie auf dem Bildschirm **IP-Adresse und IP-Bereich auswählen** eine gültige IP-Adresse oder einen IP-Adressbereich hinzu, für die bzw. den die Aufzeichnung aktiviert oder deaktiviert werden soll.

Hinweis: Die Richtlinienkonsole für die Sitzungsaufzeichnung unterstützt das Konfigurieren mehrerer Kriterien innerhalb einer Regel. Ist eine Regel anwendbar, werden zum Berechnen der endgültigen Aktion die logischen Operatoren “AND”und “OR”verwendet. Dabei wird der Operator “OR”meist zwischen Elementen innerhalb eines Kriteriums verwendet, während der Operator “AND” zwischen separaten Kriterien zum Einsatz kommt. Wenn das Ergebnis “true”ist, führt die Engine für die Sitzungsaufzeichnungsrichtlinie die Regelaktion aus. Ansonsten wird die nächste Regel aufgerufen und der Prozess wird wiederholt.

Wenn Sie mehrere Regeln in einer Aufzeichnungsrichtlinie erstellen, können einige Sitzungen die Kri-

terien für mehrere Regeln erfüllen. In diesen Situationen wird die Regel mit der höchsten Priorität auf die Sitzungen angewendet.

Die Aufzeichnungsaktion einer Regel legt die Priorität fest:

- Regeln mit der Aktion **Sitzungsaufzeichnung deaktivieren** haben die höchste Priorität.
- Regeln mit der Aktion **Sitzungsaufzeichnung mit Benachrichtigung aktivieren** haben die nächsthöhere Priorität.
- Regeln mit der Aktion **Sitzungsaufzeichnung ohne Benachrichtigung aktivieren** haben die niedrigste Priorität.

Einige Sitzungen erfüllen ggf. kein Regelkriterium in einer Aufzeichnungsrichtlinie. Für diese Sitzungen gilt die Aufzeichnungsaktion der Fallbackregel der Richtlinie. Die Aufzeichnungsaktion der Fallbackregel ist immer **Nicht aufzeichnen**. Die Fallbackregel kann nicht geändert oder gelöscht werden.

Zum Konfigurieren von benutzerdefinierten Richtlinien führen Sie folgende Schritte aus:

1. Melden Sie sich bei dem Server, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung und wählen Sie links **Aufzeichnungsrichtlinien**. Klicken Sie in der Menüleiste auf **Aktion** > **Neue Richtlinie hinzufügen.**
3. Klicken Sie mit der rechten Maustaste auf **Neue Richtlinie** und wählen Sie **Neue Regel hinzufügen**.
4. Aufzeichnungsoption: Wählen Sie im Assistenten für **Regeln** die Option **Sitzungsaufzeichnung deaktivieren**, **Sitzungsaufzeichnung mit Benachrichtigung aktivieren** oder **Sitzungsaufzeichnung ohne Benachrichtigung aktivieren** und klicken Sie auf **Weiter**.
5. Regelkriterien: Sie können eine oder eine beliebige Kombination der folgenden Optionen wählen:
   Benutzer oder Gruppen
   Veröffentlichte Ressourcen
   Bereitstellungsgruppen oder Maschinen
   IP-Adresse oder IP-Bereich
6. Regelkriterium bearbeiten: Klicken Sie zum Bearbeiten auf die unterstrichenen Werte. Welche Werte unterstrichen sind, hängt von den Kriterien ab, die Sie im vorherigen Schritt ausgewählt haben.
   Hinweis: Bei Auswahl der Option **Veröffentlichte Ressourcen** ist die **Siteadresse** die IP-Adresse, eine URL oder ein Maschinenname, wenn der Controller in einem lokalen Netzwerk ist. Die Liste **Name der Anwendung** enthält den Anzeigenamen.
7. Folgen Sie dem Assistenten, um die Konfiguration abzuschließen.

Verwenden von Active Directory-Gruppen

Beim Erstellen von Richtlinien können Sie in der Sitzungsaufzeichnung Active Directory-Gruppen verwenden. Active Directory-Gruppen statt einzelner Benutzer vereinfachen die Erstellung und Verwaltung von Regeln und Richtlinien. Beispiel: Wenn Benutzer in der Buchhaltungsabteilung des Unternehmens zur Active Directory-Gruppe "Finanz"gehören, können Sie eine Regel erstellen, die für alle Mitglieder dieser Gruppe gilt, indem Sie die Gruppe "Finanz"beim Erstellen der Regel im Assistenten für **Regeln** auswählen.

Positivliste der Benutzer

Sie können Richtlinien für die Sitzungsaufzeichnung erstellen, die sicherstellen, dass die Sitzungen bestimmter Benutzer im Unternehmen nie aufgezeichnet werden. Dies wird *Positivliste* der Benutzer genannt. Positivlisten sind nützlich für Benutzer, die mit datenschutzrelevanten Informationen umgehen oder wenn Ihre Organisation die Sitzungen einer bestimmten Mitarbeiterklasse nicht aufzeichnen möchte.

Wenn beispielsweise alle Mitglieder der Geschäftsleitung im Unternehmen zu einer Active Directory-Gruppe "Geschäftsführung"gehören, können Sie sicherstellen, dass die Sitzungen dieser Benutzer nie aufgezeichnet werden, wenn Sie eine Regel erstellen, mit der die Sitzungsaufzeichnung für die Gruppe "Geschäftsführung"deaktiviert wird. Während die Richtlinie, die diese Regel enthält, aktiv ist, werden keine Sitzungen der Mitglieder der Gruppe "Geschäftsführung"aufgezeichnet. Die Sitzungen anderer Mitarbeiter im Unternehmen werden basierend auf den anderen Regeln in der aktiven Richtlinie aufgezeichnet.

Verwendung von IP-Adressen oder IP-Bereichen als Regelkriterien

Sie können IP-Adressen von Clients als Regelkriterien für die Richtlinienzuordnung verwenden. Wenn Sie beispielsweise Sitzungen von Clients mit bestimmten IP-Adressen oder innerhalb eines IP-Adressbereichs aufzeichnen möchten, erstellen Sie mit dem Assistenten für **Regeln** eine Regel, die nur für diese Clients gilt.

Erstellen einer Richtlinie

Hinweis: Bei Verwendung des Assistenten für **Regeln** werden Sie möglicherweise aufgefordert, zum Bearbeiten auf einen unterstrichenen Wert zu klicken, obwohl kein unterstrichener Wert angezeigt wird. Unterstrichene Werte werden nur in bestimmten Situationen angezeigt. Ignorieren Sie den Schritt, wenn kein unterstrichener Wert angezeigt wird.

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf **OK**.
4. Wählen Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung **Aufzeichnungsrichtlinien**.
5. Wählen Sie im Menü **Neue Richtlinie hinzufügen**. Im linken Bereich wird eine **Neue Richtlinie** genannte Richtlinie angezeigt.
6. Klicken Sie mit der rechten Maustaste auf die neue Richtlinie und wählen Sie im Menü **Umbenennen**.
7. Geben Sie einen Namen für die Richtlinie ein, die Sie erstellen, und drücken Sie die **Eingabetaste** oder klicken Sie außerhalb des neuen Namens.
8. Klicken Sie mit der rechten Maustaste auf die Richtlinie und starten Sie durch Auswahl von **Neue Regel hinzufügen** den Assistenten für **Regeln**.
9. Folgen Sie den Anweisungen, um die Regeln für diese Richtlinie zu erstellen.

Ändern von Richtlinien

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf **OK**.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung **Aufzeichnungsrichtlinien**.
5. Wählen Sie die Richtlinie aus, die Sie ändern möchten. Die Regeln für die Richtlinie werden im rechten Bereich angezeigt.
6. Regel hinzufügen, ändern oder löschen:

    - Klicken Sie in der Menüleiste auf **Aktion** > **Neue Regel hinzufügen**. Wenn die Richtlinie aktiv ist, werden Sie in einem Popupfenster zum Bestätigen der Aktion aufgefordert. Erstellen Sie mit dem Assistenten für **Regeln** eine neue Regel.
    - Markieren Sie die Regel, die Sie ändern möchten, klicken Sie mit der rechten Maustaste und wählen Sie **Eigenschaften**. Ändern Sie die Regel mit dem Assistenten für **Regeln**.
    - Markieren Sie die Regel, die Sie löschen möchten, klicken Sie mit der rechten Maustaste und wählen Sie **Regel löschen**.

Löschen von Richtlinien

Hinweis: Eine Systemrichtlinie oder aktive Richtlinie kann nicht gelöscht werden.

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf **OK**.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung **Aufzeichnungsrichtlinien**.
5. Wählen Sie im linken Bereich die Richtlinie aus, die Sie löschen möchten. Wenn die Richtlinie aktiv ist, müssen Sie eine andere aktivieren.
6. Klicken Sie im Menü auf **Aktion** > **Richtlinie löschen**.
7. Klicken Sie auf **Ja**, um die Aktion zu bestätigen.

Hinweis: Einschränkung für vorab gestartete Anwendungssitzungen:

- Wenn die aktive Richtlinie versucht, einen Anwendungsnamen zuzuordnen, werden die in der vorab gestarteten Sitzung gestartete Anwendungen nicht zugeordnet, sodass die Sitzung nicht aufgezeichnet wird.
- Wenn die aktive Richtlinie jede Anwendung aufzeichnet und der Benutzer sich bei Citrix Receiver für Windows anmeldet (zur gleichen Zeit, zu der die vorab gestartete Sitzung eingerichtet wird), erscheint eine Aufzeichnungsbenachrichtigung und die leere Sitzung sowie alle darin ab diesem Zeitpunkt gestarteten Anwendungen werden aufgezeichnet.

Veröffentlichen Sie als Workaround Anwendungen gemäß ihrer Aufzeichnungsrichtlinien in separaten Bereitstellungsgruppen. Verwenden Sie keine Anwendungsnamen als Aufzeichnungsbedingung. Dadurch wird sichergestellt, dass vorab gestartete Sitzungen aufgezeichnet werden können. Benachrichtigungen werden jedoch weiterhin angezeigt.

Grundlegendes zu Rollover

Wenn Sie eine Richtlinie aktivieren, bleibt die vorher aktive Richtlinie bis zum Ende der Benutzersitzung in Kraft. In einigen Fällen wird die neue Richtlinie jedoch gültig, wenn ein Dateirollover erfolgt. Ein Dateirollover tritt auf, wenn die maximale Größe erreicht wird. Weitere Informationen zur maximalen Dateigröße für Aufzeichnungen finden Sie unter Angeben der Dateigröße für Aufzeichnungen.

In der folgenden Tabelle werden die Vorgänge beschrieben, die beim Anwenden einer neuen Richtlinie auftreten, während eine Sitzung aufgezeichnet wird und ein Rollover erfolgt:

Vorherige Richtlinie	Neue Richtlinie	Richtlinie nach Rollover
Nicht aufzeichnen	Jede andere Richtlinie	Keine Änderung. Die neue Richtlinie wird nur gültig, wenn sich der Benutzer an einer neuen Sitzung anmeldet.
Ohne Benachrichtigung aufzeichnen	Nicht aufzeichnen	Aufzeichnung wird gestoppt.
Ohne Benachrichtigung aufzeichnen	Mit Benachrichtigung aufzeichnen	Aufzeichnung wird fortgesetzt, und eine Benachrichtigung wird angezeigt.
Mit Benachrichtigung aufzeichnen	Nicht aufzeichnen	Aufzeichnung wird gestoppt.
Mit Benachrichtigung aufzeichnen	Ohne Benachrichtigung aufzeichnen	Aufzeichnung wird fortgesetzt. Bei der nächsten Anmeldung des Benutzers wird keine Meldung angezeigt.

Erstellen von Benachrichtigungen

February 22, 2019

Wenn in der aktiven Aufzeichnungsrichtlinie festgelegt ist, dass Benutzer über das Aufzeichnen der Sitzung benachrichtigt werden, wird ein Popupfenster mit einer Benachrichtigung angezeigt, nach dem die Benutzer die Anmeldeinformationen eingegeben haben. Die Standardbenachrichtigung lautet `"Your activity with one or more of the programs you recently started is being recorded. If you object to this condition, close the programs."`. Die Benutzer können auf **OK** klicken und die Sitzung fortsetzen.

Die Standardbenachrichtigung wird in der Sprache des Betriebssystems des Computers angezeigt, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.

Sie können benutzerdefinierte Benachrichtigungen in der gewünschten Sprache erstellen; jedoch ist nur eine Benachrichtigung pro Sprache möglich. Den Benutzern wird die Benachrichtigung in der Sprache der lokalen Einstellungen angezeigt.

Erstellen einer neuen Benachrichtigung

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.

2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Benachrichtigungen**.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie die Sprache für die Nachricht und geben Sie die neue Nachricht ein. Sie können nur eine Nachricht pro Sprache erstellen.

Nach der Annahme und Aktivierung wird die neue Benachrichtigung im Feld "Sprachspezifische Benachrichtigungen"angezeigt.

Hinweis: Die Administratorprotokollierung der Sitzungsaufzeichnung ermöglicht die Protokollierung von Änderungen an der Sitzungsaufzeichnungsserver-Richtlinie. Weitere Informationen finden Sie unter Protokollierte Verwaltungsaktivitäten.

Deaktivieren oder Aktivieren der Aufzeichnung

February 4, 2020

Der Sitzungsaufzeichnungsagent wird auf jedem Serverbetriebssystem-VDA installiert, auf dem Sie Sitzungen aufzeichnen möchten. Jeder Agent hat eine Einstellung, mit der die Aufzeichnungsfunktion auf dem Server aktiviert wird, auf dem die Agentsoftware installiert ist. Nach dem Aktivieren der Aufzeichnungsfunktion wertet die Sitzungsaufzeichnung die aktive Aufzeichnungsrichtlinie aus, mit der festgelegt wird, welche Sitzungen aufgezeichnet werden.

Bei Installation des Sitzungsaufzeichnungsagents ist die Aufzeichnungsfunktion aktiviert. Citrix empfiehlt, dass Sie die Sitzungsaufzeichnung auf Servern deaktivieren, für die kein Aufzeichnen vorgesehen ist, da die Anwendung die Serverleistung geringfügig beeinträchtigt, selbst wenn keine Aufzeichnung erfolgt.

Deaktivieren bzw. Aktivieren der Aufzeichnung auf einem Server

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Aktivieren oder deaktivieren Sie unter **Sitzungsaufzeichnung** das Kontrollkästchen **Sitzungsaufzeichnung für diese VDA-Maschine** aktivieren, um anzugeben, ob Sitzungen für den Server aufgezeichnet werden sollen.
4. Starten Sie auf Aufforderung den Sitzungsaufzeichnungsagent-Dienst neu, um die Änderung zu übernehmen.

Hinweis: Bei der Installation der Sitzungsaufzeichnung wird als aktive Richtlinie **Nicht aufzeichnen** (auf keinem Server werden Sitzungen aufgezeichnet) verwendet. Aktivieren Sie

in der Richtlinienkonsole für die Sitzungsaufzeichnung eine andere Richtlinie, um die Aufzeichnungsfunktion zu aktivieren.

Aktivieren der Aufzeichnung benutzerdefinierter Ereignisse

In der Sitzungsaufzeichnung können Sie mit Anwendungen von Drittanbietern benutzerdefinierte Daten, so genannte Ereignisse, in die Sitzungsaufzeichnungen einfügen. Diese Ereignisse werden angezeigt, wenn die Sitzung mit dem Sitzungsaufzeichnungsplayer wiedergegeben wird. Die Ereignisse sind Teil der Sitzungsaufzeichnungsdatei und können nach dem Aufzeichnen der Sitzung nicht geändert werden.

Ein Ereignis kann beispielsweise den folgenden Text enthalten: "Benutzer öffnete einen Browser". Jedes Mal, wenn ein Benutzer einen Browser in einer Sitzung öffnet, die aufgezeichnet wird, wird der Text zu diesem Zeitpunkt in die Aufzeichnung eingefügt. Wenn die Sitzung mit dem Sitzungsaufzeichnungsplayer wiedergegeben wird, kann der Benutzer die Anzahl der Marker in der Liste Ereignisse und Textmarken im Player notieren, und damit schnell die Stellen suchen und zählen, an denen der Benutzer einen Browser geöffnet hat.

Einfügen benutzerdefinierter Ereignisse in Aufzeichnungen auf einem Server

- Aktivieren Sie über die **Eigenschaften des Sitzungsaufzeichnungsagents** eine Einstellung auf jedem Server, auf dem Sie benutzerdefinierte Ereignisse einfügen möchten. Sie müssen jeden Server einzeln aktivieren. Das globale Aktivieren aller Server in einer Site ist nicht möglich.
- Entwickeln Sie Anwendungen, die auf der Event-API basieren, die in der XenApp-Sitzung jedes Benutzers ausgeführt werden (zum Einfügen der Daten in die Aufzeichnung).

Bei der Installation der Sitzungsaufzeichnung wird auch eine Ereignisaufzeichnungs-COM-Anwendung (API) installiert, mit der Sie Text von Anwendungen von Drittherstellern in die Aufzeichnung einfügen können. Sie können die API von vielen Programmiersprachen verwenden, u. a. Visual Basic, C++ oder C#. Weitere Informationen finden Sie im Citrix-Artikel CTX226844. Die DLL-Datei der Sitzungsaufzeichnungs-Event-API ist Teil der Installation der Sitzungsaufzeichnung. Die Datei ist unter C:\Programme\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll gespeichert.

Zum Aktivieren der Aufzeichnung von benutzerdefinierten Ereignissen auf einem Server führen Sie folgende Schritte aus:

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte **Aufzeichnung**.
4. Aktivieren Sie unter **Benutzerdefinierte Ereignisaufzeichnung** das Kontrollkästchen **Anwendungen von Drittherstellern können benutzerdefinierte Daten auf diesem Server aufzeichnen**.

Aktivieren und Deaktivieren von Livesitzungswiedergabe und Wiedergabeschutz

October 16, 2020

Aktivieren oder Deaktivieren der Wiedergabe von Livesitzungen

Mit dem Sitzungsaufzeichnungsplayer können Sie eine Sitzung nach oder während der Aufzeichnung anzeigen. Das Anzeigen einer Sitzung, die gerade aufgezeichnet wird, ähnelt dem Anzeigen von Live-Aktionen. Es gibt jedoch eine Verzögerung von ein oder zwei Sekunden, wenn die Daten vom XenApp- oder XenDesktop-Server übertragen werden.

Einige Funktionen stehen nicht zur Verfügung, wenn Sie Sitzungen anzeigen, deren Aufzeichnung noch nicht abgeschlossen ist:

- Eine digitale Signatur kann erst nach dem Abschluss der Aufzeichnung zugewiesen werden. Wenn die digitale Signatur aktiviert ist, können Sie Livesitzungen wiedergeben, die jedoch nicht signiert sind. Zertifikate können erst nach dem Abschluss der Aufzeichnung angezeigt werden.
- Der Wiedergabeschutz kann erst nach dem Abschluss der Aufzeichnung angewendet werden. Wenn der Wiedergabeschutz aktiviert ist, können Sie Livesitzungen wiedergeben, die jedoch erst nach dem Abschluss der Aufzeichnung verschlüsselt werden.
- Eine Datei kann erst nach dem Abschluss der Aufzeichnung zwischengespeichert werden.

In der Standardeinstellung ist die Wiedergabe von Livesitzungen aktiviert.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Wiedergabe**.
4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Wiedergabe von Livesitzungen zulassen**.

Aktivieren oder Deaktivieren des Wiedergabeschutzes

Als Sicherheitsmaßnahme werden Aufzeichnungsdateien, die zum Anzeigen im Sitzungsaufzeichnungsplayer heruntergeladen werden, automatisch von der Sitzungsaufzeichnung verschlüsselt. Dieser Wiedergabeschutz stellt sicher, dass die Dateien nur von dem Benutzer, der die Datei heruntergeladen hat, und nicht von anderen Benutzern kopiert oder angezeigt werden können. Die Wiedergabe der Dateien kann nicht auf einer anderen Arbeitsstation oder von einem anderen

Benutzer durchgeführt werden. Verschlüsselte Dateien haben die Erweiterung `.icle`. Unverschlüsselte Dateien haben die Erweiterung `.icl`. Die Dateien bleiben verschlüsselt, wenn sie unter `%localAppData%\Citrix\SessionRecording\Player\Cache` des Sitzungsaufzeichnungsplayers sind, bis ein autorisierter Benutzer sie öffnet.

Wir empfehlen, HTTPS für den Schutz der übermittelten Daten zu verwenden.

In der Standardeinstellung ist der Wiedergabeschutz aktiviert.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Wiedergabe**.
4. Aktivieren Sie das Kontrollkästchen **Für die Wiedergabe heruntergeladene Sitzungsaufzeichnungsdateien verschlüsseln** oder heben Sie die Markierung auf.

Aktivieren oder Deaktivieren der digitalen Signatur

August 23, 2019

Wenn Sie Zertifikate auf dem Computer installieren, auf dem die Komponenten der Sitzungsaufzeichnung installiert sind, können Sie die Sicherheit der Sitzungsaufzeichnungsbereitstellung erhöhen, indem Sie den Sitzungsaufzeichnungen digitale Signaturen zuweisen.

In der Standardeinstellung sind digitale Signaturen deaktiviert. Nachdem Sie das Zertifikat zum Signieren der Aufzeichnungen ausgewählt haben, gewährt die Sitzungsaufzeichnung Leseberechtigung für den Storage Manager-Dienst der Sitzungsaufzeichnung.

Aktivieren digitaler Signaturen

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Signieren**.
4. Navigieren Sie zu dem Zertifikat, das die sichere Kommunikation zwischen den Computern ermöglicht, auf denen die Sitzungsaufzeichnungskomponenten installiert sind.

Deaktivieren digitaler Signaturen

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.

2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Signieren**.
4. Klicken Sie auf **Entfernen**.

Angeben des Speicherorts für Aufzeichnungen

August 18, 2021

Geben Sie unter Sitzungsaufzeichnungsserver - Eigenschaften das Verzeichnis zum Speichern von Aufzeichnungen und Wiederherstellen archivierter Aufzeichnungen für die Wiedergabe an.

Hinweis: Archivieren oder stellen Sie gelöschte Dateien mit dem Befehl ICLDB wieder her.

Angeben von Verzeichnissen zum Speichern von Aufzeichnungen

In der Standardeinstellung werden Aufzeichnungen im Verzeichnis **Laufwerk:\SessionRecordings** des Computers mit dem Sitzungsaufzeichnungsserver gespeichert. Sie können das Verzeichnis ändern, in dem die Aufzeichnungen gespeichert werden, weitere Verzeichnisse hinzufügen, um die Last auf mehrere Volumes zu verteilen oder freien Speicherplatz zu nutzen. Mehrere Verzeichnisse in der Liste geben an, dass die Last der Aufzeichnungen auf mehrere Verzeichnisse verteilt wird. Sie können ein Verzeichnis mehrmals hinzufügen. Der Lastausgleich durchläuft alle Verzeichnisse.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Speicher**.
4. Verwenden Sie die Liste **Verzeichnisse für Dateispeicherung**, um die Verzeichnisse zu verwalten, in denen die Aufzeichnungen gespeichert werden.

Nach der Auswahl der Verzeichnisse erhalten die Dienste der Sitzungsaufzeichnung für die Verzeichnisse Vollzugriff.

Sie können die Verzeichnisse für die Dateispeicherung auf dem lokalen Datenträger, einem SAN-Volume oder an einem durch UNC-Pfad angegebenen Speicherort erstellen. Buchstaben zugeordneter Netzwerklaufwerke werden nicht unterstützt. Die Sitzungsaufzeichnung darf nicht zusammen mit NAS (Network-Attached Storage) verwendet werden, da schwere Leistungs- und Sicherheitsprobleme auftreten, die mit dem Schreiben von Aufzeichnungsdaten in ein Netzlaufwerk verbunden sind.

Angeben eines Verzeichnisses zum Wiederherstellen archivierter Aufzeichnungen für die Wiedergabe

In der Standardeinstellung werden archivierte Aufzeichnungen im Verzeichnis **Laufwerk:\SessionRecordingsRest** des Computers mit dem Sitzungsaufzeichnungsserver wiederhergestellt. Sie können das Verzeichnis ändern.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Speicher**.
4. Geben Sie im Feld **Wiederherstellungsverzeichnis für archivierte Dateien** das Verzeichnis zum Wiederherstellen archivierter Aufzeichnungen an.

Angeben der Dateigröße für Aufzeichnungen

November 29, 2018

Wenn die Größe der Aufzeichnungsdateien zunimmt, kann der Download kann länger dauern und die Reaktionszeit kann sich verlangsamen, wenn Sie mit dem Schieberegler durch die Wiedergabe navigieren. Sie können die Dateigröße durch Festlegen eines Schwellenwerts für eine Datei steuern. Wenn die Aufzeichnung dieses Limit erreicht, schließt die Sitzungsaufzeichnung die Datei und öffnet eine neue, um die Aufzeichnung fortzusetzen. Dies wird Rollover genannt.

Wichtig: Die Rollovereinstellung gilt nicht für VDI-Desktopsitzungen für XenDesktop 7.8 und den Sitzungsaufzeichnungsagent. Hier hat jede Aufzeichnungsdatei eine maximale Größe von 1 GB. Nach Erreichen dieses Limits werden Vorgänge nicht weiter aufgezeichnet.

Sie können zwei Schwellenwerte für ein Rollover angeben:

- **Dateigröße:** Wenn die Größe der Datei die angegebene Zahl Megabytes erreicht, schließt die Sitzungsaufzeichnung die Datei und öffnet eine neue. In der Standardeinstellung wird ein Dateirollover durchgeführt, wenn die Dateigröße 50 Megabytes erreicht. Sie können jedoch ein Limit von 10 Megabytes bis zu 1 Gigabyte festlegen.
- **Dauer:** Wenn die Sitzung für die angegebene Anzahl der Stunden aufgezeichnet wurde, wird die Datei geschlossen und eine neue Datei wird geöffnet. In der Standardeinstellung wird ein Dateirollover durchgeführt, wenn die Sitzung für 12 Stunden aufgezeichnet wurde. Sie können jedoch ein Limit von einer bis zu 24 Stunden festlegen.

Die Sitzungsaufzeichnung prüft beide Felder und ermittelt, welches Ereignis zuerst auftritt, und legt dann den Rollover fest. Beispiel: Wenn Sie 17 MB für die Dateigröße und sechs Stunden für die Dauer

eingeben, und die Aufzeichnung erreicht 17 MB nach drei Stunden, reagiert die Sitzungsaufzeichnung auf die Dateigröße von 17 MB, schließt die Datei und öffnet eine neue.

Unabhängig vom eingegebenen Wert für die Dateigröße führt die Sitzungsaufzeichnung ein Rollover frühestens nach einer Stunde durch (dies ist der Mindestwert, den Sie eingeben können), um das Erstellen von zu vielen kleinen Dateien zu vermeiden. Diese Regel gilt nicht, wenn die Dateigröße über ein Gigabyte ansteigt.

Angeben der maximalen Dateigröße für Aufzeichnungen

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Rollover**.
4. Geben Sie ein Ganzzahl zwischen 10 und 1024 ein, mit der Sie die maximale Dateigröße in Megabyte angeben.
5. Geben Sie ein Ganzzahl zwischen 1 und 24 ein, mit der Sie die maximale Aufzeichnungslänge in Stunden angeben.

Protokollierte Verwaltungsaktivitäten

August 18, 2021

Die Administratorprotokollierung der Sitzungsaufzeichnung erfasst die folgenden Aktivitäten:

- Änderungen an Aufzeichnungsrichtlinien, die in der Richtlinienkonsole für die Sitzungsaufzeichnung oder in Citrix Director vorgenommen werden
- Änderungen an Eigenschaften des Sitzungsaufzeichnungsservers
- Downloads von Aufzeichnungen im Sitzungsaufzeichnungsplayer
- Aufzeichnung einer Sitzung durch die Sitzungsaufzeichnung nach einer Richtlinienabfrage
- Nicht autorisierte Zugriffsversuche auf die Administratorprotokollierung

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des

> Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Deaktivieren oder Aktivieren der Administratorprotokollierung

Nach der Installation können Sie die Administratorprotokollierung der Sitzungsaufzeichnung in den Eigenschaften des Sitzungsaufzeichnungsservers deaktivieren oder aktivieren.

1. Melden Sie sich als Administrator bei dem Server an, auf dem die Administratorprotokollierung für die Sitzungsaufzeichnung installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Protokollierung**.

Wenn Sie die Administratorprotokollierung deaktivieren, werden keine neuen Aktivitäten protokolliert. Sie können die vorhandenen Protokolle über die webbasierte Oberfläche abfragen.

Wenn die **obligatorische Sperrung** aktiviert ist, werden die folgenden Aktivitäten blockiert, wenn die Protokollierung fehlschlägt. Außerdem wird ein Systemereignis mit der Ereignis-ID 6001 protokolliert:

- Änderungen an Aufzeichnungsrichtlinien, die in der Richtlinienkonsole für die Sitzungsaufzeichnung oder in Citrix Director vorgenommen werden
- Änderungen an Eigenschaften des Sitzungsaufzeichnungsservers

Die Aufzeichnung von Sitzungen ist von der Einstellung der verbindlichen Sperrung nicht betroffen.

Gewähren von Zugriffsrechten für Benutzer

Aus Sicherheitsgründen sollten Sie den Benutzern nur die Rechte geben, die sie zum Ausführen bestimmter Funktionen, z. B. die Abfrage von Administratorprotokollen, benötigen.

Zum Zuweisen von Berechtigungen weisen Sie Benutzern in der Sitzungsaufzeichnungsautorisierungskonsole auf dem Sitzungsaufzeichnungsserver Rollen zu. Für die Administratorprotokollierung gibt es zwei Rollen:

- **LoggingWriter**. Hat Berechtigung zum Schreiben von Administratorprotokollen. Standardmäßig sind lokale Administratoren und der Netzwerkdienst Mitglied dieser Rolle.

  Hinweis: Eine Änderung der Standardmitglieder der Rolle **LoggingWriter** kann dazu führen, dass das Schreiben des Protokolls fehlschlägt.

- **LoggingReader**. Hat Berechtigung zum Abfragen von Administratorprotokollen. Für diese Rolle besteht keine Standardeinstellung.

Zuweisen von Rollen zu Benutzern

1. Melden Sie sich als Administrator bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Starten Sie die **Sitzungsaufzeichnungsautorisierungskonsole**.
3. Wählen Sie die Rolle, der Sie Benutzer zuweisen möchten.
4. Wählen Sie auf der Menüleiste **Aktion** > **Windows-Benutzer und -Gruppen zuweisen**.
5. Fügen Sie Benutzer und Gruppen hinzu.

In der Konsole vorgenommene Änderungen werden beim Update (das jede Minute erfolgt) übernommen.

Konfigurieren eines Dienstkontos für die Administratorprotokollierung

In der Standardeinstellung wird die Administratorprotokollierung als Webanwendung mit der Identität "Netzwerkdienst"in IIS ausgeführt. Zur Erhöhung der Sicherheit können Sie die Identität der Webanwendung in ein Dienstkonto oder ein bestimmtes Domänenkonto ändern.

1. Melden Sie sich als Administrator bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im IIS-Manager auf **Anwendungspools**.
3. Klicken Sie unter **Anwendungspools** mit der rechten Maustaste auf **SessionRecordingLoggingAppPool** und wählen Sie **Erweiterte Einstellungen**.
4. Ändern Sie das Attribut **Identität** unter Auswahl des gewünschten Kontos.
5. Erteilen Sie dem Konto die Berechtigung **db_owner** für die Datenbank **CitrixSessionRecordingLogging** in Microsoft SQL Server.
6. Erteilen Sie dem Konto Leseberechtigung für den Registrierungsschlüssel **HKEY_LOCAL_MACHINE\SOFTWA**

Deaktivieren oder Aktivieren der Protokollierung von Aufzeichnungsaktivitäten

Standardmäßig erfasst die Administratorprotokollierung nach Abschluss der Richtlinienabfrage alle Aufzeichnungsaktionen. Dabei können große Datenmengen entstehen. Zum Verbessern der Leistung und Einsparen von Speicherplatz deaktivieren Sie diese Art von Protokollierung in der Registrierung.

1. Melden Sie sich als Administrator bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Öffnen Sie den Registrierungs-Editor.
3. Gehen Sie zu **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.
4. Legen Sie für **EnableRecordingActionLogging** folgenden Wert fest:

   0 zum Deaktivieren der Protokollierung von Aufzeichnungsaktivitäten

   1 zum Aktivieren der Protokollierung von Aufzeichnungsaktivitäten

Abfragen des Administratorprotokolls

Die Sitzungsaufzeichnung bietet eine webbasierte Oberfläche zum Abfragen des Administratorprotokolls.

Führen Sie auf dem Computer mit dem Sitzungsaufzeichnungsserver folgende Schritte aus:

1. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnung - Administratorprotokollierung**.
2. Geben Sie die Anmeldeinformationen eines **LoggingReader**-Benutzers ein.

Führen Sie bei Verwendung eines anderen Computers folgende Schritte aus:

1. Öffnen Sie einen Webbrowser und rufen Sie die Webseite der Administratorprotokollierung auf.

   HTTPS: `https://servername/SessionRecordingLoggingWebApplication/`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.

   HTTP: `http://servername/SessionRecordingLoggingWebApplication/`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.

2. Geben Sie die Anmeldeinformationen eines **LoggingReader**-Benutzers ein.

Installieren der Sitzungsaufzeichnung mit hoher Datenbankverfügbarkeit

April 1, 2021

Die Sitzungsaufzeichnung unterstützt die folgenden Lösungen für hohe Datenbankverfügbarkeit basierend auf Microsoft SQL Server. Fällt die Hardware oder Software eines wichtigen oder primären SQL Server-Computers aus, kann durch einen automatischen Failover der Datenbanken sicherstellt werden, dass die Sitzungsaufzeichnung weiterhin ordnungsgemäß funktioniert.

- AlwaysOn-Verfügbarkeitsgruppen

AlwaysOn-Verfügbarkeitsgruppen sind eine Lösung für hohe Verfügbarkeit und Wiederherstellung im Notfall, die eine für Unternehmen geeignete Alternative zur Datenbankspiegelung darstellt. AlwaysOn-Verfügbarkeitsgruppen wurden mit SQL Server 2012 eingeführt und maximieren die Verfügbarkeit diverser Benutzerdatenbanken für Unternehmen. AlwaysOn-Verfügbarkeitsgruppen erfordern, dass die SQL Server-Instanzen auf den Windows Server Failover Clustering-Knoten (WSFC) residieren. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server.

- SQL Server-Clustering

Bei dieser Technologie von Microsoft kann ein Server automatisch die Aufgaben und Verantwortlichkeiten eines anderen, fehlgeschlagenen Servers übernehmen. Es ist jedoch komplizierter, diese Lösung einzurichten. Zudem ist das automatische Failover in der Regel langsamer als bei anderen Lösungen (etwa der Spiegelung der SQL Server-Datenbank). Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/sql/sql-server/failover-clusters/windows/always-on-failover-cluster-instances-sql-server.

- SQL Server-Datenbankspiegelung

Die Datenbankspiegelung gewährleistet, dass bei einem Ausfall des aktiven Datenbankservers innerhalb von Sekunden ein automatischer Failover erfolgt. Diese Lösung ist teurer als die anderen beiden Lösungen, da auf jedem Datenbankserver eine vollständige SQL Server-Lizenz vorliegen muss. Die SQL Server Express Edition kann in einer gespiegelten Umgebung nicht verwendet werden. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/sql/database-engine/database-mirroring/database-mirroring-sql-server.

Installieren der Sitzungsaufzeichnung mit hoher Datenbankverfügbarkeit

Installieren der Sitzungsaufzeichnung mit hoher Datenbankverfügbarkeit

- Installieren Sie zuerst die Komponenten des Sitzungsaufzeichnungsservers und konfigurieren Sie anschließend die hohe Datenbankverfügbarkeit für die erstellten Datenbanken.
  Sie können die Komponenten der Sitzungsaufzeichnungsverwaltung mit Datenbanken installieren, die zur Installation auf der vorbereiteten SQL Server-Instanz konfiguriert sind, und dann die hohe Verfügbarkeit für die erstellten Datenbanken konfigurieren.
  - Für AlwaysOn-Verfügbarkeitsgruppen und Clustering müssen Sie in HKEY_LOCAL_MACHINE\SOFTWARE den Namen der SQL Server-Instanz manuell in den Namen des Verfügbarkeitsgruppen-Listeners oder des SQL Server-Netzwerks ändern.
  - Für die Datenbankspiegelung müssen Sie die Failoverpartner für die Datenbanken in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner und HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner manuell hinzufügen.
- Konfigurieren Sie zunächst die hohe Verfügbarkeit für leere Datenbanken und installieren Sie dann die Komponenten der Sitzungsaufzeichnungsverwaltung.
  Sie können zwei leere Datenbanken als Datenbank für die Sitzungsaufzeichnung und als Datenbank für die Konfigurationsprotokollierung auf der künftigen primären SQL Server-Instanz erstellen und hohe Verfügbarkeit konfigurieren. Geben Sie dann den Namen der SQL Server-Instanz bei der Installation der Komponenten des Sitzungsaufzeichnungsservers an:

- Zur Verwendung von AlwaysOn-Verfügbarkeitsgruppen geben Sie den Namen des Verfügbarkeitsgruppen-Listeners an.
- Zur Verwendung der Datenbankspiegelung geben Sie den Namen des primären SQL Server-Computers ein.
- Zur Verwendung der Clusterlösung geben Sie den Netzwerknamen des SQL Server-Computers ein.

Anzeigen von Aufzeichnungen

November 29, 2018

Mit dem Sitzungsaufzeichnungsplayer zeigen Sie aufgezeichnete XenApp- bzw. XenDesktop-Sitzungen an, suchen die Sitzungsaufzeichnungsdateien und fügen Textmarken hinzu.

Wenn Sitzungen mit aktiviertem Liveplayback aufgezeichnet werden, können Sie aktuell ausgeführte Sitzungen mit einer Verzögerung von ein paar Minuten und abgeschlossene Sitzungen anzeigen.

Sitzungen, die länger als die vom Sitzungsaufzeichnungsadministrator festgelegten Höchstwerte sind oder deren Dateigröße das Limit übersteigt, werden in mehreren Sitzungsdateien aufgezeichnet.

Hinweis: Ein Sitzungsaufzeichnungsadministrator muss Benutzern Berechtigung für den Zugriff auf aufgezeichnete Serverbetriebssystemmaschinen-Sitzungen erteilen. Wenden Sie sich an den Sitzungsaufzeichnungsadministrator, wenn Sie nicht auf Sitzungsaufzeichnungen zugreifen können.

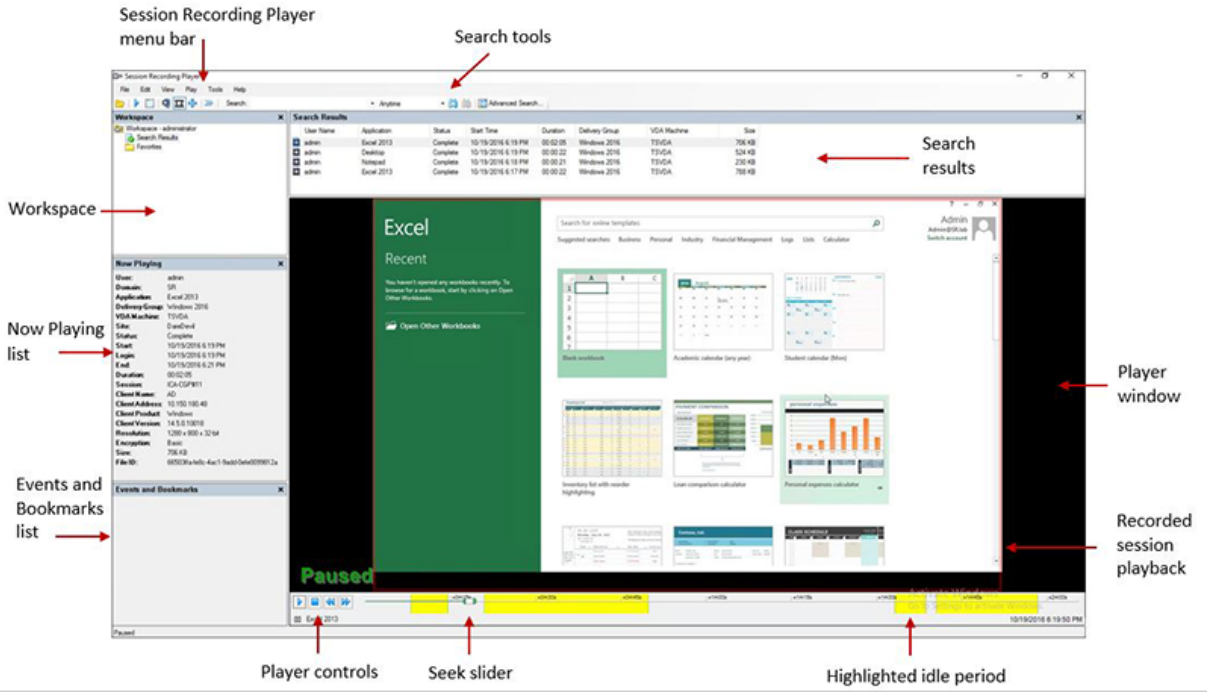
Bei der Installation des Sitzungsaufzeichnungsplayers richtet der Administrator normalerweise die Verbindung zwischen dem Player und einem Sitzungsaufzeichnungsserver ein. Wenn die Verbindung nicht eingerichtet ist, müssen Sie die Verbindung beim ersten Suchen nach Dateien angeben. Weitere Informationen zum Einrichten der Verbindung erhalten Sie vom Sitzungsaufzeichnungsadministrator.

Starten des Sitzungsaufzeichnungsplayers

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.

   Der Sitzungsaufzeichnungsplayer wird angezeigt.

Diese Abbildung zeigt den Sitzungsaufzeichnungsplayer mit Beschriftung der Hauptelemente. Die Funktion dieser Elemente wird in den folgenden Artikeln beschrieben.



Ausblenden oder Einblenden der Fensterelemente

Der Sitzungsaufzeichnungsplayer hat Fensterelemente, die Sie ein- und ausblenden können.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste auf **Ansicht**.
4. Wählen Sie die Elemente aus, die Sie anzeigen möchten. Bei der Auswahl eines Elements wird es sofort angezeigt. Ein Häkchen gibt die Auswahl des Elements an.

Wechseln des Sitzungsaufzeichnungsservers

Wenn der Administrator eine Verbindung mit mehreren Sitzungsaufzeichnungsservern im Sitzungsaufzeichnungsplayer ermöglicht hat, können Sie den Server wählen, mit dem der Player eine Verbindung herstellen soll. Der Sitzungsaufzeichnungsplayer kann nur jeweils eine Verbindung mit einem Sitzungsaufzeichnungsserver herstellen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras** > **Optionen** > **Verbindungen**.

4. Wählen Sie den Sitzungsaufzeichnungsserver aus, mit dem Sie eine Verbindung herstellen möchten.

Öffnen und Wiedergeben von Aufzeichnungen

August 18, 2021

Sie öffnen Sitzungsaufzeichnungen im Sitzungsaufzeichnungsplayer auf dreierlei Weise:

- Führen Sie eine Suche mit dem Sitzungsaufzeichnungsplayer durch. Sitzungsaufzeichnungen, die die Suchkriterien erfüllen, werden im Bereich der Suchergebnisse angezeigt.
- Greifen Sie auf Sitzungsaufzeichnungsdateien direkt von der lokalen Festplatte oder einem freigegebenen Laufwerk zu.
- Greifen Sie auf Sitzungsaufzeichnungsdateien vom Ordner “Favoriten”zu

Beim Öffnen einer Datei, die ohne digitale Signatur aufgezeichnet wurde, werden Sie in einer Warnmeldung darauf hingewiesen, dass Ursprung und Integrität der Datei nicht geprüft werden konnten. Bestätigen Sie die Warnmeldung mit **Ja** und öffnen Sie die Datei, wenn Sie hinsichtlich der Integrität der Datei keine Bedenken haben.

Hinweis: Die Administratorprotokollierung der Sitzungsaufzeichnung ermöglicht die Protokollierung der Downloads von Sitzungsaufzeichnungen im Sitzungsaufzeichnungsplayer. Weitere Informationen finden Sie unter Protokollierte Verwaltungsaktivitäten.

Öffnen und Wiedergeben einer Aufzeichnung im Bereich der Suchergebnisse

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Führen Sie eine Schnellsuche durch.
4. Wenn der Bereich mit den Suchergebnissen nicht sichtbar ist, wählen Sie **Suchergebnisse** im Arbeitsbereich.
5. Wählen Sie im Suchergebnisbereich die Sitzung aus, die Sie wiedergeben möchten.
6. Führen Sie einen der folgenden Schritte aus:

    - Doppelklicken Sie auf die Sitzung.
    - Klicken Sie mit der rechten Maustaste und wählen Sie **Wiedergeben**.
    - Klicken Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste auf **Wiedergabe** > **Wiedergabe**.

Öffnen und Wiedergeben einer Aufzeichnung durch Zugriff auf die Datei

Der Name von Sitzungsaufzeichnungsdateien beginnt mit "i_"gefolgt von einer eindeutigen alphanumerischen Datei-ID und der Dateierweiterung ".icl"oder ".icle". "icl"steht für Aufzeichnungen ohne Wiedergabeschutz und "icle"für solche mit Wiedergabeschutz. Sitzungsaufzeichnungsdateien werden in einem Ordner gespeichert, der das Datum der Sitzungsaufzeichnung enthält. Beispiel: Die Datei für eine Sitzung, die am 22. Dezember 2014 aufgezeichnet wurde, wird im Ordnerpfad 2014\12\22 gespeichert.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste **Datei** > **Öffnen** und navigieren Sie zu der Datei.
    - Navigieren Sie mit dem Windows-Explorer auf die Datei und ziehen Sie sie in das **Player**-Fenster.
    - Navigieren Sie mit dem Windows-Explorer auf die Datei und doppelklicken Sie.
    - Wenn Sie Favoriten im Arbeitsbereich erstellt haben, wählen Sie **Favoriten** und öffnen Sie die Datei im Favoritenbereich auf die gleiche Weise wie Dateien im Suchergebnisbereich.

Verwenden von Favoriten

Das Erstellen von Favoriten-Ordnern ermöglicht den schnellen Zugriff auf oft angezeigte Sitzungsaufzeichnungen. Diese Favoritenordner verweisen auf Sitzungsaufzeichnungsdateien, die auf der Arbeitsstation oder auf einem Netzwerklaufwerk gespeichert sind. Sie können diese Dateien von anderen Arbeitsstationen importieren, zu anderen exportieren und die Ordner für andere Sitzungsaufzeichnungsplayer-Benutzer freigeben.

Hinweis: Nur Benutzer mit Zugriffsrechten für den Sitzungsaufzeichnungsplayer können die Sitzungsaufzeichnungsdateien herunterladen, die dem Favoritenordner zugeordnet sind. Wenden Sie sich bezüglich Zugriffsrechten an den Sitzungsaufzeichnungsadministrator.

Erstellen eines Favoriten-Unterordners

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Wählen Sie im **Sitzungsaufzeichnungsplayer** den Ordner **Favoriten** im Bereich "Arbeitsbereich".
4. Klicken Sie auf der Menüleiste auf **Datei** > **Ordner** > **Neuer Ordner**. Ein neuer Ordner wird unter dem Ordner **Favoriten** angezeigt.

5. Geben Sie den Ordnernamen ein und drücken Sie die **Eingabetaste** oder klicken Sie auf eine beliebige Stelle, um den neuen Namen zu übernehmen.

Mit den anderen Optionen im Menü **Datei** > **Ordner** können Sie die Ordner löschen, umbenennen, verschieben, kopieren, importieren und exportieren.

Wiedergeben aufgezeichneter Sitzungen

October 30, 2019

Nach dem Öffnen einer aufgezeichneten Sitzung im Sitzungsaufzeichnungsplayer können Sie in der Aufzeichnung folgendermaßen navigieren:

- Mit den Player-Bedienelementen können Sie die Aufzeichnung wiedergeben, anhalten oder stoppen und die Wiedergabegeschwindigkeit erhöhen oder verringern.
- Mit dem Schieberegler für das Positionieren gehen Sie vorwärts oder rückwärts.

Wenn Sie Marker in die Aufzeichnung eingefügt haben, oder die aufgezeichnete Sitzung benutzerdefinierte Ereignisse enthält, können Sie mit diesen Markern oder Ereignissen durch die Sitzungsaufzeichnung navigieren.

Hinweis:

- Bei der Wiedergabe einer aufgezeichneten Sitzung wird möglicherweise ein zweiter Mauszeiger angezeigt. Der zweite Mauszeiger wird an der Stelle in der Aufzeichnung angezeigt, an der der Benutzer in Internet Explorer navigiert und auf ein Bild geklickt hat, das im Original größer als der Bildschirm war, das jedoch von Internet Explorer automatisch skaliert wurde. While only one pointer appears during the session, two might appear during playback.
- Diese Version der Sitzungsaufzeichnung unterstützt weder die SpeedScreen-Multimediabeschleunigung für XenApp noch die Richtlinieneinstellung zum Optimieren der Flash-Inhalte für XenApp. Wenn diese Option aktiviert ist, wird bei der Wiedergabe ein schwarzes Rechteck angezeigt.
- Die Sitzungsaufzeichnung kann keine Lync-Webcamvideos aufzeichnen, wenn das HDX RealTime Optimization Pack verwendet wird.
- Beim Aufzeichnen einer Sitzung mit einer Auflösung über 4096 x 4096 ist die Aufzeichnungsanzeige u. U. fragmentiert.
- Sie können Windows 7-Desktop-Sitzungen nicht ordnungsgemäß aufzeichnen, wenn über die XenDesktop-Siterichtlinie **Legacygrafikmodus** und über die Citrix Receiver für Windows-Richtlinie die **datenträgerbasierte Zwischenspeicherung** aktiviert sind. Die Aufzeichnungen erscheinen als schwarzer Bildschirm.
  Deaktivieren Sie als Workaround die **datenträgerbasierte Zwischenspeicherung** durch Bereitstellung mit einem Gruppenrichtlinienobjekt auf den Maschinen, auf denen Citrix Receiver für

Windows installiert ist. Weitere Informationen zur Deaktivierung der **datenträgerbasierten Zwischenspeicherung** finden Sie unter CTX123169.

- Die Sitzungsaufzeichnung unterstützt den Framehawk-Anzeigemodus nicht. Sitzungen im Framehawk-Anzeigemodus können nicht aufgezeichnet und einwandfrei wiedergegeben werden. Im Framehawk-Modus aufgezeichnete Sitzungen enthalten ggf. keine Sitzungsaktivitäten.

Verwenden der Player-Bedienelemente

Sie können auf die Player-Bedienelemente unten im Player-Fenster klicken oder im **Sitzungsaufzeichnungsplayer**-Menü auf **Wiedergabe** klicken. Die Player-Bedienelemente ermöglichen Folgendes:

Player-Bedienelement	Funktion
	Wiedergeben der ausgewählten Sitzungsdatei.
	Anhalten der Wiedergabe.
	Stoppen der Wiedergabe. Wenn Sie auf **Stopp** und dann auf **Wiedergabe** klicken, springt die Wiedergabe wieder an den Anfang der Datei.
	Halbieren der momentanen Wiedergabegeschwindigkeit um die Hälfte auf mindestens ein Viertel der Normalgeschwindigkeit.
	Verdoppeln der momentanen Wiedergabegeschwindigkeit auf maximal das 32-fache der Normalgeschwindigkeit.

Verwenden des Schiebereglers für das Positionieren

Mit dem Schieberegler für das Positionieren unten im Player-Fenster springen Sie auf eine andere Stelle in der aufgezeichneten Sitzung. Sie können den Schieberegler für das Positionieren auf eine Stelle in der Aufzeichnung ziehen, die Sie anzeigen möchten, oder auf eine Stelle auf dem Schieberegler klicken, um auf diese Stelle zu gehen.

Sie können den Schieberegler für das Positionieren auch mit den folgenden Tasten auf der Tastatur steuern:

Key	Positionieren
Pos1	An den Anfang positionieren.
Ende	An das Ende positionieren.
Nach-Rechts-Taste	Fünf Sekunden vorwärts positionieren.
Nach-Links-Taste	Fünf Sekunden rückwärts positionieren.
Verschieben des Mausrads um einen Anschlag nach unten	15 Sekunden vorwärts positionieren.
Verschieben des Mausrads um einen Anschlag nach oben	15 Sekunden rückwärts positionieren.
Strg + Nach-Rechts-Taste	30 Sekunden vorwärts positionieren.
Strg + Nach-Links-Taste	30 Sekunden rückwärts positionieren.
Bild ab	Eine Minute vorwärts positionieren.
Bild auf	Eine Minute rückwärts positionieren.
Strg + Mausrad einen Klick nach unten bewegen.	90 Sekunden vorwärts positionieren.
Strg + Mausrad einen Klick nach oben bewegen	90 Sekunden rückwärts positionieren.
Strg + Bild-Ab	Sechs Minuten vorwärts positionieren.
Strg + Bild-Auf	Sechs Minuten rückwärts positionieren.

Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Extras** > **Optionen** > **Player** und verschieben Sie den Schieberegler, um die Reaktionszeit des Schiebereglers zu verlängern oder zu verkürzen. Für eine schnellere Reaktionszeit wird mehr Speicher benötigt. Die Reaktion kann, abhängig von der Größe der Aufzeichnungen und der Computerhardware, langsam sein.

Ändern der Wiedergabegeschwindigkeit

Sie können die Wiedergabe aufgezeichneter Sitzungen im Sitzungsaufzeichnungsplayer in exponentiellen Erhöhungen von einem Viertel der normalen Wiedergabegeschwindigkeit bis zum 32-fachen der normalen Wiedergabegeschwindigkeit einstellen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste auf **Wiedergabe** > **Wiedergabegeschwindigkeit**.
4. Wählen Sie eine Geschwindigkeitsoption.

Die Geschwindigkeit wird sofort geändert. Eine Zahl gibt die erhöhte oder verringerte Wiedergabegeschwindigkeit unter den Bedienelementen im Player-Fenster an. Text, der die exponentielle Rate angibt, wird kurz in grün im Player-Fenster angezeigt.

Hervorheben von Leerlaufperioden in aufgezeichneten Sitzungen

Leerlaufperioden sind die Teile einer aufgezeichneten Sitzung, in denen keine Aktion stattfindet. Der Sitzungsaufzeichnungsplayer kann Leerlaufperioden aufgezeichneter Sitzungen bei der Wiedergabe hervorheben. Die Standardeinstellung ist **Ein**.

Bei der Wiedergabe aktiver Sitzungen werden Leerlaufperioden nicht hervorgehoben.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie in der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Ansicht** > **Leerlauf** und aktivieren oder deaktivieren Sie die Option.

Überspringen von Stellen ohne Aktionen

Im Schnellprüfmodus überspringt der Sitzungsaufzeichnungsplayer die Teile von aufgezeichneten Sitzungen, in denen keine Aktion stattfindet. Mit dieser Einstellung sparen Sie Zeit bei der Wiedergabe, animierte Folgen werden jedoch nicht übersprungen, z. B. ein animierter Mauszeiger, blinkende Cursor oder angezeigte Uhren, bei denen sich die zweite Hand bewegt.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Wiedergabe** > **Schnellprüfmodus**.

Sie können die Option aktivieren oder deaktivieren. Bei jeder Auswahl wird der Status kurz in grün im Player -Fenster angezeigt.

Verwenden von Ereignissen und Textmarken

November 29, 2018

Ereignisse und Textmarken erleichtern das Navigieren in aufgezeichneten Sitzungen.

Ereignisse werden bei der Aufzeichnung mit der Ereignis-API oder einer Anwendung eines Drittherstellers in die Sitzungen eingefügt. Ereignisse werden als Teil der Sitzungsdatei gespeichert. Sie können mit dem Sitzungsaufzeichnungsplayer nicht gelöscht oder geändert werden.

Textmarken sind Marker, die Sie während der Sitzungswiedergabe mit dem Sitzungsaufzeichnungsplayer in Sitzungsaufzeichnungen einfügen. Textmarken werden der aufgezeichneten Sitzung zugeordnet, bis sie gelöscht werden, sie werden jedoch nicht mit der Sitzungsdatei gespeichert. Textmarken werden als eigene ICLB-Datei im Cacheordner **Bookmarks** auf dem Sitzungsaufzeichnungsplayer gespeichert (Beispiel: C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookma
Der Name ist mit dem der ICL-Datei (Aufzeichnungsdatei) identisch. Wenn Sie eine Aufzeichnungsdatei mit Textmarken auf einem anderen Player wiedergeben möchten, kopieren Sie die ICLB-Dateien in den Cacheordner **Bookmarks** auf dem betreffenden Player. In der Standardeinstellung ist jede Textmarke mit "Textmarke"beschriftet. Sie können diese Beschriftung beliebig ändern und maximal 128 Zeichen eingeben.

Ereignisse und Textmarken werden als Punkte unten im Player-Fenster angezeigt. Ereignisse werden als gelbe Punkte und Textmarken als blaue Punkte angezeigt. Wenn Sie die Maus auf diese Punkte verschieben, wird der zugeordnete Text angezeigt. Sie können die Ereignisse und Textmarken auch in der Liste **Ereignisse und Textmarken** im Sitzungsaufzeichnungsplayer anzeigen. Sie werden in dieser Liste in chronologischer Reihenfolge mit den Textbeschriftungen und den Uhrzeiten angezeigt, zu denen sie in der aufgezeichneten Sitzung erscheinen.

Ereignisse und Textmarken erleichtern das Navigieren in aufgezeichneten Sitzungen. Wenn Sie auf ein Ereignis oder eine Textmarke gehen, springen Sie auf die Stelle in der aufgezeichneten Sitzung, an der das Ereignis oder die Textmarke eingefügt ist.

Anzeigen von Ereignissen und Textmarken in der Liste

In der Liste **Ereignisse und Textmarken** werden die Ereignisse und Textmarken angezeigt, die in der momentan wiedergegebenen Sitzungsaufzeichnung eingefügt sind. Sie können in der Liste nur Ereignisse, nur Textmarken oder Ereignisse und Textmarken anzeigen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Verschieben Sie den Mauszeiger auf die Liste **Ereignisse und Textmarken** und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
4. Wählen Sie **Nur Ereignisse anzeigen**, **Nur Textmarken anzeigen** oder **Alle anzeigen**.

Einfügen einer Textmarke

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Beginnen Sie mit der Wiedergabe der aufgezeichneten Sitzung, der Sie eine Textmarke hinzufügen möchten.
4. Schieben Sie den Schieberegler für das Positionieren auf die Stelle, an der Sie die Textmarke einfügen möchten.
5. Schieben Sie den Mauszeiger in den Player-Fensterbereich und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Fügen Sie eine Textmarke mit der Standardbeschriftung **Textmarke** hinzu oder erstellen Sie eine Anmerkung:

    - Zum Hinzufügen einer Textmarke mit der Standardbeschriftung **Textmarke** wählen Sie **Textmarke hinzufügen**.
    - Um eine Textmarke mit einer von Ihnen erstellten Beschriftung hinzuzufügen, wählen Sie **Anmerkung hinzufügen**. Geben Sie die Anmerkung (max. 128 Zeichen) ein, die Sie der Textmarke zuordnen möchten. Klicken Sie auf **OK**.

Hinzufügen oder Ändern einer Anmerkung

Nach dem Erstellen einer Textmarke können Sie eine Anmerkung hinzufügen oder eine bestehende Anmerkung ändern.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Beginnen Sie mit der Wiedergabe der aufgezeichneten Sitzung, die eine Textmarke hat.
4. Stellen Sie sicher, dass in der Liste "Ereignisse und Textmarken"Textmarken angezeigt werden.
5. Wählen Sie die Textmarke aus der Liste **Ereignisse und Textmarken** aus und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Wählen Sie **Anmerkung bearbeiten**.
7. Geben Sie im angezeigten Fenster die neue Anmerkung ein und klicken Sie auf **OK**.

Löschen einer Textmarke

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.

3. Beginnen Sie mit der Wiedergabe der aufgezeichneten Sitzung, die eine Textmarke hat.
4. Stellen Sie sicher, dass in der Liste "Ereignisse und Textmarken"Textmarken angezeigt werden.
5. Klicken Sie mit der rechten Maustaste auf die Textmarke in der Liste "Ereignisse und Textmarken", um das Menü anzuzeigen.
6. Wählen Sie **Löschen**.

Gehen auf ein Ereignis oder eine Textmarke

Wenn Sie auf ein Ereignis oder eine Textmarke gehen, springt der Sitzungsaufzeichnungsplayer an die Stelle in der Sitzungsaufzeichnung, an der das Ereignis oder die Textmarke eingefügt ist.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Beginnen Sie mit der Wiedergabe einer Sitzungsaufzeichnung mit Ereignissen oder Textmarken.
4. Gehen Sie auf ein Ereignis oder eine Textmarke.

    - Klicken Sie unten im Player-Fenster auf den Punkt, der das Ereignis oder die Textmarke darstellt, um auf das Ereignis oder die Textmarke zu gehen.
    - Doppelklicken Sie in der Liste **Ereignisse und Textmarken** auf ein Ereignis oder eine Textmarke, um an die entsprechende Stelle zu gehen. Um zum nächsten Ereignis oder der nächsten Textmarke zu gelangen, klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen, und wählen Sie **Auf Textmarke positionieren**.

Ändern der Wiedergabeanzeige

November 29, 2018

Mit Optionen können Sie ändern, wie die aufgezeichneten Sitzungen im Player-Fenster angezeigt werden. Sie können das Bild mit Panning und Skalieren ändern, die Wiedergabe im Vollbild anzeigen, das Player-Fenster in einem eigenen Fenster und einen Rahmen um die Sitzungsaufzeichnung anzeigen, um sie vom Hintergrund des Player-Fensters zu unterscheiden.

Anzeigen des Player-Fensters im Vollbild

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Ansicht** > **Player-Vollbild**.

4. Drücken Sie ESC oder F11, um die Originalgröße des Fensters wiederherzustellen.

Anzeigen des Player-Fensters in einem eigenen Fenster

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers**auf **Ansicht** > **Player in neuem Fenster**. Ein neues Fenster wird mit dem Player-Fenster angezeigt. Sie können das Fenster ziehen und seine Größe ändern.
4. Wenn Sie das Player-Fenster im Hauptfenster einbetten möchten, wählen Sie **Ansicht** > **Player in neuem Fenster** oder drücken Sie **F10**.

Skalieren der Sitzungswiedergabe auf die Größe des Player-Fensters

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Wiedergabe** > **Panning und Skalieren** > **Passend skalieren**.

    - **Bei Passend skalieren (Schnellrendering)** wird das Bild verkleinert, die Bildqualität ist jedoch noch gut. Bilder werden schneller als mit der Option "Passend skalieren (hohe Qualität)"aufgebaut, die Bilder und der Text sind jedoch nicht scharf. Verwenden Sie diese Option, wenn Sie Leistungsprobleme mit der Option "Passend skalieren (hohe Qualität)" feststellen.
    - **Bei Passend skalieren (hohe Qualität)** wird das Bild verkleinert, die Qualität ist sehr gut. Bei dieser Option werden die Bilder möglicherweise langsamer als bei der Option "Passend skalieren (Schnellrendering)"aufgebaut.

Durchführen von Panning des Bilds

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Wiedergabe** > **Panning und Skalieren** > **Panning**. Der Zeiger ändert sich zu einer Hand und eine kleine Darstellung des Bildschirms wird oben rechts im Player-Fenster angezeigt.
4. Ziehen Sie das Bild. Die kleine Bildschirmdarstellung zeigt an, wo Sie sich im Bild befinden.
5. Um das Verschieben zu stoppen, wählen Sie eine der Skalierungsoptionen.

Anzeigen eines roten Rahmens um die Sitzungsaufzeichnung

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras** > **Optionen** > **Player**.
4. Aktivieren Sie das Kontrollkästchen **Rahmen um Sitzungsaufzeichnung anzeigen**.
   Tipp: Ist **Rahmen um Sitzungsaufzeichnung anzeigen** nicht aktiviert, können Sie den roten Rahmen vorübergehend anzeigen, indem Sie die linke Maustaste gedrückt halten, wenn der Zeiger im Player-Fenster ist.

Zwischenspeichern von Sitzungsaufzeichnungsdateien

July 1, 2019

Bei jedem Öffnen einer Sitzungsaufzeichnungsdatei lädt der Sitzungsaufzeichnungsplayer die Datei vom Speicherort herunter, auf dem die Aufzeichnungen gespeichert sind. Wenn Sie dieselben Dateien oft herunterladen, sparen Sie Zeit, wenn Sie die Dateien auf der Arbeitsstation zwischenspeichern. Zwischengespeicherte Dateien werden auf der Arbeitsstation in diesem Ordner gespeichert:

```
userprofile\\AppData\\Local\\Citrix\\SessionRecording\\Player\\Cache
```

Sie können die verwendete Cachegröße angeben. Wenn die Aufzeichnungen den angegebenen Speicherplatz auf der Festplatte vollständig belegen, löscht die Sitzungsaufzeichnung die ältesten und am wenigsten verwendeten Aufzeichnungen, um Platz für neue Aufzeichnungen zu machen. Sie können den Cache jederzeit leeren, um freien Speicherplatz auf der Festplatte zu erhalten.

Aktivieren der Zwischenspeicherung

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras** > **Optionen** > **Cache**.
4. Aktivieren Sie das Kontrollkästchen **Heruntergeladene Dateien lokal zwischenspeichern**.
5. Wenn Sie den für die Zwischenspeicherung verwendeten Speicherplatz auf dem Datenträger beschränken möchten, aktivieren Sie das Kontrollkästchen **Verwendeten Speicherplatz auf Datenträger beschränken**, und geben Sie den Speicherplatz in Megabyte an.

6. Klicken Sie auf **OK**.

Leeren des Cache

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras** > **Optionen** > **Cache**.
4. Aktivieren Sie das Kontrollkästchen **Heruntergeladene Dateien lokal zwischenspeichern**.
5. Klicken Sie im Sitzungsaufzeichnungsplayer auf **Extras** > **Optionen** > **Cache**.
6. Klicken Sie auf **Cache löschen** und dann zur Bestätigung auf **OK**.

Suchen nach Aufzeichnungen

March 19, 2020

Im Sitzungsaufzeichnungsplayer können Sie Schnellsuchen und erweiterte Suchen durchführen und Optionen festlegen, die für alle Suchen gelten. Die Suchergebnisse werden im Bereich "Suchergebnisse"des Sitzungsaufzeichnungsplayers angezeigt.

> **Hinweis:**
>
> Wenn Sie alle verfügbaren Sitzungsaufzeichnungen (bis zur Höchstanzahl der in einer Suche angezeigten Sitzungen) anzeigen möchten, führen Sie die Suche ohne Suchparameter durch.

Ausführen einer Schnellsuche

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Definieren Sie die Suchkriterien:
   - Geben Sie ein Suchkriterium im Feld **Suchen** ein.
   - Zeigen Sie auf **Suchen**, um eine Liste der Parameter als Richtlinie zu anzuzeigen.
   - Klicken Sie auf den Pfeil rechts neben dem Feld **Suchen**, um den Text für die letzten 64 Suchen anzuzeigen.
   - Wählen Sie in der Dropdownliste rechts neben dem Feld **Suchen** den Zeitraum der Aufzeichnung der Sitzung aus.

4. Klicken Sie auf das Fernglas-Symbol rechts von der Dropdownliste, um die Suche zu starten.

Durchführen einer erweiterten Suche

Die erweiterte Suche kann bis zu 20 Sekunden dauern, wenn das Ergebnis über 150.000 Einheiten umfasst. Citrix empfiehlt die Verwendung gezielterer Suchbedingungen, z. B. einen Datumsbereich oder Benutzer, um den Umfang des Ergebnisses zu limitieren.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im **Sitzungsaufzeichnungsplayer**-Fenster auf der Symbolleiste auf **Erweiterte Suche** oder wählen Sie auf der Symbolleiste **Extras** > **Erweiterte Suche**.
4. Legen Sie die Suchkriterien auf den Registerkarten im Dialogfeld **Erweiterte Suche** fest:

   - **Allgemein** ermöglicht die Suche nach Domäne oder Kontoautorität, Site, Gruppe, VDA für Serverbetriebssystem, Anwendung oder Datei-ID.
   - **Datum/Uhrzeit** ermöglicht die Suche nach Datum, Wochentag und Tageszeit.
   - **Ereignisse** ermöglicht die Suche nach Citrix-definierten und benutzerdefinierten Ereignissen, die in die Sitzungen eingefügt werden.
   - **Sonstiges** ermöglicht die Suche nach Sitzungsname, Clientname, Clientadresse und Aufzeichnungsdauer. Sie können für diese Suche auch die Höchstzahl der angezeigten Suchergebnisse und den Einschluss von archivierten Dateien in der Suche festlegen.
     Wenn Sie Suchkriterien angeben, wird die erstellte Abfrage im unteren Bereich des Dialogfelds angezeigt.

5. Klicken Sie auf **Suchen**, um die Suche zu starten.

   Sie können erweiterte Suchen speichern und abrufen. Klicken Sie im Dialogfeld **Erweiterte Suche** auf **Speichern**, um die aktuelle Abfrage zu speichern. Klicken Sie im Dialogfeld **Erweiterte Suche** auf **Öffnen**, um eine gespeicherte Abfrage abzurufen. Abfragen werden als Dateien mit der ISQ-Erweiterung gespeichert.

Festlegen von Suchoptionen

Mit den Suchoptionen im Sitzungsaufzeichnungsplayer beschränken Sie die Höchstzahl der Sitzungsaufzeichnungen, die in den Suchergebnissen angezeigt werden, und legen den Ein- oder Ausschluss von archivierten Sitzungsaufzeichnungsdateien fest.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.

2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras** > **Optionen** > **Suche**.
4. Geben Sie im Feld **Angezeigte Ergebnisse (max.)** die Anzahl der Suchergebnisse ein, die angezeigt werden. Sie können maximal 500 Ergebnisse anzeigen.
5. Abhängig davon, ob Sie archivierte Dateien in Suchen einschließen möchten, aktivieren oder deaktivieren Sie **Archivierte Dateien einschließen**.

Problembehandlung bei der Sitzungsaufzeichnung

August 18, 2021

In diesen Informationen finden Sie Lösungen zu Problemen, auf die Sie möglicherweise während oder nach der Installation der Sitzungsaufzeichnungskomponenten stoßen:

- Probleme bei der Komponentenverbindung
- Probleme bei der Sitzungsaufzeichnung
- Probleme beim Sitzungsaufzeichnungsplayer oder der Richtlinienkonsole für die Sitzungsaufzeichnung
- Probleme beim Kommunikationsprotokoll

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Sitzungsaufzeichnungsagent kann keine Verbindung herstellen

Wenn der Sitzungsaufzeichnungsagent keine Verbindung herstellen kann, wird die Ereignismeldung **Exception caught while sending poll messages to Session Recording Broker** gefolgt vom Ausnahmetext protokolliert. Der Ausnahmetext gibt die Gründe für den Verbindungsfehler an. Es sind folgende Ursachen möglich:

- **Die zugrundeliegende Verbindung wurde geschlossen. Eine vertrauenswürdige Beziehung konnte für den sicheren Kanal (SSL/TLS) nicht erstellt werden.** Diese Ausnahme bedeutet, dass der Sitzungsaufzeichnungsserver ein Zertifikat verwendet, das von einer

Zertifizierungsstelle signiert ist, die der Server mit dem Sitzungsaufzeichnungsagent nicht als vertrauenswürdig einstuft oder für die der Server kein Zertifikat der Zertifizierungsstelle hat. Das Zertifikat kann auch abgelaufen oder widerrufen sein.

Lösung: Stellen Sie sicher, dass das richtige Zertifikat der Zertifizierungsstelle auf dem Server mit dem Sitzungsaufzeichnungsagent installiert ist oder ein vertrauenswürdiges Zertifikat verwendet wird.

- **Der Remoteserver gaben einen Fehler zurück: (403) verboten.** Dies ist ein HTTPS-Standardfehler, der angezeigt wird, wenn Sie eine Verbindung mit HTTP (nicht sicheres Protokoll) versuchen. Der Computer mit dem Sitzungsaufzeichnungsserver lehnt die Verbindung ab, da er nur sichere Verbindungen annimmt.

  Lösung: Ändern Sie in den Eigenschaften des Sitzungsaufzeichnungsagents das Protokoll des Sitzungsaufzeichnungsbrokers in **HTTPS**.

Der Sitzungsaufzeichnungsbroker gab beim Auswerten einer Aufzeichnungsrichtlinienabfrage einen unbekannten Fehler zurück. Fehlercode 5 (Zugriff verweigert). Weitere Informationen finden Sie im Ereignisprotokoll auf dem Sitzungsaufzeichnungsserver. Dieser Fehler tritt auf, wenn Sitzungen gestartet werden und eine Anfrage für eine Auswertung der Aufzeichnungsrichtlinie gemacht wird. Der Fehler tritt auf, wenn die Gruppe der authentifizierten Benutzer (die Standardmitglieder) von der Rolle "PolicyQuery"in der Sitzungsaufzeichnungsautorisierungskonsole entfernt werden.

Lösung: Fügen Sie die Gruppe der authentifizierten Benutzer wieder der Rolle hinzu oder fügen Sie alle Server mit dem Sitzungsaufzeichnungsagent der Rolle "PolicyQuery"hinzu.

Die zugrundeliegende Verbindung wurde geschlossen. Eine Verbindung, die aktiv bleiben sollte, wurde vom Server geschlossen. Dieser Fehler bedeutet, dass der Sitzungsaufzeichnungsserver nicht ausgeführt wird oder keine Anfragen annehmen kann. IIS können offline geschaltet sein oder werden neu gestartet oder der Server ist offline geschaltet.

Lösung: Stellen Sie sicher, dass der Sitzungsaufzeichnungsserver gestartet wurde, IIS auf dem Server ausgeführt wird und der Server eine Verbindung zum Netzwerk hat.

Installation von Sitzungsaufzeichnungsserverkomponenten schlägt fehl

Die Installation der Sitzungsaufzeichnungsserverkomponenten schlägt mit den Fehlercodes 2503 und 2502 fehl.
Lösung:
Überprüfen Sie die Zugriffssteuerungsliste (ACL) im Ordner C:\windows\temp, um sicherzustellen, dass lokale Benutzer und Gruppen Schreibberechtigung für diesen Ordner haben. Falls nicht, fügen Sie die Schreibberechtigung manuell hinzu.

Sitzungsaufzeichnungsplayer kann keine Verbindung mit der Datenbank für die Sitzungsaufzeichnung herstellen

Wenn der Sitzungsaufzeichnungsserver keine Verbindung mit der Datenbank für die Sitzungsaufzeichnung herstellen kann, wird möglicherweise eine Fehlermeldung mit ungefähr dem folgenden Wortlaut angezeigt:

Ereignisquelle:

A network-related or instance-specific error occurred while establishing a connection to SQL Server. Dieser Fehler wird mit der ID 2047 im Anwendungsereignisprotokoll der Ereignisanzeige des Computers aufgezeichnet, auf dem der Sitzungsaufzeichnungsserver gehostet wird.

Citrix Speichermanager der Sitzungsaufzeichnung - Beschreibung: Citrix: Ausnahme beim Herstellen der Datenbankverbindung. Dieser Fehler wird im Anwendungsereignisprotokoll der Ereignisanzeige des Computers aufgezeichnet, auf dem der Sitzungsaufzeichnungsserver gehostet wird.

Verbindung mit dem Sitzungsaufzeichnungsserver kann nicht hergestellt werden. Überprüfen Sie, ob der Sitzungsaufzeichnungsserver ausgeführt wird. Diese Fehlermeldung wird angezeigt, wenn Sie die Richtlinienkonsole für die Sitzungsaufzeichnung starten.

Lösung:

- Die Express Edition von Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014 oder Microsoft SQL Server 2016 ist auf einem eigenständigen Server installiert und Dienste oder Einstellungen sind nicht richtig für die Sitzungsaufzeichnung konfiguriert. Auf dem Server muss das TCP/IP-Protokoll aktiviert sein, und der SQL Server Browser-Dienst muss ausgeführt werden. Weitere Informationen zur Aktivierung dieser Einstellungen finden Sie in der Microsoft Dokumentation.
- Bei der Installation der Sitzungsaufzeichnung (Verwaltungskomponenten) wurden falsche Server- und Datenbankinformationen angegeben. Deinstallieren Sie die Datenbank für die Sitzungsaufzeichnung und installieren Sie sie mit den richtigen Informationen neu.
- Der Server mit der Datenbank für die Sitzungsaufzeichnung ist ausgefallen. Prüfen Sie die Serverkonnektivität.
- Der Computer mit dem Sitzungsaufzeichnungsserver oder der Computer mit dem Server für die Datenbank für die Sitzungsaufzeichnung kann den vollqualifizierten Domänennamen oder den NetBIOS-Namen des jeweils anderen nicht auflösen. Stellen Sie mit “Ping”sicher, dass die Namen aufgelöst werden können.
- Prüfen Sie, ob in der Firewallkonfiguration für die Datenbank für die Sitzungsaufzeichnung SQL Server-Verbindungen zugelassen sind. Weitere Informationen finden Sie im Microsoft-Artikel https://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access.

Logon failed for user 'NT_AUTHORITY\ANONYMOUS LOGON'. Diese Fehlermeldung gibt an, dass die Dienste falsch als .\administrator angemeldet sind.

Lösung: Starten Sie die Dienste als lokaler Systembenutzer und die SQL-Dienste neu.

Sitzungen werden nicht aufgezeichnet

Wenn die Anwendungssitzungen nicht aufgezeichnet werden, prüfen Sie zuerst das Anwendungsereignisprotokoll in der Ereignisanzeige auf dem Serverbetriebssystem-VDA, auf dem der Sitzungsaufzeichnungsagent und der Sitzungsaufzeichnungsserver ausgeführt werden. Sie können nützliche Diagnoseinformationen erhalten.

Wenn Sitzungen nicht aufgezeichnet werden, kann dies folgende Gründe haben:

- **Komponentenverbindungen und Zertifikate**. Wenn die Sitzungsaufzeichnungskomponenten nicht miteinander kommunizieren können, können Sitzungsaufzeichnungen fehlschlagen. Zur Behebung von Aufzeichnungsproblemen sollten Sie sicherstellen, dass alle Komponenten richtig konfiguriert sind und auf die richtigen Computer verweisen, und dass alle Zertifikate gültig und richtig installiert sind.
- **Umgebungen ohne Active Directory-Domäne**. Die Sitzungsaufzeichnung ist für eine Ausführung in einer Microsoft Active Directory-Domänenumgebung konzipiert. Wenn Sie keine Active Directory-Umgebung ausführen, können Aufzeichnungsprobleme auftreten. Stellen Sie sicher, dass alle Komponenten der Sitzungsaufzeichnung auf Computern ausgeführt werden, die Mitglieder einer Active Directory-Domäne sind.
- **Die Sitzungsfreigabe verursacht einen Konflikt mit der aktiven Richtlinie:** Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet. Anwendungen, die später in derselben Sitzung geöffnet werden, halten die Richtlinie ein, die für die erste Anwendung gilt. Veröffentlichen Sie die problematischen Anwendungen auf eigenständigen Serverbetriebssystem-VDAs oder deaktivieren Sie die Sitzungsfreigabe, um einen Konflikt zwischen der Sitzungsfreigabe und der aktiven Richtlinie zu vermeiden.
- **Die Aufzeichnung ist nicht aktiviert:** Wenn Sie den Sitzungsaufzeichnungsagent auf einem Serverbetriebssystem-VDA installieren, wird die Aufzeichnung auf dem Server standardmäßig aktiviert. Die Aufzeichnung erfolgt erst, wenn eine aktive Aufzeichnungsrichtlinie konfiguriert ist, die Aufzeichnungen zulässt.
- **Die aktive Aufzeichnungsrichtlinie lässt die Aufzeichnung nicht zu.** Zum Aufzeichnen einer Sitzung muss die aktive Aufzeichnungsrichtlinie zulassen, dass die Sitzungen für den Benutzer, Server oder die veröffentlichte Anwendung aufgezeichnet werden können.
- **Die Dienste der Sitzungsaufzeichnung werden nicht ausgeführt.** Zum Aufzeichnen von Sitzungen muss der Sitzungsaufzeichnungsagent-Dienst auf dem Serverbetriebssystem-VDA und der Dienst des Speichermanagers der Sitzungsaufzeichnung auf dem Computer mit dem Sitzungsaufzeichnungsserver ausgeführt werden.

- **MSMQ ist nicht konfiguriert:** Wenn MSMQ auf dem Computer mit dem Sitzungsaufzeichnungsagent und dem Computer mit dem Sitzungsaufzeichnungsserver falsch konfiguriert ist, können Aufzeichnungsprobleme auftreten.

Wiedergabe von Livesitzungen nicht möglich

Wenn Sie Probleme beim Wiedergeben von Aufzeichnungen im Sitzungsaufzeichnungsplayer haben, werden möglicherweise die folgenden Fehlermeldungen angezeigt:

Fehler beim Download der Sitzungsaufzeichnungsdatei. Wiedergabe einer Livesitzung ist nicht zulässig. Die Konfiguration des Servers lässt diese Funktion nicht zu. Dieser Fehler gibt an, dass der Server die Aktion nicht zulässt.

Lösung: Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Wiedergabe** und aktivieren Sie das Kontrollkästchen **Wiedergabe von Livesitzungen zulassen**.

Aufzeichnungen sind beschädigt oder unvollständig

- Wenn Aufzeichnungen beim Anzeigen im Sitzungsaufzeichnungsplayer beschädigt oder unvollständig sind, werden u. U. auch Warnungen in den Ereignisprotokollen auf dem Sitzungsaufzeichnungsagent protokolliert.

  Ereignisquelle: Citrix Speichermanager der Sitzungsaufzeichnung

  Beschreibung: Datenverlust bei der Aufzeichnung von <Name der ICL-Datei>.

  Dies passiert normalerweise, wenn mit Maschinenerstellungsdienste (MCS) oder Provisioning Services VDAs mit einem Masterimage und installiertem Microsoft Message Queuing (MSMQ) erstellt werden. In diesem Fall haben die VDAs die gleiche QMId für MSMQ.

  Erstellen Sie als Workaround eine eindeutige QMId für jeden VDA. Weitere Informationen finden Sie unter **Installieren, Aktualisieren und Deinstallieren der Sitzungsaufzeichnung** in Schritt 8 des Verfahrens Installieren des Sitzungsaufzeichnungsagents.

- Im Sitzungsaufzeichnungsplayer wird bei der Wiedergabe einer Aufzeichnungsdatei möglicherweise folgender interner Fehler gemeldet: **Die wiedergegebene Datei meldet, dass ein interner Systemfehler (Fehlercode: 9) bei der Originalaufzeichnung aufgetreten ist. Die Datei kann noch bis zu der Stelle wiedergegeben werden, an der der Aufzeichnungsfehler auftrat.**

  Dies wird in der Regel durch eine unzureichende Puffergröße des Sitzungsaufzeichnungsagents verursacht, wenn grafikintensive Sitzungen aufgezeichnet werden.

  Legen Sie als Workaround im Sitzungsaufzeichnungsagent für HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Sm einen höheren Wert fest und starten Sie den Computer neu.

Test der Verbindung mit Datenbankinstanz schlägt bei Installation der Datenbank für Sitzungsaufzeichnung oder Sitzungsaufzeichnungsserver fehl

Bei der Installation der Datenbank für die Sitzungsaufzeichnung oder des Sitzungsaufzeichnungsservers schlägt der Test der Verbindung fehl und es wird die Fehlermeldung **Database connection test failed. Please correct Database instance name** angezeigt, selbst wenn der Datenbankinstanzname richtig ist.

Stellen Sie in diesem Fall sicher, dass der aktuelle Benutzer die öffentliche SQL Server-Rollenberechtigung hat, damit der Test nicht aufgrund einer fehlenden Berechtigung fehlschlägt.

Administratorprotokollierung

Installieren Sie unter Windows Server 2008 R2 SP1 vor der Administratorprotokollierung **.NET Framework 3.5-Features** > **WCF-Aktivierung** > **HTTP-Aktivierung** und dann .NET Framework 4.5 oder eine höhere Version. Installieren Sie diese beiden erforderlichen Elemente nicht in umgekehrter Reihenfolge. Ansonsten funktioniert die Administratorprotokollierung möglicherweise nicht einwandfrei. Beim Ändern der Sitzungsaufzeichnungskonfiguration über die Eigenschaften des Sitzungsaufzeichnungsservers und beim Aktualisieren von Sitzungsaufzeichnungsrichtlinien über die Richtlinienkonsole für die Sitzungsaufzeichnung kann es vorkommen, dass Vorgänge blockiert werden, wenn die verbindliche Protokollierung aktiviert ist.

Lösen des Problems:

1. Öffnen Sie den IIS-Manager und navigieren Sie zum Knoten **Anwendungspools**.
2. Klicken Sie mit der rechten Maustaste auf **SessionRecordingLoggingAppPool** und öffnen Sie das Dialogfeld **Grundeinstellungen**.
3. Ändern Sie die .NET Framework-Version in 4.0.

Prüfen der Komponentenverbindungen

April 30, 2019

Beim Setup der Sitzungsaufzeichnung stellen die Komponenten möglicherweise keine Verbindung mit den anderen Komponenten her. Alle Komponenten kommunizieren mit dem Sitzungsaufzeichnungsserver (Broker). In der Standardeinstellung ist der Broker (eine IIS-Komponente) mit dem Standardwebsitezertifikat von IIS gesichert. Wenn eine Komponente keine Verbindung mit dem Sitzungsaufzeichnungsserver herstellen kann, kann der Verbindungsversuch der anderen Komponenten auch fehlschlagen.

Der Sitzungsaufzeichnungsagent und der Sitzungsaufzeichnungsserver (Speichermanager und Broker) protokollieren Verbindungsfehler im Ereignisprotokoll der Anwendungen in der Ereignisanzeige auf dem Computer mit dem Sitzungsaufzeichnungsserver. Die Richtlinienkonsole für die Sitzungsaufzeichnung und der Sitzungsaufzeichnungsplayer zeigen Fehlermeldungen auf dem Bildschirm an, wenn keine Verbindung hergestellt werden kann.

Prüfen, ob der Sitzungsaufzeichnungsagent verbunden ist

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf **Verbindung**.
4. Stellen Sie sicher, dass der Wert für den Sitzungsaufzeichnungsserver den Namen des Computers enthält, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
5. Stellen Sie sicher, dass der für den Sitzungsaufzeichnungsserver angegebene Server vom VDA für Serverbetriebssysteme kontaktiert werden kann.

Hinweis: Überprüfen Sie das Anwendungsereignisprotokoll auf Fehler und Warnungen.

Prüfen, ob der Sitzungsaufzeichnungsserver verbunden ist

Achtung: Die Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Öffnen Sie den Registrierungs-Editor.
3. Navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Stellen Sie sicher, dass der Wert für **SmAudDatabaseInstance** richtig auf die Datenbank für die Sitzungsaufzeichnung verweist, die Sie in der SQL Server-Instanz installiert haben.

Prüfen, ob die Datenbank für die Sitzungsaufzeichnung verbunden ist

1. Öffnen Sie mit einem SQL-Verwaltungswerkzeug die SQL-Instanz, die die installierte Sitzungsaufzeichnungsdatenbank enthält.
2. Öffnen Sie die Sicherheitsberechtigungen der Datenbank für die Sitzungsaufzeichnung.
3. Stellen Sie sicher, dass das Computerkonto der Sitzungsaufzeichnung Zugriffsrechte auf die Datenbank hat. Beispiel: Wenn der Server mit dem Sitzungsaufzeichnungsserver **SsRecSrv** in der MIS-Domäne genannt wird, muss das Computerkonto in der Datenbank als

MIS\SsRecSrv$ konfiguriert werden. Dieser Wert wird während der Installation der Datenbank für die Sitzungsaufzeichnung konfiguriert.

Testen der IIS-Konnektivität

Mit dem Testen der Verbindungen zwischen Sitzungsaufzeichnungsserver und IIS-Site unter Zugriff auf die Webseite des Sitzungsaufzeichnungsbrokers mit einem Webbrowser können Sie feststellen, ob Kommunikationsprobleme zwischen den Sitzungsaufzeichnungskomponenten auf eine falsche Protokollkonfiguration, Zertifizierungsprobleme oder Probleme beim Start des Sitzungsaufzeichnungsbrokers zurückzuführen sind.

Prüfen der IIS-Konnektivität für den Sitzungsaufzeichnungsagent

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
   - HTTPS: `https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
   - HTTP: `http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Prüfen der IIS-Konnektivität für den Sitzungsaufzeichnungsplayer

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
   - HTTPS: `https://servername/SessionRecordingBroker/Player.rem?wsdl`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
   - HTTP: `http://servername/SessionRecordingBroker/Player.rem?wsdl`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Prüfen der IIS-Konnektivität für die Richtlinienkonsole für die Sitzungsaufzeichnung

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
    - HTTPS: `https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
    - HTTP: `http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Wenn ein XML-Dokument im Browser angezeigt wird, bestätigt dies, dass der Computer, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung ausgeführt wird, mit dem Sitzungsaufzeichnungsserver-Computer verbunden ist und das konfigurierte Protokoll verwendet.

Problembehandlung bei Zertifikaten

Wenn Sie HTTPS als Kommunikationsprotokoll verwenden, muss der Computer mit dem Sitzungsaufzeichnungsserver mit einem Serverzertifikat konfiguriert werden. Alle Komponentenverbindungen mit dem Sitzungsaufzeichnungsserver müssen ein Zertifikat der Stammzertifizierungsstelle haben. Sonst schlagen die Verbindungen zwischen den Komponenten fehl.

Sie können die Zertifikate genauso wie beim Testen der IIS-Konnektivität durch Zugriff auf die Webseite des Sitzungsaufzeichnungsbrokers testen. Wenn Sie auf die XML-Seite für jede Komponente zugreifen können, sind die Zertifikate richtig konfiguriert.

Im Anschluss finden Sie Gründe, warum Zertifikate zu Verbindungsproblemen führen:

- **Ungültige oder fehlende Zertifikate:** Wenn der Server mit dem Sitzungsaufzeichnungsagent kein Stammzertifikat für die Vertrauenswürdigkeit des Serverzertifikats hat, den Sitzungsaufzeichnungsserver nicht als vertrauenswürdig ansieht und keine Verbindung über HTTPS herstellen kann, schlägt die Verbindung fehl. Stellen Sie in diesem Fall sicher, dass alle Komponenten das Serverzertifikat auf dem Sitzungsaufzeichnungsserver als vertrauenswürdig einstufen.
- **Inkonsistente Benennung:** Wenn das Serverzertifikat, das dem Computer mit dem Sitzungsaufzeichnungsserver zugewiesen ist, mit einem FQDN erstellt wurde, müssen alle Komponenten, die eine Verbindung herstellen, für die Verbindung mit dem Sitzungsaufzeichnungsserver den FQDN verwenden. Wenn ein NetBIOS-Name verwendet wird, konfigurieren Sie die Komponenten mit einem NetBIOS-Namen für den Sitzungsaufzeichnungsserver.

- **Abgelaufene Zertifikate.** Wenn ein Serverzertifikat abgelaufen ist, schlägt eine Verbindung mit dem Sitzungsaufzeichnungsserver über HTTPS fehl. Stellen Sie sicher, dass das Zertifikat, das dem Computer mit dem Sitzungsaufzeichnungsserver zugewiesen ist, gültig und nicht abgelaufen ist. Wenn dasselbe Zertifikat für die digitale Signatur der Sitzungsaufzeichnungen verwendet wird, enthält das Ereignisprotokoll des Computers mit dem Sitzungsaufzeichnungsserver Fehlermeldungen, dass das Zertifikat abgelaufen ist, oder Warnmeldungen, wenn das Zertifikat bald abläuft.

Fehler beim Suchen nach Aufzeichnungen im Player

August 18, 2021

Wenn Sie Probleme beim Suchen nach Aufzeichnungen im Sitzungsaufzeichnungsplayer haben, werden möglicherweise die folgenden Fehlermeldungen angezeigt:

- **Fehler bei der Suche nach Sitzungsaufzeichnungsdateien. Der Name des Remoteservers konnte nicht aufgelöst werden: servername.** **Servername** ist der Name des Servers, mit dem der Sitzungsaufzeichnungsplayer versucht, eine Verbindung herzustellen. Der Sitzungsaufzeichnungsplayer kann den Sitzungsaufzeichnungsserver nicht kontaktieren. Zu den beiden möglichen Gründen gehören ein falsch eingegebener Servername, oder DNS kann den Servernamen nicht auflösen.

  Lösung: Klicken Sie im Player-Menü auf **Extras** > **Optionen** > **Verbindungen** und prüfen Sie die Richtigkeit des Servernamens, der in der Liste **Sitzungsaufzeichnungsserver** aufgeführt ist. Wenn der Name richtig ist, stellen Sie mit dem Ping-Befehl sicher, dass der Name aufgelöst werden kann. Wenn der Sitzungsaufzeichnungsserver nicht betriebsbereit oder offline geschaltet ist, tritt ein Fehler beim Suchen nach Sitzungsaufzeichnungsdateien auf. Die Fehlermeldung ist **Fehler beim Verbinden mit dem Remoteserver**.

- **Fehler beim Verbinden mit dem Remoteserver.** Dieser Fehler tritt auf, wenn der Sitzungsaufzeichnungsserver nicht betriebsbereit oder offline geschaltet ist.

  Resolution: Verify that the Session Recording Server is connected.

- **Zugriff verweigert.** Ein Fehler “Zugriff verweigert”kann auftreten, wenn der Benutzer nicht berechtigt ist, Sitzungsaufzeichnungsdateien zu suchen und herunterzuladen.

  Lösung: Weisen Sie den Benutzer in der Sitzungsaufzeichnungs-Autorisierungskonsole der Rolle “Player”zu.

- **Zugriff bei zugewiesener Playerrolle verweigert.** Dieser Fehler tritt auf, wenn Sie den Sitzungsaufzeichnungsplayer auf derselben Maschine wie den Sitzungsaufzeichnungsserver

installiert und die Benutzerkontensteuerung (UAC) aktiviert haben. Wenn Sie der Playerrolle die Gruppe der Domänenadministratoren oder Administratoren zuweisen, kann es vorkommen, dass ein in der Gruppe enthaltenes, nicht integriertes Administratorkonto bei der Suche von Aufzeichnungsdateien mit dem Sitzungsaufzeichnungsplayer die rollenbasierte Prüfung nicht besteht.

Resolutions:

- Run Session Recording Player as administrator.
- Assign specific users as Player role rather than the entire group.
- Install Session Recording Player in a separate machine rather than Session Recording Server.

- **Fehler bei der Suche nach Sitzungsaufzeichnungsdateien. Die zugrundeliegende Verbindung wurde geschlossen. Eine vertrauenswürdige Beziehung konnte für den sicheren Kanal (SSL/TLS) nicht erstellt werden.** Diese Ausnahme tritt auf, wenn der Sitzungsaufzeichnungsserver ein Zertifikat verwendet, das von einer Zertifizierungsstelle signiert ist, die das Clientgerät nicht vertrauenswürdig ansieht oder für die das Clientgerät kein Zertifikat der Zertifizierungsstelle hat.

  Resolution: Install the correct or trusted CA certificate workstation where the Session Recording Player is installed.

- **Der Remoteserver gaben einen Fehler zurück: (403) verboten.** Dies ist ein HTTPS-Standardfehler, der angezeigt wird, wenn Sie eine Verbindung mit HTTP (nicht sicheres Protokoll) versuchen. Der Server lehnt die Verbindung ab, da er standardmäßig nur sichere Verbindungen annimmt.

  Lösung: Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras** > **Optionen** > **Verbindungen**. Wählen Sie den Server aus der Liste **Sitzungsaufzeichnungsserver** aus und klicken Sie auf **Ändern**. Ändern Sie das Protokoll von **HTTP** in **HTTPS**.

Problembehandlung bei MSMQ

Wenn eine Benachrichtigung angezeigt wird, mit einer Suche im Sitzungsaufzeichnungsplayer jedoch keine Aufzeichnungen gefunden werden, kann ein Problem mit MSMQ bestehen. Prüfen Sie, ob die Warteschlange mit dem Sitzungsaufzeichnungsserver (Speichermanager) verbunden ist. Testen Sie mit einem Webbrowser, ob Verbindungsfehler bestehen (wenn Sie HTTP oder HTTPS als MSMQ-Kommunikationsprotokoll verwenden).

Sicherstellen der Verbindung der Warteschlange

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent gehostet wird, und zeigen Sie die ausgehenden Warteschlangen an.

2. Stellen Sie sicher, dass die Warteschlange des Computers mit dem Sitzungsaufzeichnungsserver verbunden ist.

    - Wenn der Zustand **Warten auf Verbindung** ist, Nachrichten in der Warteschlange sind und als Protokoll HTTP oder HTTPS verwendet wird (gemäß Auswahl auf der Registerkarte **Verbindungen** unter **Sitzungsaufzeichnungsagent - Eigenschaften**), führen Sie Schritt 3 aus.
    - Wenn der Zustand **Verbunden** ist und keine Nachrichten in der Warteschlange sind, besteht möglicherweise ein Problem mit dem Server, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird. Überspringen Sie Schritt 3 und führen Sie Schritt 4 aus.

3. Wenn Nachrichten in der Warteschlange sind, öffnen Sie einen Webbrowser und geben Sie folgende Adresse ein:

    - HTTPS: `https://servername/msmq/private$/CitrixSmAudData`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.
    - HTTP: `http://servername/msmq/private$/CitrixSmAudData`, wobei *servername* der Name des Computers ist, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird.

    Wenn die Seite einen Fehler zurückgibt, z. B. **Der Server nimmt nur sichere Verbindungen an**, ändern Sie das für MSMQ unter **Sitzungsaufzeichnungsagent - Eigenschaften** aufgeführte Protokoll in HTTPS. Wird ein Problem mit dem Websitesicherheitszertifikat gemeldet, besteht möglicherweise ein Problem mit der Vertrauensbeziehung für den sicheren Kanal (TLS). Installieren Sie dann das richtige Zertifikat der Zertifizierungsstelle oder verwenden Sie eine vertrauenswürdige Zertifizierungsstelle.

4. Wenn die Warteschlange keine Nachrichten enthält, melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an und zeigen Sie private Warteschlangen an. Wählen Sie **citrixsmauddata**. Wenn Nachrichten in der Warteschlange sind (Spalte “Nachrichtenanzahl”), stellen Sie sicher, dass der Dienst des Speichermanagers der Sitzungsaufzeichnung gestartet ist. Starten Sie sonst den Dienst neu.

Ändern des Kommunikationsprotokolls

November 29, 2018

Aus Sicherheitsgründen empfiehlt Citrix, HTTP nicht als Kommunikationsprotokoll zu verwenden. Die Sitzungsaufzeichnung ist für die Verwendung von HTTPS konfiguriert. Zur Verwendung von HTTP anstelle von HTTPS müssen Sie mehrere Einstellungen ändern.

Verwenden von HTTP als Kommunikationsprotokoll

1. Melden Sie sich bei dem Computer an, der den Sitzungsaufzeichnungsserver hostet, und deaktivieren Sie sichere Verbindungen für den Sitzungsaufzeichnungsbroker in IIS.
2. Ändern Sie auf jedem Server, auf dem der Sitzungsaufzeichnungsagent installiert ist, das eingestellte Protokoll von HTTPS in HTTP im Dialogfeld **Sitzungsaufzeichnungsagent - Eigenschaften**:

    a) Melden Sie sich bei jedem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
    b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
    c) Klicken unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte **Verbindungen**.
    d) Klicken Sie im Bereich **Sitzungsaufzeichnungsbroker** in der Dropdownliste **Protokoll** auf **HTTP** und bestätigen Sie die Änderung mit **OK**. Bestätigen Sie den Neustart des Dienstes mit **Ja**.

3. Ändern Sie die Protokolleinstellung von HTTPS zu HTTP in den Einstellungen des Sitzungsaufzeichnungsplayers:

    a) Melden Sie sich an jeder Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
    b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
    c) Klicken Sie im Menü von **Sitzungsaufzeichnungsplayer** auf **Extras** > **Optionen** > **Verbindungen**, wählen Sie den Server aus und klicken Sie auf **Ändern**.
    d) Wählen Sie **HTTP** aus der Dropdownliste **Protokoll** und klicken Sie zwei Mal auf **OK**, um die Änderung zu akzeptieren und das Dialogfeld zu schließen.

4. Ändern Sie die Protokolleinstellung von HTTPS zu HTTP in der Richtlinienkonsole für die Sitzungsaufzeichnung:

    a) Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
    b) Klicken Sie im Menü **Start** auf **Richtlinienkonsole für die Sitzungsaufzeichnung**.
    c) Wählen Sie **HTTP** in der Dropdownliste **Protokoll** und klicken Sie auf **OK**, um die Verbindung herzustellen. Wenn die Verbindung erfolgreich hergestellt wird, wird diese Einstellung gespeichert und beim nächsten Starten der Richtlinienkonsole für die Sitzungsaufzeichnung verwendet.

Zurücksetzen des Kommunikationsprotokolls auf HTTPS

1. Melden Sie sich an dem Computer an, der den Sitzungsaufzeichnungsserver hostet, und aktivieren Sie sichere Verbindungen für den Sitzungsaufzeichnungsbroker in IIS.
2. Ändern Sie auf jedem Server, auf dem der Sitzungsaufzeichnungsagent installiert ist, das eingestellte Protokoll von HTTP in HTTPS im Dialogfeld **Sitzungsaufzeichnungsagent - Eigenschaften**:

    a) Melden Sie sich bei jedem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
    b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
    c) Klicken unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte **Verbindungen**.
    d) Klicken Sie im Bereich **Sitzungsaufzeichnungsbroker** in der Dropdownliste **Protokoll** auf **HTTPS** und bestätigen Sie die Änderung mit **OK**. Bestätigen Sie den Neustart des Dienstes mit **Ja**.

3. Ändern Sie die Protokolleinstellung von HTTP zu HTTPS in den Einstellungen des Sitzungsaufzeichnungsplayers:

    a) Melden Sie sich an jeder Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
    b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
    c) Klicken Sie im Menü von **Sitzungsaufzeichnungsplayer** auf **Extras** > **Optionen** > **Verbindungen**, wählen Sie den Server aus und klicken Sie auf **Ändern**.
    d) Wählen Sie **HTTPS** aus der Dropdownliste **Protokoll** und klicken Sie zwei Mal auf **OK**, um die Änderung zu akzeptieren und das Dialogfeld zu schließen.

4. Ändern Sie die Protokolleinstellung von HTTP zu HTTPS in der Sitzungsregistrierungsrichtlinienkonsole:

    a) Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
    b) Klicken Sie im Menü **Start** auf **Richtlinienkonsole für die Sitzungsaufzeichnung**.
    c) Wählen Sie **HTTPS** in der Dropdownliste **Protokoll** und klicken Sie auf **OK**, um die Verbindung herzustellen. Wenn die Verbindung erfolgreich hergestellt wird, wird diese Einstellung gespeichert und beim nächsten Starten der Richtlinienkonsole für die Sitzungsaufzeichnung verwendet.

Verwalten der Datensätze in der Datenbank

August 18, 2021

Das ICLDB-Hilfsprogramm (ICA Log database) ist ein Datenbankbefehlszeilenprogramm, mit dem Sie Sitzungsaufzeichnungsdatensätze in der Datenbank manipulieren. Dieses Hilfsprogramm wird mit der Sitzungsaufzeichnung in Laufwerk:\Programme\Citrix\SessionRecording\Server\Bin auf dem Server mit der Serversoftware der Sitzungsaufzeichnung installiert.

Übersichtstabelle

In der folgenden Tabelle finden Sie die Befehle und Optionen für das ICLDB-Hilfsprogramm. Geben Sie die Befehle im folgenden Format ein:

icldb [version | locate | dormant | import | archive | remove | removeall] Befehlsoptionen [/l] [/f] [/s] [/?]

> **Hinweis:**
>
> Ausführlichere Anweisungen finden Sie in der Hilfe des Hilfsprogramms. Zum Öffnen der Hilfe geben Sie an der Eingabeaufforderung Laufwerk:**\%ProgramFiles%\Citrix\SessionRecording\Server\Bin** den Befehl **icldb /?** ein. Hilfe für bestimmte Befehle rufen Sie mit dem Befehl **icldb** Befehl */?* auf.

Befehl	Beschreibung
archive	Archiviert Sitzungsaufzeichnungsdateien, die älter als der angegebene Aufbewahrungszeitraum sind. Archivieren Sie Dateien mit diesem Befehl.

Befehl	Beschreibung
dormant	Zählt oder zeigt die Sitzungsaufzeichnungsdateien an, die als inaktiv angesehen werden. Inaktive Dateien sind Sitzungsaufzeichnungen, die aufgrund von Datenverlust nicht abgeschlossen wurden. Verwenden Sie diesen Befehl, wenn Sie den Verdacht haben, dass Sie Daten verlieren. Sie können prüfen, ob die Sitzungsaufzeichnungsdateien für die ganze Datenbank oder nur Aufzeichnungen inaktiv werden, die in der angegebenen Anzahl von Tagen, Stunden oder Minuten aufgezeichnet wurden.
import	Importiert Sitzungsaufzeichnungsdateien in die Datenbank für die Sitzungsaufzeichnung. Mit diesem Befehl erstellen Sie die Datenbank neu, wenn Sie Datensätze der Datenbank verlieren. Mit diesem Befehl führen Sie auch Datenbanken zusammen (wenn Sie zwei Datenbanken haben, können Sie die Dateien von einer der Datenbanken importieren).
locate	Sucht und zeigt den vollständigen Pfad einer Sitzungsaufzeichnungsdatei an. Als Kriterium wird die Datei-ID verwendet. Mit diesem Befehl suchen Sie den Speicherort einer Sitzungsaufzeichnungsdatei. Außerdem können Sie mit einer bestimmten Datei prüfen, ob die Datenbank aktuell ist.
remove	Entfernt die Verweise auf Sitzungsaufzeichnungsdateien aus der Datenbank. Mit diesem Befehl bereinigen Sie die Datenbank (verwenden Sie diesen Befehl mit Vorsicht). Geben Sie den Aufbewahrungszeitraum als Kriterium an. Sie können auch die zugeordnete physische Datei löschen.

Befehl	Beschreibung
removeall	Entfernt alle Verweise auf Sitzungsaufzeichnungsdateien aus der Datenbank für die Sitzungsaufzeichnung und setzt diese auf den Originalzustand zurück. Die physische Datei wird nicht gelöscht. Sie können diese Dateien jedoch nicht im Sitzungsaufzeichnungsplayer suchen. Mit diesem Befehl bereinigen Sie die Datenbank (verwenden Sie diesen Befehl mit Vorsicht). Gelöschte Verweise können nur von einer Sicherungskopie wieder hergestellt werden.
version	Zeigt die Schemaversion der Datenbank für die Sitzungsaufzeichnung an.
/l	Protokolliert die Ergebnisse und Fehler im Windows-Ereignisprotokoll.
/f	Erzwingt die Ausführung des Befehls ohne Aufforderungen.
/s	Unterdrückt die Copyright-Nachricht.
/?	Zeigt die Hilfe für die Befehle an.

Archivieren von Sitzungsaufzeichnungsdateien

Archivieren Sie Sitzungsaufzeichnungsdateien regelmäßig, damit an den Speicherorten für die Aufzeichnung immer ausreichend freier Platz zur Verfügung steht. Das Archivierungsintervall hängt von dem verfügbaren Speicherplatz und der Größe typischer Sitzungsaufzeichnungsdateien ab. Sitzungsaufzeichnungsdateien können ab zwei Tage nach dem Sitzungsstart archiviert werden. Diese Regel soll verhindern, dass Liveaufzeichnungen vor Abschluss archiviert werden.

Sitzungsaufzeichnungen können auf zweierlei Weise archiviert werden. Der Datenbankdatensatz einer Sitzungsaufzeichnung kann auf den Status “Archiviert”aktualisiert werden, während die Sitzungsaufzeichnungsdatei an ihrem Speicherort verbleibt. Durch diese Methode werden die Suchergebnisse im Player verringert. Die zweite Methode besteht darin, den Datenbankdatensatz der Sitzungsaufzeichnung auf “Archiviert”zu aktualisieren und die Sitzungsaufzeichnungsdatei zur Sicherung auf ein alternatives Speichermedium zu verschieben. Bei Verwendung des ICLDB-Hilfsprogramms werden Sitzungsaufzeichnungsdateien in das angegebene Verzeichnis verschoben, in dem die ursprüngliche Ordnerstruktur “Jahr/Monat/Tag”nicht besteht.

Ein Datensatz in der Sitzungsaufzeichnungsdatenbank enthält zwei mit der Archivierung verbundene Felder: die Archivierungszeit (Datum und Uhrzeit der Archivierung) und die Archivierungsnotiz, d. h. ein optionaler Text, den der Administrator bei der Archivierung eingeben kann. Die beiden Felder weisen darauf hin, dass und wann eine Sitzungsaufzeichnung archiviert wurde.

Im Sitzungsaufzeichnungsplayer werden archivierte Sitzungsaufzeichnungen mit dem Status "Archiviert"und dem Datum und der Uhrzeit der Archivierung angezeigt. Archivierte Sitzungsaufzeichnungen können weiterhin abgespielt werden, sofern die Dateien nicht verschoben wurden. Wurde eine Sitzungsaufzeichnungsdatei bei der Archivierung verschoben, wird gemeldet, dass die Datei nicht gefunden wurde. Die Sitzungsaufzeichnungsdatei muss wiederhergestellt werden, damit sie abgespielt werden kann. Zum Wiederherzustellen einer Sitzungsaufzeichnung benötigt der Administrator die im Dialogfeld "Eigenschaften"des Sitzungsaufzeichnungsplayers zu der Sitzung angezeigte Datei-ID und Uhrzeit der Archivierung. Das Verfahren zur Wiederherstellung archivierter Dateien wird unter Wiederherstellen von Sitzungsaufzeichnungsdateien weiter unten erläutert.

Der Befehl **archive** des Hilfsprogramms ICLDB kann mit folgenden Parametern verwendet werden:

- **/RETENTION:<Tage>:** Dauer der Aufbewahrung von Sitzungsaufzeichnungen in Tagen. Aufnahmen, die älter als die angegebene Anzahl von Tagen sind, werden in der Sitzungsaufzeichnungsdatenbank als archiviert markiert. Der Aufbewahrungszeitraum muss mindestens 2 Tage betragen.
- **/LISTFILES:** vollständigen Pfad und Dateiname der Sitzungsaufzeichnungsdateien bei der Archivierung. Dieser Parameter ist optional.
- **/MOVETO:<Verzeichnis>:** Verzeichnis, in das archivierte Sitzungsaufzeichnungsdateien verschoben werden. Das Verzeichnis muss vorhanden sein. Dieser Parameter ist optional. Wird kein Verzeichnis angegeben, verbleiben die Dateien an ihrem ursprünglichen Speicherort.
- **/NOTE:<Notiz>:** Textnotiz, die dem Datenbankdatensatz für jede archivierte Sitzungsaufzeichnung hinzugefügt wird. Die Notiz muss in doppelte Anführungszeichen gesetzt werden. Dieser Parameter ist optional.
- **/L:** protokolliert Ergebnisse und Fehler in Verbindung mit den archivierten Sitzungsaufzeichnungsdateien im Windows-Ereignisprotokoll. Dieser Parameter ist optional.
- **/F:** erzwingt die Ausführung des Archivierungsbefehls ohne Aufforderungen. Dieser Parameter ist optional.

Archivieren von Sitzungsaufzeichnungen in der Sitzungsaufzeichnungsdatenbank unter physischem Verschieben der Sitzungsaufzeichnungsdateien

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.

2. Rufen Sie eine Eingabeaufforderung auf.
3. Wechseln Sie vom aktuellen Arbeitsverzeichnis in das Bin-Verzeichnis des Sitzungsaufzeichnungsserver-Installationspfads (<Installationspfad>/Server/Bin).
4. Führen Sie den Befehl **ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /MOVETO:<directory> /NOTE:<note> /L** aus. **days** ist der Aufbewahrungszeitraum für Sitzungsaufzeichnungsdateien, **directory** ist das Verzeichnis, in das archivierte Sitzungsaufzeichnungsdateien verschoben werden, und **note** ist eine Textnotiz, die dem Datenbankdatensatz jeder archivierten Sitzungsaufzeichnungsdatei hinzugefügt wird. Geben Sie **Y** ein, um die Archivierung zu bestätigen.

Ausschließliches Archivieren von Sitzungsaufzeichnungen in der Sitzungsaufzeichnungsdatenbank

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.
2. Rufen Sie eine Eingabeaufforderung auf.
3. Wechseln Sie vom aktuellen Arbeitsverzeichnis in das Bin-Verzeichnis des Sitzungsaufzeichnungsserver-Installationspfads (<Installationspfad>/Server/Bin).
4. Führen Sie den Befehl **ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /NOTE:<note> /L** aus. **days** entspricht dem Aufbewahrungszeitraum für Sitzungsaufzeichnungen und **note** ist eine Textnotiz, die dem Datenbankdatensatz jeder archivierten Sitzungsaufzeichnung hinzugefügt wird. Geben Sie **Y** ein, um die Archivierung zu bestätigen.

Wiederherstellen von Sitzungsaufzeichnungsdateien

Sitzungsaufzeichnungsdateien müssen wiederhergestellt werden, wenn Sie eine Sitzungsaufzeichnung aufrufen möchten, die in der Sitzungsaufzeichnungsdatenbank unter Verschieben der Datei aus dem Speicherort der Aufzeichnung archiviert wurde. Archivierte Sitzungsaufzeichnungen, die nicht aus dem Speicherort der Aufzeichnung verschoben wurden, stehen im Sitzungsaufzeichnungsplayer weiterhin zur Verfügung.

Es gibt zwei Wiederherstellungsmethoden für Sitzungsaufzeichnungsdateien, die verschoben wurden. Kopieren der Sitzungsaufzeichnungsdatei in das Wiederherstellungsverzeichnis für archivierte Dateien, oder Reimportieren der Datei mithilfe von ICLDB in die Sitzungsaufzeichnungsdatenbank. Citrix empfiehlt das Kopieren. Entfernen Sie in das Wiederherstellungsverzeichnis kopierte archivierte Dateien, wenn Sie sie nicht mehr benötigen.

Der Sitzungsaufzeichnungsbroker verwendet das **Wiederherstellungsverzeichnis für archivierte Dateien**, wenn eine Sitzungsaufzeichnungsdatei nicht am ursprünglichen Speicherort gefunden wird.

Dies passiert, wenn der Sitzungsaufzeichnungsplayer eine Sitzungsaufzeichnungsdatei zur Wiedergabe anfordert. Der Sitzungsaufzeichnungsbroker sucht die Datei zunächst am ursprünglichen Speicherort. Wird sie dort nicht gefunden, überprüft der Sitzungsaufzeichnungsbroker das **Wiederherstellungsverzeichnis**. Befindet sich die Datei im Wiederherstellungsverzeichnis, sendet der Sitzungsaufzeichnungsbroker sie zur Wiedergabe an den Sitzungsaufzeichnungsplayer. Andernfalls sendet er eine Fehlermeldung an den Sitzungsaufzeichnungsplayer, dass die Datei nicht gefunden wurde.

Beim Importieren einer archivierten Sitzungsaufzeichnungsdatei mit ICLDB wird die Sitzungsaufzeichnungsdatenbank durch die in der Datei enthaltenen Sitzungsaufzeichnungsinformationen einschließlich des neuen Speicherpfads aktualisiert. Beim Importieren mit ICLDB werden Sitzungsaufzeichnungsdateien nicht an den ursprünglichen Speicherort ihrer Aufzeichnung zurückverschoben.

Hinweis: Bei importierten Sitzungsaufzeichnungsdateien werden die Uhrzeit der Archivierung und die Archivierungsnotiz gelöscht. Wenn Sie das nächste Mal den ICLDB-Archivierungsbefehl ausführen, können solche importierten Dateien daher wieder archiviert werden.

Der ICLDB-Befehl “import”eignet sich zum Importieren großer Zahlen archivierter Sitzungsaufzeichnungsdateien, zum Reparieren bzw. Aktualisieren falscher oder fehlender Sitzungsaufzeichnungsdaten in der Sitzungsaufzeichnungsdatenbank und zum Verschieben von Sitzungsaufzeichnungsdateien an einen anderen Speicherort auf dem Sitzungsaufzeichnungsserver. Der ICLDB-Befehl **import** kann auch verwendet werden, um die Sitzungsaufzeichnungsdatenbank wieder aufzufüllen, nachdem der Befehl **removeall** ausgeführt wurde.

Der ICLDB-Befehl **import** kann mit folgenden Parametern verwendet werden:

- **/LISTFILES:** vollständigen Pfad und Dateiname der Sitzungsaufzeichnungsdateien beim Import. Dieser Parameter ist optional.
- **/RECURSIVE:** durchsucht alle Unterverzeichnisse nach Sitzungsaufzeichnungsdateien. Dieser Parameter ist optional.
- **/L:** protokolliert Ergebnisse und Fehler in Verbindung mit den importierten Sitzungsaufzeichnungsdateien im Windows-Ereignisprotokoll. Dieser Parameter ist optional.
- **/F:** erzwingt die Ausführung des Importbefehls ohne Aufforderungen. Dieser Parameter ist optional.

Wiederherstellen von Sitzungsaufzeichnungsdateien unter Verwendung des Wiederherstellungsverzeichnisses für archivierte Dateien

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.

2. Sehen Sie im Sitzungsaufzeichnungsplayer unter “Eigenschaften”die Datei-ID und die Archivierungszeit der gewünschten Sitzungsaufzeichnungsdatei nach.
3. Suchen Sie die Sitzungsaufzeichnungsdatei anhand der Datei-ID in der Sicherung. Jede Sitzungsaufzeichnung hat einen Dateinamen im Format **i_<FileID>.icl**, wobei “FileID”die Datei-ID der Sitzungsaufzeichnungsdatei ist.
4. Kopieren Sie die Sitzungsaufzeichnungsdatei aus Ihrer Sicherung in das Wiederherstellungsverzeichnis für archivierte Dateien. Suchen des Wiederherstellungsverzeichnisses für archivierte Dateien

    a) Klicken Sie im Menü **Start** auf **Start** > **Programme** > **Citrix** > **Sitzungsaufzeichnungsserver - Eigenschaften**.

    b) Klicken Sie unter “Sitzungsaufzeichnungsserver - Eigenschaften”auf die Registerkarte **Speicher**. Das aktuelle Wiederherstellungsverzeichnis wird im Feld **Wählen Sie das Wiederherstellungsverzeichnis für archivierte Dateien aus** angezeigt.

Wiederherstellen von Sitzungsaufzeichnungsdateien mit dem ICLDB-Befehl “import”

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.
2. Rufen Sie eine Eingabeaufforderung auf.
3. Wechseln Sie vom aktuellen Arbeitsverzeichnis in das Bin-Verzeichnis des Sitzungsaufzeichnungsserver-Installationspfads (<Installationspfad>/Server/Bin).
4. Führen Sie einen der folgenden Schritte aus:

    - Führen Sie den Befehl **ICLDB IMPORT /LISTFILES /RECURSIVE /L <directory>** aus. **directory** steht für ein oder mehrere Verzeichnisse mit Sitzungsaufzeichnungsdateien. Mehrere Verzeichnisse trennen Sie durch Leerzeichen. Geben Sie **Y** ein, um den Import zu bestätigen.
    - Führen Sie **ICLDB IMPORT /LISTFILES /L <Datei>** aus. **Datei** ist der Name einer oder mehrerer Sitzungsaufzeichnungsdateien (Angabe mehrerer Dateien durch Leerzeichen getrennt). Platzhalterzeichen können beim Angeben Sitzungsaufzeichnungsdateien verwendet werden. Geben Sie **Y** ein, um den Import zu bestätigen.

Konfigurationsprotokollierung

August 18, 2021

Die Konfigurationsprotokollierung dient zum Erfassen der Sitekonfigurationsänderungen und Administratoraktivitäten in einer Datenbank. Sie können den protokollierten Inhalt folgendermaßen verwenden:

- Diagnose und Problembehandlung nach der Durchführung von Konfigurationsänderungen; das Protokoll liefert eine Breadcrumbspur.
- Hilfe beim Änderungsmanagement und der Nachverfolgung von Konfigurationen
- Bericht über Administratoraktivitäten

Zum Festlegen der Einstellungen für die Konfigurationsprotokollierung, zum Anzeigen der Konfigurationsprotokolle und zum Generieren von HTML- und CSV-Berichten verwenden Sie Citrix Studio. Sie können die Anzeige des Konfigurationsprotokolls durch Datumsbereiche und durch Ergebnisse der Volltextsuche filtern. Ist die verbindliche Protokollierung aktiviert, verhindert sie, dass Änderungen an der Konfiguration vorgenommen werden, es sei denn diese können protokolliert werden. Mit der entsprechenden Berechtigung können Sie Einträge aus dem Konfigurationsprotokoll löschen. Sie können das Feature der Konfigurationsprotokollierung nicht zum Bearbeiten des Inhalts von Protokollen verwenden.

Die Konfigurationsprotokollierung verwendet ein PowerShell-SDK und den Konfigurationsprotokollierungsdienst. Der Konfigurationsprotokollierungsdienst wird auf allen Controllern in der Site ausgeführt. Wenn ein Controller ausfällt, übernimmt automatisch der Dienst auf einem anderen Controller die Verarbeitung von Protokollanforderungen.

Standardmäßig ist die Konfigurationsprotokollierung aktiviert und verwendet die Datenbank, die zusammen mit der Site erstellt wurde (die Sitekonfigurationsdatenbank). Sie können einen anderen Speicherort für die Datenbank angeben. Die Konfigurationsprotokollierungsdatenbank unterstützt dieselben Features für hohe Verfügbarkeit wie die Sitekonfigurationsdatenbank.

Der Zugriff auf die Konfigurationsprotokollierung wird über die delegierte Administration mit den Einstellungen “Protokollierungseinstellungen bearbeiten”und “Konfigurationsprotokolle anzeigen”gesteuert.

Konfigurationsprotokolle werden bei der Erstellung lokalisiert. Beispiel: Ein in Englisch erstelltes Protokoll wird unabhängig vom Gebietsschema des Lesers in Englisch gelesen.

Gegenstand der Protokollierung

Konfigurationsänderungen und Administratoraktivitäten, die von Studio, Director und PowerShell-Skripts ausgehen, werden protokolliert. Beispiele protokollierter Konfigurationsänderungen sind Arbeiten (Erstellen, Bearbeiten, Löschen, Zuweisen) mit:

- Maschinenkataloge
- Bereitstellungsgruppen (einschließlich Ändern der Energieverwaltungseinstellungen)

- Administratorrollen und Geltungsbereiche
- Hostressourcen und Verbindungen
- Citrix Richtlinien über Studio

Beispiele protokollierter Administratoraktivitäten:

- Energieverwaltung für eine virtuelle Maschine oder einen Benutzerdesktop
- Senden einer Nachricht an einen Benutzer von Studio oder Director aus

Die folgenden Vorgänge werden nicht protokolliert:

- Autonome Vorgänge wie das Einschalten virtueller Maschinen per Poolverwaltung.
- Über die Gruppenrichtlinien-Verwaltungskonsole implementierte Richtlinienaktionen; verwenden Sie Microsoft-Tools, um Protokolle dieser Aktionen anzuzeigen.
- Über die Registrierung vorgenommene Änderungen, direkter Zugriff von der Datenbank oder von anderen Quellen als Studio, Director oder PowerShell.
- Wenn die Bereitstellung initialisiert wird, steht die Konfigurationsprotokollierung ab dem Zeitpunkt zur Verfügung, zu dem die erste Instanz des Konfigurationsprotokollierungsdiensts sich beim Konfigurationsdienst registriert. Daher werden die frühen Phasen der Konfiguration nicht protokolliert (z. B., wenn das Datenbankschema bei der Initialisierung eines Hypervisors abgerufen und angewendet wird).

Verwalten der Konfigurationsprotokollierung

Standardmäßig wird für die Konfigurationsprotokollierung die Datenbank verwendet, die zusammen mit einer Site erstellt wird (die Sitekonfigurationsdatenbank). Citrix empfiehlt aus folgenden Gründen, einen anderen Speicherort für die Konfigurationsprotokollierungsdatenbank und die Überwachungsdatenbank zu wählen:

- Die Backupstrategie für die Konfigurationsprotokollierungsdatenbank unterscheidet sich wahrscheinlich von der Backupstrategie für die Sitekonfigurationsdatenbank.
- Die Menge der für die Konfigurationsprotokollierung (und den Überwachungsdienst) gesammelten Daten kann den für die Sitekonfigurationsdatenbank verfügbaren Speicherplatz zu stark limitieren.
- Eine einzelne Fehlerquelle für die drei Datenbanken wird beseitigt (d. h. aufgeteilt).

Hinweis: Produkteditionen, die keine Konfigurationsprotokollierung unterstützen, haben keinen Knoten namens “Protokollierung”in Studio.

Aktivieren/Deaktivieren der Konfigurationsprotokollierung und der verbindlichen Protokollierung

Standardmäßig ist die Konfigurationsprotokollierung aktiviert und die verbindliche Protokollierung ist deaktiviert.

1. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
2. Wählen Sie im Aktionsbereich **Einstellungen** aus. Das Dialogfeld "Konfigurationsprotokollierung"enthält die Datenbankinformationen und Angaben dazu, ob Konfigurationsprotokollierung und verbindliche Protokollierung aktiviert oder deaktiviert sind.
3. Wählen Sie die gewünschte Aktion:

Zum Aktivieren der Konfigurationsprotokollierung wählen Sie das Optionsfeld **Aktivieren**. Dies ist die Standardeinstellung. Wenn nicht in die Datenbank geschrieben werden kann, werden die Informationen verworfen, der Vorgang wird jedoch fortgesetzt.

Zum Deaktivieren der Konfigurationsprotokollierung wählen Sie das Optionsfeld **Deaktivieren**. Wenn die Protokollierung zuvor aktiviert war, können bereits vorhandene Protokolle weiterhin mit dem PowerShell-SDK gelesen werden.

Zum Aktivieren der obligatorischen Protokollierung wählen Sie das Optionsfeld **Keine Änderungen der Sitekonfiguration ohne Datenbankzugriff**. Es wird dann keine Konfigurationsänderung oder administrative Aktivität, die normalerweise protokolliert würde, zugelassen, es sei denn, sie kann in die Konfigurationsprotokollierungsdatenbank geschrieben werden. Sie können die verbindliche Protokollierung nur aktivieren, wenn die Konfigurationsprotokollierung aktiviert ist, d. h. wenn das Optionsfeld **Aktivieren** für die Konfigurationsprotokollierung aktiviert ist. Tritt bei dem Dienst für die Konfigurationsprotokollierung ein Fehler auf, und die hohe Verfügbarkeit wird nicht verwendet, beginnt die verbindliche Protokollierung. In solchen Fällen werden Vorgänge, die normalerweise protokolliert würden, nicht ausgeführt.

Zum Deaktivieren der obligatorischen Protokollierung wählen Sie das Optionsfeld **Änderungen der Sitekonfiguration ohne Datenbankzugriff**. Konfigurationsänderungen und administrative Aktivitäten sind dann zulässig, selbst wenn kein Zugriff auf die Datenbank für die Konfigurationsprotokollierung besteht. Dies ist die Standardeinstellung.

Ändern des Speicherorts für die Konfigurationsprotokollierungsdatenbank

Hinweis: Sie können den Speicherort der Datenbank nicht ändern, wenn die verbindliche Protokollierung aktiviert ist, da bei der Standortänderung eine kurze Trennung verursacht wird, die nicht protokolliert werden kann.

1. Erstellen Sie einen Datenbankserver mit einer unterstützten SQL Server-Version.
2. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.

3. Wählen Sie im Aktionsbereich **Einstellungen** aus.
4. Klicken Sie im Dialogfeld "Protokollierungseinstellungen"auf **Protokollierungsdatenbank ändern**.
5. Geben Sie im Dialogfeld "Protokollierungsdatenbank ändern"den Speicherort des Servers mit dem neuen Datenbankserver ein. Gültige Formate sind unter Datenbanken aufgeführt.
6. Damit die Datenbank von Studio erstellt wird, klicken Sie auf **OK**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK** und die Datenbank wird automatisch erstellt. Studio versucht, mit den Anmeldeinformationen des aktuellen Studio-Benutzers auf die Datenbank zuzugreifen; wenn dies fehlschlägt, werden Sie zur Eingabe der Anmeldeinformationen des Datenbankbenutzers aufgefordert. Das Datenbankschema wird dann von Studio in die Datenbank hochgeladen. (Die Anmeldeinformationen werden nur während der Datenbankerstellung gespeichert.)
7. Zum manuellen Erstellen der Datenbank klicken Sie auf **Datenbankskript erstellen**. Das generierte Skript enthält Anweisungen zum manuellen Erstellen der Datenbank. Stellen Sie vor dem Hochladen des Schemas sicher, dass die Datenbank leer ist und dass mindestens ein Benutzer Zugriffs- bzw. Änderungsberechtigung für die Datenbank hat.

Die Daten der Konfigurationsprotokollierung aus der älteren Datenbank werden nicht in die neue Datenbank importiert. Die Protokolle beider Datenbanken können beim Abrufen von Protokollen nicht aggregiert werden. Der erste Protokolleintrag in der neuen Datenbank für die Konfigurationsprotokollierung gibt an, dass eine Datenbankänderung stattfand; die vorherige Datenbank wird jedoch nicht identifiziert.

Anzeigen des Konfigurationsprotokolls

Beim Initiieren von Konfigurationsänderungen und bei Verwaltungsaktivitäten werden die von Studio und Director bewirkten High-Level-Operationen im oberen mittleren Bereich von Studio angezeigt. Eine High-Level-Operation führt zu mindestens einem Dienst- und SDK-Aufruf, bei dem es sich um eine Low-Level-Operation handelt. Wenn Sie eine High-Level-Operation im oberen mittleren Bereich auswählen, werden im unteren mittleren Bereich die Low-Level-Operationen angezeigt.

Schlägt eine Operation vor der Beendigung fehl, kann die Protokollierung evtl. in der Datenbank nicht abgeschlossen werden, sodass z. B. ein Startdatensatz keinen entsprechenden Stoppdatensatz hat. In solchen Fällen wird im Protokoll angezeigt, dass Informationen fehlen. Wenn Sie Protokolle auf Zeitbereichsbasis anzeigen, werden unvollständige Protokolle angezeigt, wenn die Daten in den Protokollen mit den Kriterien übereinstimmen. Beispiel: Wenn alle Protokolle für die letzten fünf Tage angefordert werden und ein Protokoll eine in den letzten fünf Tagen gelegene Startzeit aber keine Endzeit hat, wird dieses ebenfalls angezeigt.

Wenn Sie bei Verwendung eines Skripts zum Aufrufen von PowerShell-Cmdlets eine Low-Level-Operation erstellen ohne die übergeordnete High-Level-Operation anzugeben, wird von der

Konfigurationsprotokollierung eine Ersatz-High-Level-Operation erstellt.

Zum Anzeigen des Inhalts des Konfigurationsprotokolls wählen Sie im Studio-Navigationsbereich **Protokollierung**. Standardmäßig wird im mittleren Bereich der Protokollinhalt chronologisch (neueste Einträge zuerst), angezeigt, wobei die Einträge durch das Datum getrennt sind.

Zum Filtern der Anzeige nach folgenden Kriterium	Führen Sie folgenden Schritt aus
Suchergebnisse	Geben Sie Text in das Feld "Suchen"oben im mittleren Bereich ein. Die gefilterte Anzeige enthält die Anzahl der Suchergebnisse. Um zur Standardanzeige der Protokollierung zurückzukehren, löschen Sie den Text im Feld "Suchen".
Spaltenüberschrift	Klicken Sie auf eine Spaltenüberschrift, um die Anzeige nach dem entsprechenden Feld zu sortieren.
Datumsbereich	Wählen Sie aus der Dropdownliste neben dem Feld "Suchen"oben im mittleren Bereich ein Intervall aus.

Erstellen von Berichten

Sie können CSV- und HTML-Berichte mit Konfigurationsprotokolldaten generieren.

- Der CSV-Bericht enthält alle Protokolldaten aus einem angegebenen Zeitintervall. Die hierarchischen Daten in der Datenbank werden in eine einzelne CSV-Tabelle vereinfacht. Kein Aspekt der Daten hat Vorrang in der Datei. Es wird keine Formatierung verwendet und keine Lesbarkeit angenommen. Die Datei (unter dem Namen "MyReport") enthält lediglich die Daten in einem allgemein verwendbaren Format. CSV-Dateien werden oft für die Archivierung oder als Datenquelle für ein Tool zur Bearbeitung von Berichten oder Daten (z. B. Microsoft Excel) verwendet.
- Der HTML-Bericht enthält Protokolldaten aus einem angegebenen Zeitintervall in lesbarem Format. Er bietet eine strukturierte Ansicht für die Prüfung auf Änderungen, durch die navigiert werden kann. Der HTML-Bericht umfasst zwei Dateien: Zusammenfassung und Details. Die Zusammenfassung enthält High-Level-Operationen mit Informationen zu Zeitpunkt, Auslöser und Ergebnis. Klicken Sie auf den Link Details neben jedem Vorgang, um zu den Low-Level-Operationen in der Detailsdatei zu navigieren, die zusätzliche Informationen bietet.

Zum Generieren eines Konfigurationsprotokollierungsberichts wählen Sie im Studio-Navigationsbereich **Protokollierung** und dann im Aktionsbereich **Benutzerdefinierten Bericht erstellen**.

- Wählen Sie den Datumsbereich für den Bericht.
- Wählen Sie das Berichtsformat: CSV, HTML oder beides.
- Navigieren Sie zu dem Speicherort, an dem der Bericht gespeichert werden soll.

Löschen des Konfigurationsprotokolls

Zum Löschen des Konfigurationsprotokolls müssen Sie über bestimmte Rechte der delegierten Administration und Berechtigungen für die SQL Server-Datenbank verfügen.

- **Delegierte Administration**: Sie müssen eine Rolle der delegierten Administration haben, mit der die Bereitstellungskonfiguration gelesen werden kann. Die integrierte Volladministratorrolle hat diese Berechtigung. Für eine benutzerdefinierte Rolle muss für die Kategorie "Andere Berechtigungen"*"Lesen"oder "Verwalten"aktiviert sein.

  Wenn Sie die Konfigurationsprotokolldaten vor dem Löschen sichern möchten, muss die benutzerdefinierte Rolle in der Kategorie der Protokollierungsberechtigungen Lese- oder Verwaltungsberechtigung haben.

- **SQL Server-Datenbank**: Sie müssen einen Anmeldenamen für SQL Server haben und zum Löschen von Datensätzen aus der Datenbank berechtigt sein. Dies kann mit zwei Möglichkeiten erreicht werden:

  - Verwenden Sie zur Anmeldung für die SQL Server-Datenbank die Serverrolle "sysadmin" , mit der Sie beliebige Aktivitäten auf dem Datenbankserver durchführen können. Auch die Serverrollen "serveradmin"oder "setupadmin"sind zum Löschen von Vorgängen berechtigt.
  - Wenn Ihre Bereitstellung zusätzliche Sicherheit erfordert, verwenden Sie Anmeldeinformationen einer anderen Rolle als "sysadmin", die einem Datenbankbenutzer zugeordnet sind, der zum Löschen von Datensätzen aus der Datenbank berechtigt ist.

    1. Erstellen Sie in SQL Server Management Studio eine SQL Server-Anmeldung mit einer anderen Serverrolle (nicht "sysadmin").
    2. Ordnen Sie diese Anmeldung einem Benutzer in der Datenbank zu; SQL Server erstellt automatisch einen Benutzer in der Datenbank mit dem gleichen Namen wie die Anmeldung.
    3. Geben Sie für die Datenbankrollen-Mitgliedschaft mindestens eines der Rollenmitglieder für den Datenbankbenutzer an: ConfigurationLoggingSchema_ROLE oder dbowner.

    Weitere Informationen finden Sie in der Dokumentation zu SQL Server Management Studio.

Löschen der Konfigurationsprotokolle:

1. Wählen Sie im Studio-Navigationsbereich **Protokollierung** aus.
2. Wählen Sie im Aktionsbereich **Protokolle löschen** aus.
3. Sie haben nun die Möglichkeit, vor dem Löschen ein Backup der Protokolle anzulegen. Wenn Sie eine Backupdatei erstellen, navigieren Sie zu dem Speicherort, an dem diese gespeichert werden soll. Das Backup wird als CSV-Datei erstellt.

Nach dem Löschen der Konfigurationsprotokolle wird das Löschen des Protokolls als erste Aktivität im leeren Protokoll erfasst. Dieser Eintrag enthält Details darüber, wann und von wem die Protokolle gelöscht wurden.

Ereignisprotokolle

January 25, 2021

Der folgenden Artikel enthält Beschreibungen der Ereignisse, die von XenApp- und XenDesktop-Diensten protokolliert werden können.

Die Informationen sind nicht vollständig, weitere Informationen zu Ereignissen enthalten die Artikel zu den einzelnen Features.

Citrix Brokerdienstereignisse (HTML)

Citrix FMA Service SDK-Ereignisse (HTML)

Citrix Konfigurationsdienstereignisse (HTML)

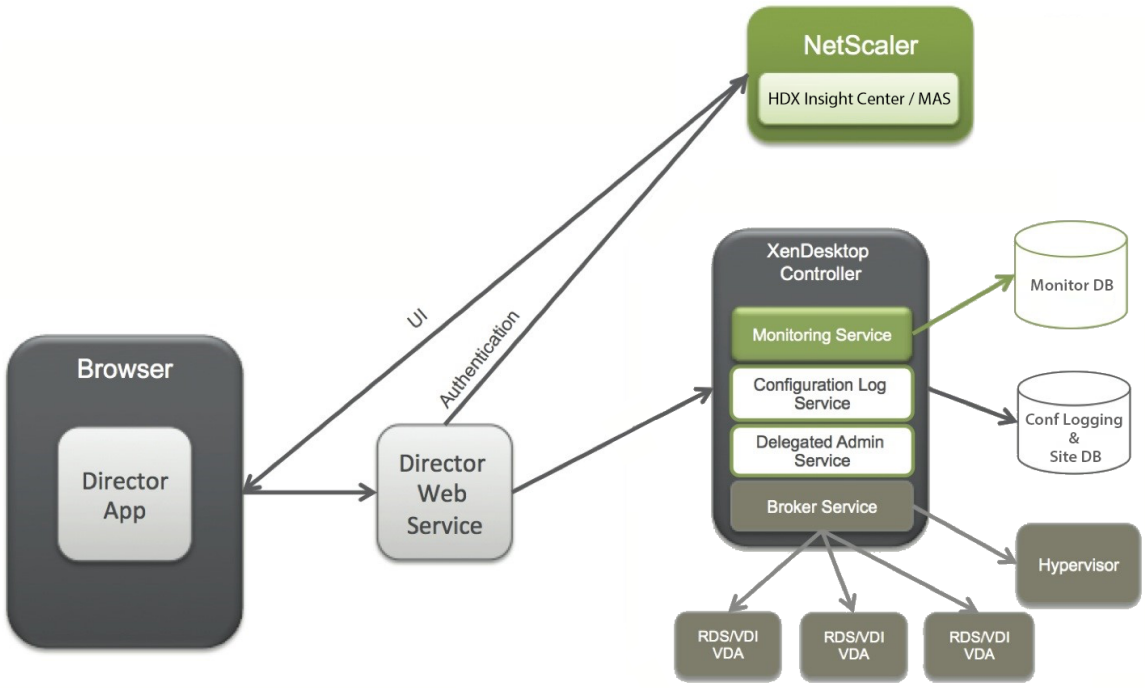
Citrix Delegated Administration Service-Ereignisse (HTML)

Director

August 18, 2021

Info über Director

Director ist eine Konsole zur Überwachung und Problembehandlung für XenApp und XenDesktop.



Director hat auf Folgendes Zugriff:

- Echtzeitdaten vom Brokeragent über eine einheitliche Konsole, die mit Analytics, Leistungsverwaltung und Netzwerkinspektion integriert ist.
  - Analytics umfasst Leistungsverwaltung zum Sicherstellen von Integrität und Kapazität, sowie historische Trends und Netzwerkanalysedaten (von NetScaler Insight Center oder NetScaler MAS) zum Identifizieren von Engpässen, die auf dem Netzwerk in der XenApp- oder XenDesktop-Umgebung beruhen.
- In der Überwachungsdatenbank gespeicherte historische Daten für den Zugriff auf die Datenbank für die Konfigurationsprotokollierung.
- ICA-Daten von NetScaler Gateway mit dem NetScaler Insight Center oder NetScaler MAS.
  - Übersicht über die Endbenutzererfahrung für virtuelle Anwendungen, Desktops und Benutzer in XenApp oder XenDesktop.
  - Korrelation von Netzwerkdaten mit Anwendungsdaten und Echtzeitmetrik für effektive Problembehandlung.
  - Integration mit dem Überwachungstool von XenDesktop 7 Director.
- Personal vDisk-Daten, die die Ausführungsüberwachung anhand von Basiszuordnung und Helpdesk-Administratoren das Zurücksetzen von Personal vDisks ermöglichen (nur im Notfall zu verwenden).
  - Das Befehlszeilentool CtxPvdDiag.exe wird zum Sammeln von Benutzerinformationen in einer Datei zur Problembehandlung verwendet.

Director hat ein Dashboard zur Problembehandlung, das die Echtzeitzustandsüberwachung der XenApp- oder XenDesktop-Site sowie die Prüfung historischer Zustandsdaten ermöglicht. Mit diesem Feature können Sie Fehler in Echtzeit sehen und einen besseren Eindruck von der Endbenutzererfahrung erhalten.

Weitere Informationen zur Kompatibilität von Director-Features mit Delivery Controller (DC), VDA und anderen abhängigen Komponenten finden Sie unter Featurekompatibilitätsmatrix.

Ansichten

Director bietet verschiedene Ansichten der Schnittstelle, die auf bestimmte Administratoren abgestimmt sind. Produktberechtigungen bestimmen, was angezeigt wird und welche Befehle verfügbar sind.

Beispiel: Helpdeskadministratoren sehen eine auf Helpdeskaufgaben abgestimmte Schnittstelle. Director ermöglicht Helpdeskadministratoren, nach dem Benutzer zu suchen, der das Problem gemeldet hat, und die diesem Benutzer zugeordneten Aktivitäten anzuzeigen, z. B. den Status der Anwendungen und Prozesse des Benutzers. So können Probleme schnell gelöst werden, indem Aktionen wie z. B. das Beenden einer nicht reagierenden Anwendung oder eines Prozesses, das Spiegeln von Vorgängen auf der Maschine des Benutzers, der Neustart der Maschine oder das Zurücksetzen des Benutzerprofils durchgeführt werden.

Im Gegensatz dazu sehen und verwalten Volladministratoren die gesamte Site und können Befehle für mehrere Benutzer und Maschinen ausführen. Das Dashboard bietet einen Überblick über die wichtigsten Aspekte einer Bereitstellung, z. B. den Status von Sitzungen und Benutzeranmeldungen und die Infrastruktur der Site. Die Informationen werden jede Minute aktualisiert. Wenn Probleme auftreten, werden automatisch Details zu Anzahl und Art der Fehler angezeigt.

Bereitstellen und Konfigurieren von Director

Director ist standardmäßig als Website auf dem Delivery Controller installiert. Informationen zu Voraussetzungen und anderen Details finden Sie in der Dokumentation zu den Systemanforderungen für dieses Release.

Dieses Release von Director ist nicht kompatibel mit XenApp-Bereitstellungen vor Version 6.5 und XenDesktop-Bereitstellungen vor Version 7.

Wenn Director in einer Umgebung mit mehreren Sites verwendet wird, synchronisieren Sie die Systemuhren auf allen Servern, auf denen Controller, Director und andere wichtige Kernkomponenten installiert sind. Ansonsten werden die Sites in Director möglicherweise nicht richtig angezeigt.

Tipp: Wenn Sie beabsichtigen, neben XenApp 7.5- und XenDesktop 7.x-Sites auch XenApp 6.5-Sites zu überwachen, empfiehlt Citrix, Director und die Director-Konsole, die zur Überwachung von XenApp

6.5-Sites verwendet wird, auf separaten Servern zu installieren.

Wichtig: Zum Schutz von als Nur-Text über das Netzwerk gesendeten Benutzernamen und Kennwörtern empfiehlt Citrix dringend, nur Director-Verbindungen mit HTTPS und nicht mit HTTP zuzulassen. Bestimmte Tools können Nur-Text-Benutzernamen und -Kennwörter in (unverschlüsselten) HTTP-Netzwerkpaketen lesen, wodurch ein Sicherheitsrisiko für Benutzer entstehen kann.

Konfigurieren von Berechtigungen

Um eine Anmeldung bei Director vornehmen zu können, müssen Administratoren mit den Berechtigungen für Director Active Directory-Domänenbenutzer sein und die folgenden Berechtigungen haben:

- Leseberechtigungen in allen zu durchsuchenden Active Directory-Gesamtstrukturen (siehe Erweiterte Konfiguration)
- Konfigurieren Sie die Rollen für "Delegierter Administrator"(siehe Delegierte Administration und Director)
- Zum Spiegeln von Benutzern muss für Administratoren eine Microsoft-Gruppenrichtlinie für Windows-Remoteunterstützung konfiguriert werden. Darüber hinaus gilt Folgendes:
  - Bei der Installation von VDAs stellen Sie sicher, dass die Windows-Remoteunterstützung auf allen Benutzergeräten aktiviert ist (standardmäßig aktiviert).
  - Wenn Sie Director auf einem Server installieren, stellen Sie sicher, dass die Windows-Remoteunterstützung installiert ist (standardmäßig ausgewählt). Allerdings ist sie auf dem Server standardmäßig deaktiviert. Das Feature muss für Director nicht aktiviert werden, um Benutzern zu helfen. Citrix empfiehlt, das Feature deaktiviert zu lassen, um die Sicherheit auf dem Server zu erhöhen.
  - Damit Administratoren die Windows-Remoteunterstützung initiieren können, müssen Sie ihnen mit den entsprechenden Einstellungen der Microsoft-Gruppenrichtlinie die Berechtigungen für die Remoteunterstützung erteilen. Informationen finden Sie unter CTX127388: How to Enable Remote Assistance for Desktop Director.
- Bei Benutzergeräten mit VDA-Versionen vor 7 ist eine zusätzliche Konfiguration erforderlich. Siehe Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7.

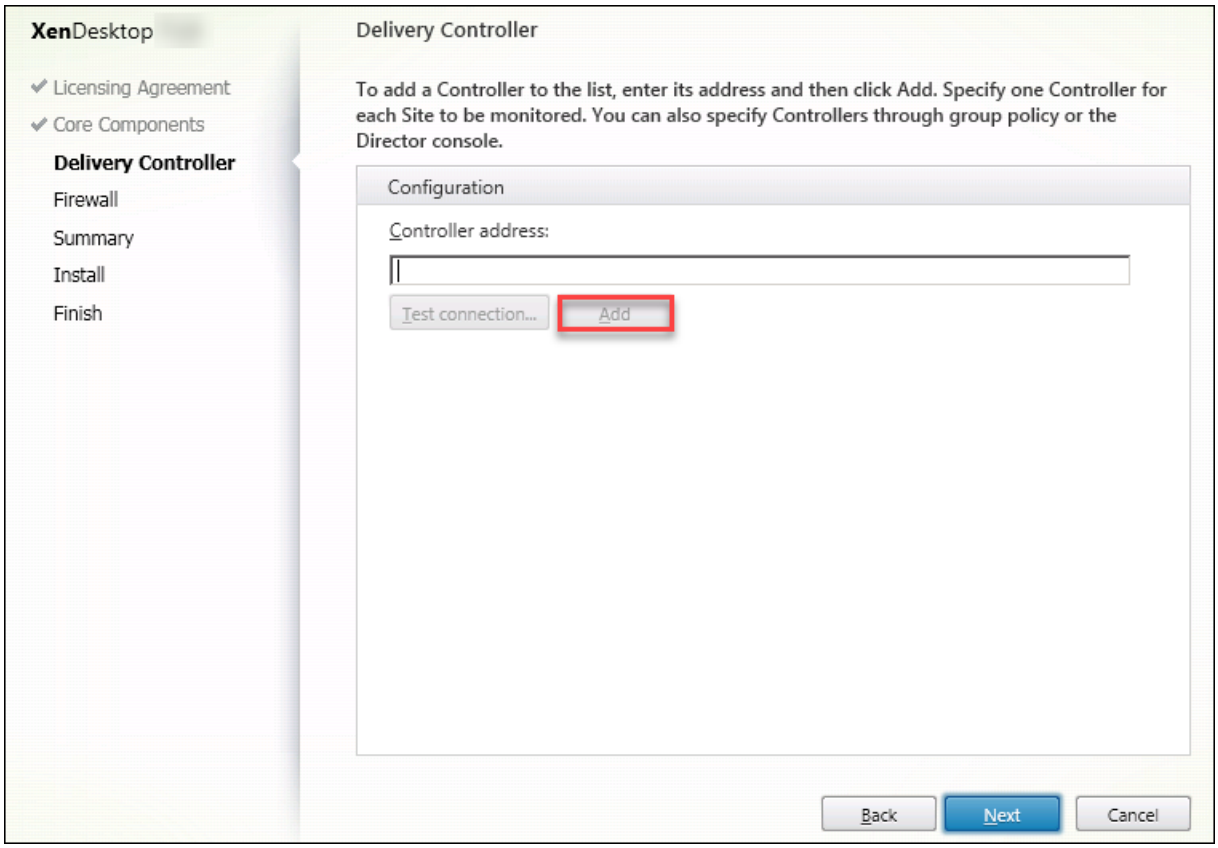
Installieren von Director

Installieren Sie Director mit dem ISO-Produktinstallationsprogramm für XenApp und XenDesktop. Dieses prüft, ob die Voraussetzungen erfüllt sind, installiert fehlende Komponenten, richtet die Director-Website ein und führt die Grundkonfiguration durch. Die Standardkonfiguration, die der ISO-Installer bietet, eignet sich für typische Bereitstellungen. Fügen Sie Director mit dem ISO-Installer

hinzu, falls dies während der Installation nicht geschehen ist. Zum Hinzufügen zusätzlicher Komponenten führen Sie den ISO-Installer erneut aus und wählen die zu installierenden Komponenten. Informationen zur Verwendung des ISO-Installers finden Sie in der Installationsdokumentation unter Installieren der Kernkomponenten. Citrix empfiehlt, dass Sie die Installation ausschließlich mit dem ISO-Installer des Produkts und nicht über die MSI-Datei durchführen.

Wenn Director auf dem Controller installiert ist, erfolgt automatisch eine Konfiguration mit "localhost" als Serveradresse und Director kommuniziert standardmäßig mit dem lokalen Controller.

Zur Installation von Director auf einem dedizierten, Controller-remoten Server werden Sie zur Eingabe des FQDN oder der IP-Adresse eines Controllers aufgefordert.



Hinweis: Klicken Sie auf **Hinzufügen**, um den Controller hinzuzufügen, der überwacht werden soll.

Director kommuniziert standardmäßig mit diesem angegebenen Controller. Geben Sie nur eine Controlleradresse für jede zu überwachende Site ein. Director ermittelt automatisch alle anderen Controller in derselben Site und wechselt zu diesen anderen Controllern, wenn der von Ihnen angegebene Controller ausfällt.

Hinweis: Director führt keinen Lastausgleich zwischen Controllern aus.

Citrix empfiehlt die Implementierung von TLS auf der IIS-Website, die Director hostet, um die Kommunikation zwischen dem Browser und dem Webserver zu schützen. In der Dokumentation

von Microsoft zu IIS finden Sie entsprechende Anweisungen. Zum Aktivieren von TLS ist keine Director-Konfiguration erforderlich.

Installieren von Director für XenApp 6.5

Führen Sie die folgenden Schritte aus, um Director für XenApp 6.5 zu installieren. In der Regel wird Director auf einem anderen Computer als die XenApp-Controller installiert.

1. Installieren Sie Director von dem XenApp-Installationsmedium. Wenn Director bereits für XenDesktop installiert ist, überspringen Sie diesen Schritt und fahren Sie mit dem nächsten Schritt fort.
2. Verwenden Sie die IIS-Verwaltungskonsole auf jedem Director-Server, um die Liste der XenApp-Serveradressen in den Anwendungseinstellungen zu aktualisieren (siehe Abschnitt **Hinzufügen von Sites zu Director** im Artikel Erweiterte Konfiguration).
   Geben Sie pro XenApp-Site die Serveradresse eines Controllers an: Die anderen Controller in einer XenApp-Site werden dann automatisch zum Failover verwendet. Director führt keinen Lastausgleich zwischen Controllern aus.
   Wichtig: Stellen Sie bei XenApp-Adressen sicher, dass Sie die Einstellung "Service.AutoDiscoveryAddressesX
   und nicht die Standardeinstellung "Service.AutoDiscoveryAddresses"verwenden.
3. Der Installer für den WMI Provider von Director ist auf der DVD im Ordner **Support\DirectorWMIProvider**. Installieren Sie ihn auf den jeweiligen XenApp-Servern (Controller und Worker, wenn Sitzungen ausgeführt werden).
   Wenn **winrm** nicht konfiguriert ist, führen Sie den Befehl **winrmqc** aus.
4. Konfigurieren Sie jeden XenApp-Workerserver für die Annahme von WinRM-Abfragen, wie unter Konfigurieren von Berechtigungen beschrieben.
5. Konfigurieren Sie eine Firewallausnahme für Port 2513, der für die Kommunikation zwischen Director und XenApp verwendet wird.
6. Citrix empfiehlt die Implementierung von TLS auf der IIS-Website, die Director hostet, um die Kommunikation zwischen dem Browser und dem Webserver zu schützen.
   In der Dokumentation von Microsoft zu IIS finden Sie entsprechende Anweisungen. Zum Aktivieren von TLS ist keine Director-Konfiguration erforderlich.

Hinweis: Damit Director alle XenApp-Worker in der Farm findet, müssen Sie eine Reverse-DNS-Zone für die Subnetze hinzufügen, in denen sich die XenApp-Server auf den von der Farm verwendeten DNS-Servern befinden.

Anmelden bei Director

Die Director-Website ist unter https oder `http://<ServerFQDN>/Director`.

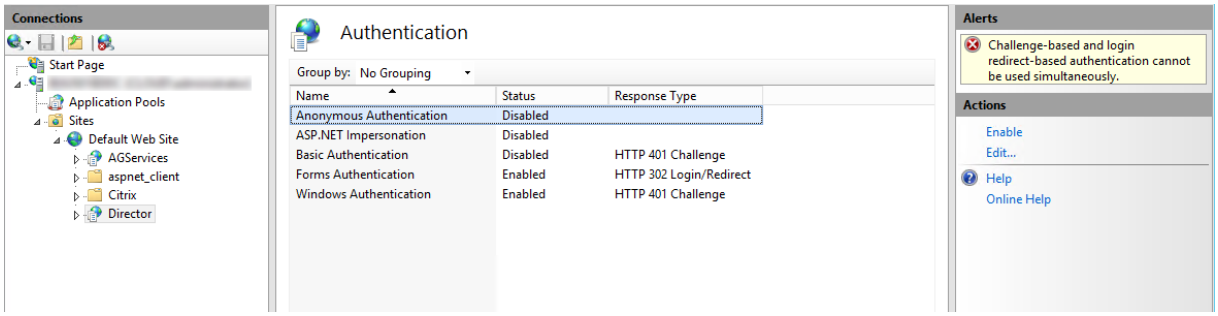
Wenn eine der Sites einer Bereitstellung mit mehreren Sites ausfällt, dauert die Anmeldung für Director etwas länger, während Verbindungsversuche mit dieser Site laufen.

Verwenden von Director mit der integrierten Windows-Authentifizierung

Mit der integrierten Windows-Authentifizierung erhalten in die Domäne eingebundene Benutzer direkten Zugriff auf Director, ohne ihre Anmeldeinformationen auf der Director-Anmeldeseite erneut eingeben zu müssen. Für die Verwendung der integrierten Windows-Authentifizierung mit Director gelten folgende Voraussetzungen:

- Die integrierte Windows-Authentifizierung muss auf der IIS-Website, die Director hostet, aktiviert werden. Bei der Installation von Director sind Formularauthentifizierung und anonyme Authentifizierung aktiviert. Zur Verwendung der integrierten Windows-Authentifizierung mit Director deaktivieren Sie die anonyme Authentifizierung und aktivieren Sie die Windows-Authentifizierung. Die Formularauthentifizierung muss für die Authentifizierung domänenexterner Benutzer aktiviert bleiben.

  1. Starten Sie IIS-Manager.
  2. Rufen Sie **Sites** > **Standardwebsite** > **Director** auf.
  3. Wählen Sie **Authentifizierung**.
  4. Klicken Sie mit der rechten Maustaste auf **Anonyme Authentifizierung** und wählen Sie **Deaktivieren**.
  5. Klicken Sie mit der rechten Maustaste auf **Windows-Authentifizierung** und wählen Sie **Deaktivieren**.



- Konfigurieren Sie die Active Directory-Delegierungsberechtigung für den Director-Computer. Dies ist nur erforderlich, wenn Director und Delivery Controller auf separaten Computern installiert sind.

  1. Öffnen Sie auf dem Active Directory-Computer die Active Directory-Verwaltungskonsole.
  2. Navigieren Sie in der Active Directory-Verwaltungskonsole zu **Domänenname** > **Computer**. Wählen Sie die Director-Maschine aus.
  3. Klicken Sie mit der rechten Maustaste und wählen Sie **Eigenschaften**.
  4. Wählen Sie die Registerkarte **Delegierung**.

5. Wählen Sie die Option **Computer bei Delegierungen aller Dienste vertrauen (nur Kerberos)**.

- Der Browser, der für den Zugriff auf Director verwendet wird, muss die integrierte Windows-Authentifizierung unterstützen. Dies erfordert möglicherweise zusätzliche Konfigurationsschritte in Firefox und Chrome. Weitere Informationen finden Sie in der Dokumentation zu dem Browser.
- Der Überwachungsdienst muss Microsoft .NET Framework 4.5.1 oder höher ausführen (unterstützte Versionen siehe Systemanforderungen für Director). Weitere Informationen finden Sie unter Systemanforderungen.

Wenn sich ein Benutzer von Director abmeldet oder ein Sitzungstimeout auftritt, wird die Anmeldeseite angezeigt. Auf der Anmeldeseite kann der Benutzer den Authentifizierungstyp **Automatische Anmeldung** oder **Benutzeranmeldeinformationen** einstellen.

Erfassung von Nutzungsdaten durch Google Analytics
Der Director-Dienst erfasst unter Einsatz von Google Analytics anonyme Nutzungsdaten nach der Installation. Es werden Statistiken und Informationen über die Nutzung der Seite "Trends"und zugehöriger Registerkarten gesammelt. Die Datenerfassung ist standardmäßig aktiviert, wenn Sie Director installieren.
Zum Beenden der Teilnahme an der Datenerfassung durch Google Analytics bearbeiten Sie den Registrierungsschlüssel "HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall"auf der Maschine mit Director (siehe "Analysedaten zu Installationen und Upgrades"unter Citrix Insight Services).

Hinweis: Der Registrierungsschlüssel HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall steuert die Sammlung von Nutzungsdaten durch Citrix Insight Services und Google Analytics. Änderungen an dem Schlüsselwert wirken sich auf die Datensammlung durch beide Dienste aus.

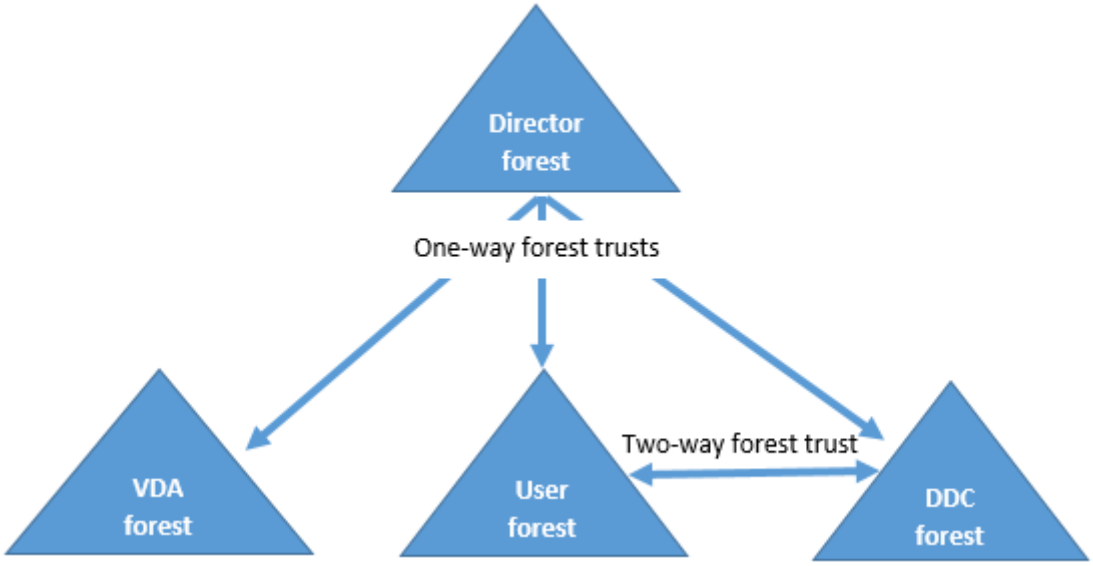
Erweiterte Konfiguration

August 18, 2021

Director unterstützt Umgebungen mit mehreren Gesamtstrukturen, in denen Benutzer, Domänen-Delivery Controller (DDC), VDAs und Directors in unterschiedlichen Gesamtstrukturen angesiedelt sind. Dies erfordert die Einrichtung entsprechender Vertrauensstellungen zwischen den Gesamtstrukturen und das Festlegen von Konfigurationseinstellungen.

Empfohlene Konfiguration für Director bei Einsatz in einer Umgebung mit mehreren Gesamtstrukturen

Die empfohlene Konfiguration erfordert die Erstellung ausgehender und eingehender Vertrauensstellungen zwischen den Gesamtstrukturen mit domänenweiter Authentifizierung.



Die Vertrauensstellung von Director ermöglicht Ihnen die Problembehandlung an Benutzersitzungen, VDAs und Domänencontrollern in unterschiedlichen Gesamtstrukturen.

Die erweiterte Director-Konfigurationen zur Unterstützung mehrerer Gesamtstrukturen wird über die Einstellungen im Internetinformationsdienste-Manager (IIS) festgelegt.

> **Wichtig:**
>
> Wenn Sie eine Einstellung in IIS ändern, wird der Director-Dienst automatisch neu gestartet und die Benutzer werden abgemeldet.

Konfigurieren von erweiterten Einstellungen mit IIS

1. Öffnen Sie die IIS-Verwaltungskonsole.
2. Wechseln Sie zur Director-Website unter der Standardwebsite.
3. Doppelklicken Sie auf **Anwendungseinstellungen**.
4. Doppelklicken Sie auf eine Einstellung, um diese zu bearbeiten.

Director sucht in Active Directory nach Benutzern und nach zusätzlichen Benutzer- und Maschineninformationen. Standardmäßig durchsucht Director die folgende Domäne oder Gesamtstruktur:

- In der das Konto des Administrators Mitglied ist
- In der der Director-Webserver Mitglied ist (falls unterschiedlich)

Director versucht, Suchen auf Gesamtstrukturebene mit dem globalen Active Directory-Katalog durchzuführen Wenn Sie keine Berechtigungen zum Suchen auf der Gesamtstrukturebene haben, wird nur die Domäne durchsucht.

Für die Suche nach Daten aus einer anderen Active Directory-Domäne oder Gesamtstrukturebene müssen Sie explizit die zu durchsuchenden Domänen oder Gesamtstrukturen festlegen. Konfigurieren Sie die folgenden Einstellungen:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

Die Werte der Attribute "Benutzer"und "Server"stellen die Domänen des Director-Benutzers (Administrator) bzw. des Director-Servers dar.

Um Suchen von einer zusätzlichen Domäne oder Gesamtstruktur zu ermöglichen, fügen Sie, wie in diesem Beispiel gezeigt, den Namen der Domäne der Liste hinzu:

```
Connector.ActiveDirectory.Domains = (user),(server),<domain1>,<domain2>
```

Director versucht, Suchen für jede Domäne in der Liste auf der Gesamtstrukturebene durchzuführen. Wenn Sie keine Berechtigungen zum Suchen auf der Gesamtstrukturebene haben, wird nur die Domäne durchsucht.

> **Hinweis:**
>
> In einer Umgebung mit mehreren Gesamtstrukturen zeigt Director nicht die Sitzungsdetails von Benutzern anderer Gesamtstrukturen an, die der XenDesktop-Bereitstellungsgruppe mit der lokalen Gruppe der Domäne zugewiesen wurden.

Hinzufügen von Sites zu Director

Wenn Director bereits installiert ist, richten Sie das Programm für die Funktion mit mehreren Sites ein. Verwenden Sie hierzu die IIS-Manager-Konsole auf jedem Director-Server zum Aktualisieren der Liste der Serveradressen in den Anwendungseinstellungen.

Fügen Sie folgender Einstellung die Adresse eines Controllers aus jeder Site hinzu:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAController und *SiteBController* sind die Adressen von Delivery Controllern aus zwei verschiedenen Sites.

Fügen Sie bei XenApp 6.5-Sites der folgenden Einstellung die Adresse eines Controllers aus jeder XenApp-Farm hinzu:

```
Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController
```


FarmAController und *FarmBController* sind die Adressen von XenApp-Controllern von zwei verschiedenen Farmen.

Dies ist eine weitere Methode für XenApp 6.5-Sites, einen Controller aus einer XenApp-Farm hinzuzufügen:

```
DirectorConfig.exe /xenapp FarmControllerName
```

Deaktivieren der Sichtbarkeit von ausgeführten Anwendungen im Aktivitätsmanager

Standardmäßig wird im Aktivitätsmanager von Director eine Liste aller in einer Benutzersitzung ausgeführten Anwendungen angezeigt. Diese Informationen können von allen Administratoren angezeigt werden, die Zugriff auf den Aktivitätsmanager in Director haben. Bei delegierten Administratorrollen sind dies Volladministratoren, Bereitstellungsgruppenadministratoren und Helpdeskadministratoren.

Zum Datenschutz für Benutzer und die von ihnen ausgeführten Anwendungen können Sie die Auflistung der ausgeführten Anwendungen auf der Registerkarte Anwendungen deaktivieren.

> **Warnung:**
>
> Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. Ändern Sie für den VDA den Registrierungsschlüssel in HKEY_LOCAL_MACHINE\Software\Citrix\Director\Task
   Standardmäßig ist dieser Schlüssel auf 1 eingestellt. Ändern Sie den Wert auf 0, was bedeutet, dass die Informationen nicht vom VDA gesammelt und daher auch nicht im Aktivitätsmanager angezeigt werden.
2. Bearbeiten Sie auf dem Server, auf dem Director installiert ist, die Einstellung zur Steuerung der Sichtbarkeit ausgeführter Anwendungen. In der Standardeinstellung ist der Wert “Wahr” , wodurch die Sichtbarkeit der ausgeführten Anwendungen auf der Registerkarte Anwendungen zugelassen wird. Ändern Sie den Wert in “false”, wodurch die Sichtbarkeit deaktiviert wird. Diese Option gilt nur für den Aktivitätsmanager in Director, nicht für den VDA.

   Ändern Sie den Wert der folgenden Einstellung:

   ```
   UI.TaskManager.EnableApplications = false
   <!--NeedCopy-->
   ```

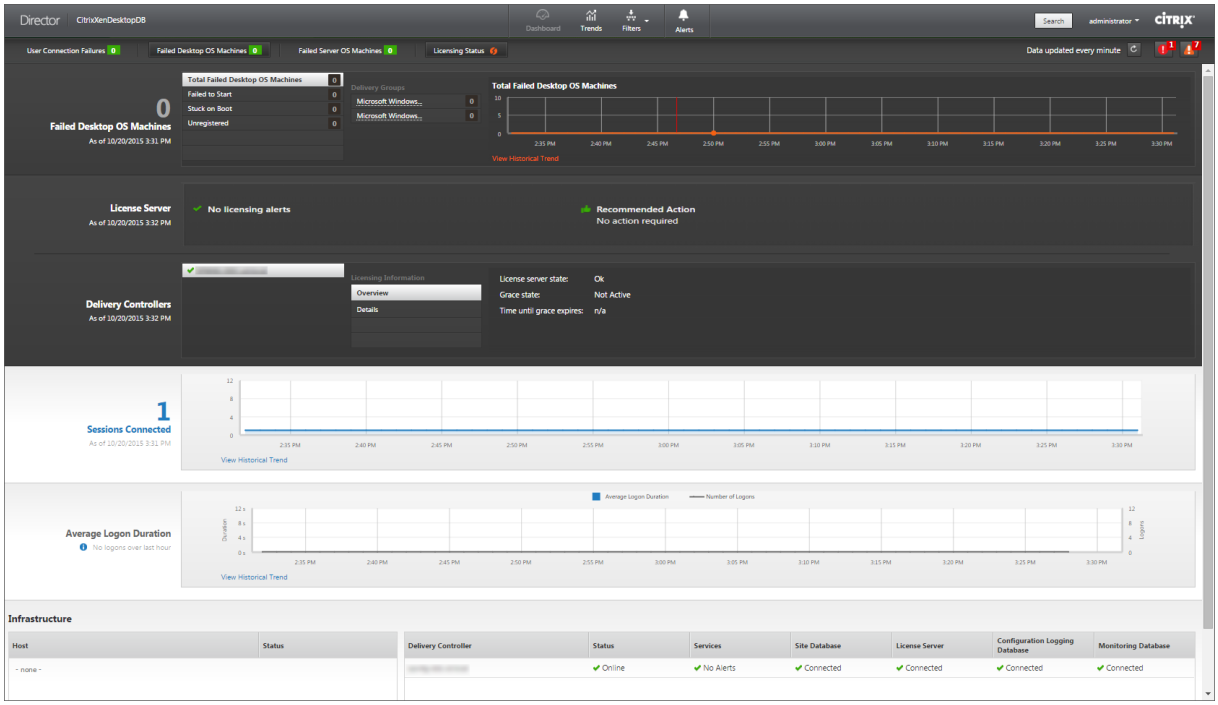

> **Wichtig:**
>
> Zum Deaktivieren der Ansicht ausgeführter Anwendungen empfiehlt Citrix, dass beide Änderungen durchgeführt werden, damit die Daten im Aktivitätsmanager nicht angezeigt werden.

Überwachen von Bereitstellungen

August 18, 2021

Überwachen von Sites

Wenn Sie Director mit Volladministratorrechten öffnen, erscheint das Dashboard zur Überwachung der Integrität und Nutzung einer Site.



Wenn es zurzeit keine Fehler gibt und keine Fehler in den letzten 60 Minuten aufgetreten sind, bleiben Bereiche ausgeblendet. Wenn Fehler auftreten, wird der zugehörige Fehlerbereich automatisch angezeigt.

Hinweis: Je nachdem, über welche Lizenz Ihre Organisation verfügt und welche Administratorrechte vorliegen, stehen einige Optionen oder Features möglicherweise nicht zur Verfügung.

Bereich	Beschreibung
Benutzerverbindungsfehler	Verbindungsfehler während der letzten 60 Minuten. Klicken Sie auf die Kategorien neben der Gesamtzahl zum Anzeigen von Metriken für diesen Fehlertyp. In der nebenstehenden Tabelle wird angezeigt, wie sich dieser Wert auf die Bereitstellungsgruppen verteilt. Verbindungsfehler umfassen auch solche, die aufgrund von Anwendungslimits auftreten. Weitere Informationen zu Anwendungslimits finden Sie unter Anwendungen.
Fehlgeschlagene Desktopbetriebssystemmaschinen bzw. Fehlgeschlagene Serverbetriebssystemmaschinen	Gesamtanzahl der Fehler in den letzten 60 Minuten unterteilt nach Bereitstellungsgruppen. Fehler unterteilt nach Typ, einschließlich “konnte nicht gestartet werden”, “beim Starten hängen geblieben”und “nicht registriert”. Bei Serverbetriebssystemmaschinen wird auch das Erreichen der maximalen Last angegeben.
Lizenzierungsstatus	Lizenzserverwarnungen werden vom Lizenzserver gesendet und enthalten Informationen zu den zur Problembeseitigung erforderlichen Aktionen. Erfordert Lizenzserver 11.12.1 oder höher. Delivery Controller-Warnungen enthalten vom Controller erfasste Zustandsangaben zur Lizenzierung und werden vom Controller gesendet. Erfordert Controller für XenApp 7.6 oder XenDesktop 7.6 oder höher. Sie können den Schwellenwert für Warnungen in Studio festlegen.
Verbundene Sitzungen	Verbunden Sitzungen in allen Bereitstellungsgruppen in den letzten 60 Minuten.

Bereich	Beschreibung
Durchschnittliche Anmeldedauer	Anmeldedaten für die letzten 60 Minuten. Die große Zahl links ist die durchschnittliche Anmeldedauer während einer Stunde. Anmeldedaten für VDAs vor XenDesktop 7.0 sind nicht in diesem Durchschnitt enthalten. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.
Infrastruktur	Liste der zu der Siteinfrastruktur gehörigen Hosts und Controller. Auf XenServer oder VMware können für die Infrastruktur Leistungswarnungen angezeigt werden. Sie können beispielsweise XenCenter so konfigurieren, dass Warnungen zur Leistung generiert werden, wenn die CPU-, Netzwerk-E/A- oder Datenträger-E/A-Nutzung einen angegebenen Schwellenwert auf einem verwalteten Server oder einer virtuellen Maschine übersteigt. Standardmäßig ist das Warnungswiederholungsintervall 60 Minuten, Sie können jedoch auch eine andere Einstellung wählen. Weitere Informationen finden Sie unter XenServer Current Release und im Abschnitt "XenCenter Performance Alerts"des Handbuchs "Citrix XenServer Administrator's Guide".

Hinweis: Wird für eine bestimmte Metrik kein Symbol angezeigt, bedeutet dies, dass die Metrik von dem verwendeten Hosttyp nicht unterstützt wird. Beispiel: Für System Center Virtual Machine Manager-, AWS- und CloudStack-Hosts sind keine Integritätsdaten verfügbar.

Fahren Sie mit dem Beheben von Problemen mit den folgenden Optionen (Erläuterung siehe weiter unten) fort:

- Steuern der Energiezustände von Benutzermaschinen
- Verhindern von Verbindungen mit Maschinen

Überwachen von Sitzungen

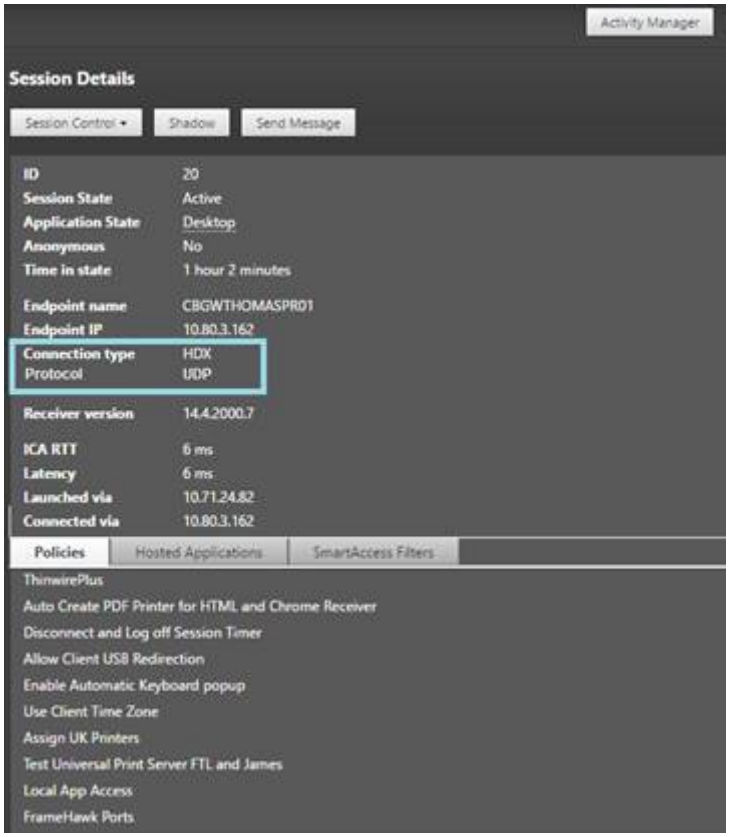
Wenn eine Sitzung getrennt wird, bleibt sie aktiv und die Anwendungen werden weiter ausgeführt, das Benutzergerät kommuniziert jedoch nicht mehr mit dem Server.

Aktion	Beschreibung
Anzeigen einer zurzeit verbundenen Maschine oder Sitzung des Benutzers	Mit den Ansichten Aktivitäts-Manager und Benutzerdetails zeigen Sie die aktuell verbundene Maschine oder Sitzung des Benutzers an und eine Liste aller Maschinen und Sitzungen, auf die dieser Benutzer zugreifen kann. Klicken Sie auf das Symbol zum Sitzungswechsel in der Titelleiste des Benutzers, um auf diese Liste zuzugreifen. Weitere Informationen finden Sie unter Wiederherstellen von Sitzungen.
Anzeigen der Gesamtanzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen	Rufen Sie über das Dashboard im Bereich Verbundene Sitzungen die Gesamtzahl der verbundenen Sitzungen in allen Bereitstellungsgruppen während der letzten 60 Minuten auf. Wenn Sie anschließend auf die Gesamtzahl klicken, wird die Ansicht Filter angezeigt, in der Sie die grafischen Sitzungsdaten basierend auf ausgewählten Bereitstellungsgruppen und Bereichen und Nutzung von Bereitstellungsgruppen anzeigen.
Beenden von Sitzungen im Leerlauf	Die Filteransicht “Sitzungen”enthält Daten für alle aktiven Sitzungen. Sie können die Sitzungen basierend auf dem zugeordneten Benutzer, der Bereitstellungsgruppe, dem Sitzungszustand und der Überschreitung des Leerlauflimits filtern. Wählen Sie aus der gefilterten Liste Sitzungen zum Abmelden oder Trennen. Weitere Informationen finden Sie unter Problembehandlung bei Anwendungen.

Aktion	Beschreibung
Anzeigen der Daten über einen längeren Zeitraum	Wählen Sie in der Ansicht “Trends”die Registerkarte Sitzungen für einen Drilldown auf spezifische Nutzungsdaten für verbundene und getrennte Sitzungen über einen längeren Zeitraum (d. h. Zahlen für Zeiträume vor den letzten 60 Minuten). Klicken Sie zum Anzeigen dieser Informationen auf **Verlaufstrends anzeigen**.

Hinweis: Wenn auf dem Benutzergerät eine ältere Virtual Delivery Agent-Version ausgeführt wird, z. B. eine VDA-Version vor 7 oder ein VDA für Linux, kann Director keine vollständigen Sitzungsinformationen anzeigen. Stattdessen wird gemeldet, dass die Informationen nicht verfügbar sind.

Das Transportprotokoll für den HDX-Verbindungstyp der aktuellen Sitzung können Sie im Bereich Sitzungsdetails ansehen. Diese Informationen sind für Sitzungen verfügbar, die auf VDAs ab Version 7.13 gestartet wurden.



- **HDX**-Verbindungen:

  - Als Protokoll wird **UDP** angezeigt, wenn EDT für die HDX-Verbindung verwendet wird.
  - Als Protokoll wird **TCP** angezeigt, wenn TCP für die HDX-Verbindung verwendet wird.

- Für **RDP**-Verbindungen wird als Protokoll **Nicht zutreffend** angezeigt.

Wenn der adaptive Transport konfiguriert ist, wechselt das Sitzungstransportprotokoll basierend auf den Netzwerkbedingungen dynamisch zwischen EDT (über UDP) und TCP. Kann die HDX-Sitzung nicht über EDT hergestellt werden, erfolgt ein Fallback auf TCP.

Informationen zum adaptiven Transport und seiner Konfiguration finden Sie unter Adaptiver Transport.

Filtern von Daten zur Problembehandlung

Wenn Sie auf Zahlen im Dashboard klicken oder im Filtermenü einen vordefinierten Filter auswählen, wird die Ansicht "Filter"geöffnet und zeigt Daten für die ausgewählte Maschine oder den Fehlertyp an.

Vordefinierte Filter können nicht bearbeitet werden. Sie können einen vordefinierten Filter jedoch als benutzerdefinierten Filter speichern und dann bearbeiten. Sie können auch benutzerdefinierte Ansichten mit Filter für Maschinen, Verbindungen, Sitzungen und Anwendungsinstanzen für alle Bereitstellungsgruppen erstellen.

1. Wählen Sie eine Ansicht aus:

   - **Maschinen**. Wählen Sie Desktopbetriebssystemmaschinen oder Serverbetriebssystemmaschinen. Diese Ansicht zeigt die Anzahl der konfigurierten Computer. Die Registerkarte "Server-OS-Maschinen"enthält auch den Lastauswertungsprogrammindex, der die Verteilung der Leistungsindikatoren und Quickinfo der Sitzungsanzahl angibt, wenn Sie mit dem Mauszeiger auf den Link zeigen.
   - **Sitzungen**. Sie können die Sitzungsanzahl auch in der Ansicht "Sitzungen"anzeigen. Anhand der Leerlaufmessung können Sie Sitzungen suchen, die länger als der vorgegebene Schwellenwert im Leerlauf sind.
   - **Verbindungen**. Filtern Sie Verbindungen nach verschiedenen Zeiträumen, u. a. die letzten 60 Minuten, die letzten 24 Stunden, oder die letzten 7 Tage.
   - **Anwendungsinstanzen**. Diese Ansicht zeigt die Eigenschaften aller Anwendungsinstanzen auf VDAs für Server- und Desktopbetriebssysteme. Die Sitzungsleerlaufzeiten stehen für Anwendungsinstanzen auf Serverbetriebssystem-VDAs zur Verfügung.

2. Wählen Sie für **Filtern nach** das Kriterium aus.
3. Verwenden Sie die zusätzlichen Registerkarten für jede Ansicht ggf. zum Abschließen des Filters.
4. Wählen Sie zusätzliche Spalten bei Bedarf aus, um weitere Fehler zu beheben.
5. Speichern und benennen Sie den Filter.

6. Für den Zugriff auf Filter von mehreren Director-Servern speichern Sie die Filter in einem freigegebenen, für die Server zugänglichen Ordner:
   - Der freigegebene Ordner muss Berechtigung zum Ändern von Konten auf dem Director-Server haben.
   - Die Director-Server müssen für den Zugriff auf den freigegebenen Ordner konfiguriert sein. Führen Sie hierfür **IIS-Manager** aus. Ändern Sie unter **Sites > Standardwebsite > Director > Anwendungseinstellungen** die Einstellung **Service.UserSettingsPath** auf den UNC-Pfad des freigegebenen Ordners.
7. Wenn Sie den Filter später öffnen möchten, wählen Sie im Menü Filter den Filtertyp (Maschinen, Sitzungen, Verbindungen oder Anwendungsinstanzen) und dann den gespeicherten Filter.
8. Verwenden Sie u. U. für die Ansichten **Maschinen** oder **Verbindungen** Energiesteuerelemente für alle in der gefilterten Liste ausgewählten Maschinen. Verwenden Sie in der Ansicht Sitzungen die Sitzungssteuerelemente oder die Option zum Senden von Nachrichten.
9. Klicken Sie in den Ansichten **Maschinen** und **Verbindungen** für fehlerhafte Maschinen oder Verbindungen auf **Fehlerursache**, um eine detaillierte Beschreibung des Fehlers und Empfehlungen zur Behebung aufzurufen. Informationen zu Ursachen von Maschinen- und Verbindungsfehlern sowie empfohlene Korrekturmaßnahmen finden Sie in dem Handbuch Citrix Director 7.12 Failure Reasons Troubleshooting Guide.
10. Klicken Sie in der Ansicht **Maschinen** auf Link mit dem Maschinennamen, um die zugehörige Seite **Maschinendetails** aufzurufen. Die Seite enthält Details zur Maschine, Optionen zur Energiesteuerung und Diagramme zur Überwachung von CPU, Arbeitsspeicher, Festplattenüberwachung und GPU. Durch Klicken auf **Historische Auslastung anzeigen** können Sie Ressourcenauslastungstrends für die Maschine aufrufen. Weitere Informationen finden Sie unter Problembehandlung bei Maschinen.
11. In der Ansicht **Anwendungsinstanzen** können Sie die Instanzen basierend auf der **Leerlaufzeit**, die einen Schwellenwert überschreitet, sortieren und filtern. Wählen Sie die Anwendungsinstanzen im Leerlauf aus, die Sie beenden möchten. Durch Abmelden oder Trennen einer Anwendungsinstanz werden alle aktiven Anwendungsinstanzen in derselben Sitzung beendet. Weitere Informationen finden Sie unter Problembehandlung bei Anwendungen.
    Hinweis: Die Seite zum Filtern von Anwendungsinstanzen und die Leerlaufzeitmessungen auf der Seite zum Filtern von Sitzungen stehen zur Verfügung, wenn Director, Delivery Controller und VDAs in der Version 7.13 oder höher vorliegen.

Siteübergreifendes Überwachen von Verlaufstrends

In der Ansicht "Trends"werden Verlaufstrenddaten für Sitzungen, Verbindungsfehler, Maschinenfehler, Anmeldeleistung, Lastauswertung, Kapazitätsverwaltung und Maschinen- und Ressourcenauslastung sowie eine Netzwerkanalyse für jede Site angezeigt. Sie finden diese Informationen im Menü **Trends**.

Das Vergrößerungsfeature beim Drilldown ermöglicht Ihnen das Navigieren durch Trenddiagramme, indem Sie bestimmte Zeiträume vergrößern (durch Klicken auf einen Datenpunkt im Diagramm) und die Detailinformationen zum Trend anzeigen. Durch dieses Feature können Sie die genauen Auswirkungen der angezeigten Trends besser verstehen.

Wenden Sie einen anderen Filter auf die Daten an, um den Standardgeltungsbereich der einzelnen Diagramme zu ändern.

Wählen Sie einen Zeitraum für die historischen Trenddaten. Welche Optionen zur Verfügung stehen, hängt von Ihrer Director-Bereitstellung ab:

- Trendberichte über das letzte Jahr (365 Tage) stehen in Sites mit Platinum-Lizenz zur Verfügung.
- Trendberichte über den letzten Monat (31 Tage) stehen in Sites mit Enterprise-Lizenz zur Verfügung.
- Trendberichte über die letzten 7 Tage stehen in Editionen mit einer anderen Lizenz als Enterprise und Platinum zur Verfügung.

Hinweis:

- In allen Director-Bereitstellungen stehen Informationen zu Sitzungen, Fehlern und Anmeldungsleistungstrends in Form von Diagrammen und Tabellen zur Verfügung, wenn Sie den Zeitraum auf den letzten Monat (**der jetzt endet**) oder kürzer festlegen. Wenn Sie den Zeitraum auf "Letzter Monat"mit einem benutzerdefinierten Enddatum oder auf das letzte Jahr festlegen, werden die Trendinformationen nur in Form von Diagrammen angezeigt.
- Die Standardwerte der Granularität und Aufbewahrung von Trenddaten für den Überwachungsdienst finden Sie im Abschnitt Datengranularität und -aufbewahrung. In Sites mit Platinum-Lizenz kann der gewünschte Aufbewahrungszeitraum in Tagen festgelegt werden.

Verfügbare Trends

Trends für Sitzungen anzeigen: Wählen Sie auf der Registerkarte "Sitzungen"die Bereitstellungsgruppe und den Zeitraum aus, um weitere Informationen zur Anzahl gleichzeitiger Sitzungen anzuzeigen.

Trends für Verbindungsfehler anzeigen: Wählen Sie auf der Registerkarte "Fehler"die Verbindung, den Maschinentyp, den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum, um weitere Informationen über die Verbindungsfehler der Site anzuzeigen.

Trends für Maschinenfehler anzeigen: Wählen Sie auf der Registerkarte "Desktopbetriebssystemmaschinenfehler"bzw. "Serverbetriebssystemmaschinen"den Fehlertyp, die Bereitstellungsgruppe und den Zeitraum, um weitere Informationen über die Maschinenfehler der Site anzuzeigen.

Trends für die Anmeldeleistung anzeigen: Wählen Sie auf der Registerkarte "Anmeldeleistung"die Bereitstellungsgruppe und den Zeitraum, um ein Diagramm mit ausführlichen Informationen über

die Dauer der Benutzeranmeldungen bei der Site und wie sich die Anzahl der Anmeldungen auf die Leistung auswirkt, anzuzeigen. In dieser Ansicht wird auch die durchschnittliche Dauer der Anmeldephasen angezeigt, u. a. Vermittlungsdauer und VM-Startzeit.
Diese Daten beziehen sich speziell auf Benutzeranmeldungen und nicht auf Benutzer, die sich mit getrennten Sitzungen wieder verbinden.
Die Tabelle unterhalb des Diagramms zeigt die Anmeldedauer nach Benutzersitzung. Sie können die Spalten für die Anzeige auswählen und den Bericht nach einer beliebigen Spalte sortieren.
Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.

Trends für die Lastauswertung anzeigen: Auf der Registerkarte "Lastauswertungsindex"zeigen Sie ein Diagramm an, das ausführliche Informationen zur Last enthält, die auf die Serverbetriebssystemmaschinen verteilt ist. Als Filteroptionen für dieses Diagramm stehen Bereitstellungsgruppe oder Serverbetriebssystemmaschine in einer Bereitstellungsgruppe, Serverbetriebssystemmaschine (nur bei Auswahl von Serverbetriebssystemmaschine in einer Bereitstellungsgruppe) und Bereich zur Verfügung.

Anzeigen der Verwendung gehosteter Anwendungen: Die Verfügbarkeit dieses Features hängt von der Lizenz ab.
Wählen Sie auf der Registerkarte "Kapazitätsverwaltung"die Registerkarte "Verwendung gehosteter Anwendungen"und dann die Bereitstellungsgruppe und den Zeitraum, um eine Kurve der höchsten gleichzeitigen Nutzung sowie eine Tabelle mit der anwendungsbasierten Verwendung anzuzeigen. In der Tabelle "Anwendungsbasierte Verwendung"können Sie eine bestimmte Anwendung auswählen, um Details und eine Liste der Benutzer anzuzeigen, die die Anwendung verwenden oder verwendet haben.

Anzeigen der Nutzung von Desktop- und Serverbetriebssystem: In der Ansicht "Trends"wird die Desktopbetriebssystemnutzung nach Site und Bereitstellungsgruppe angezeigt. Wenn Sie Site wählen, wird die Nutzung nach Bereitstellungsgruppe angezeigt. Wenn Sie "Bereitstellungsgruppe" wählen, wird die Nutzung nach Benutzer angezeigt.
In der Ansicht "Trends"wird außerdem die Serverbetriebssystemnutzung nach Site, Bereitstellungsgruppe und Maschine angezeigt. Wenn Sie Site wählen, wird die Nutzung nach Bereitstellungsgruppe angezeigt. Wenn Sie "Bereitstellungsgruppe"wählen, wird die Nutzung nach Maschine und nach Benutzer angezeigt. Wenn Sie "Maschine"wählen, wird die Nutzung nach Benutzer angezeigt.

Anzeigen der Verwendung virtueller Maschinen: Wählen Sie auf der Registerkarte "Maschinennutzung"die Option "Desktopbetriebssystemmaschinen"oder "Serverbetriebssystemmaschinen", um einen Überblick über die Nutzung der VMs in Echtzeit zu erhalten, sodass Sie den Kapazitätsbedarf der Site schnell einschätzen können.
Verfügbarkeit der Desktopbetriebssysteme: zeigt den aktuellen Zustand der Desktopbetriebssystemmaschinen (VDIs) nach Verfügbarkeit für die gesamte Site oder für eine bestimmte Bereitstellungsgruppe an.
Verfügbarkeit der Serverbetriebssysteme: zeigt den aktuellen Zustand der Serverbetriebssystem-

maschinen nach Verfügbarkeit für die gesamte Site oder für bestimmte Bereitstellungsgruppen an.

Anzeigen der Ressourcennutzung: Zur Vereinfachung der Kapazitätsplanung wählen Sie auf der Registerkarte "Ressourcenauslastung"die Option "Desktopbetriebssystemmaschinen"oder "Serverbetriebssystemmaschinen", um historische Trends zur CPU- und Arbeitsspeicherauslastung, IOPS und Datenträgerlatenz der einzelnen VDI-Maschine anzuzeigen.
Für dieses Feature sind Director und Delivery Controller ab **Version 7.11** erforderlich.
Die Daten für die Parameter "Durchschnittliche CPU", "Speicherdurchschnitt", "Durchschnittliche IOPS", "Datenträgerlatenz"und "Max. gleichzeitiger Sitzungen"werden in Form von Diagrammen dargestellt. Sie können einen Drilldown für die einzelnen Maschinen ausführen, um Daten und Diagramme für die 10 Prozesse mit der höchsten CPU-Auslastung anzuzeigen. Filtern Sie die Anzeige nach Bereitstellungsgruppe und Zeitraum. Die Diagramme zu CPU, Speichernutzung und maximaler Zahl gleichzeitiger Sitzungen können für die letzten 2 Stunden, 24 Stunden, 7 Tage, den letzten Monat und das letzte Jahr angezeigt werden. Diagramme zu IOPS und Datenträgerlatenz sind für die letzten 24 Stunden, den letzten Monat und das letzte Jahr verfügbar.

Hinweise:

- Die Überwachungsrichtlinieneinstellung Prozessüberwachung aktivieren muss auf "Zugelassen"festgelegt sein, damit Daten für die Tabelle "Top-10-Prozesse"auf der Seite "Historische Maschinenauslastung"gesammelt und angezeigt werden können. Die Richtlinie ist standardmäßig auf "Nicht zugelassen"festgelegt. Standardmäßig werden alle Daten zur Ressourcenauslastung gesammelt. Diese Datensammlung kann über die Richtlinieneinstellung Ressourcenüberwachung aktivieren deaktiviert werden. Die Tabelle unterhalb der Diagrammen enthält die Ressourcenauslastung pro Maschine.
- Für "Durchschnittliche IOPS"werden Tagesdurchschnittswerte angezeigt. Als maximale IOPS gilt der höchste IOPS-Durchschnittswert des ausgewählten Zeitraums. (Der IOPS-Durchschnittswert ist der Durchschnitt von IOPS im Zeitraum von einer Stunde auf dem VDA.)

Anzeigen von Netzwerkanalysedaten: Die Verfügbarkeit dieses Features richtet sich nach Lizenz und Administratorberechtigungen. Für dieses Feature sind Director und Delivery Controller ab **Version 7.11** erforderlich.

Überwachen Sie auf der Registerkarte Netzwerk die Netzwerkanalyse, die eine kontextbezogene Ansicht der Benutzer, Anwendungen und Desktops im Netzwerk bereitstellt. Mit diesem Feature liefert Director eine erweiterte Analyse des ICA-Datenverkehrs der Bereitstellung über HDX Insight-Berichte von NetScaler Insight Center oder NetScaler MAS. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkanalyse.

Anzeigen der Anwendungsstörungen: Auf der Registerkarte "Anwendungsstörungen"werden Fehler bei den veröffentlichten Anwendungen auf den VDAs angezeigt.

Für dieses Feature sind Delivery Controller und VDAs ab **Version 7.15** erforderlich. Desktopbetriebssystem-VDAs unter Windows Vista und höher und Serverbetriebssystem-VDAs unter Windows Server 2008 und höher werden unterstützt.
Weitere Informationen finden Sie unter Überwachen historischer Anwendungsstörungen.

Standardmäßig werden nur Anwendungsstörungen von Serverbetriebssystem-VDAs angezeigt. Sie können die Überwachung von Anwendungsstörungen über die Überwachungsrichtlinien steuern. Weitere Informationen finden Sie unter Einstellungen der Überwachungsrichtlinie.

Erstellen benutzerdefinierter Berichte: Über die Registerkarte "Benutzerdefinierte Berichte"können benutzerdefinierte Berichte mit Echtzeit- und historischen Daten aus der Überwachungsdatenbank in tabellarischer Form erstellt werden.

Für dieses Feature sind Director und Delivery Controller ab **Version 7.12** erforderlich.

Von der Liste der benutzerdefinierten Berichtsabfragen aus können Sie auf **Ausführen** klicken, um Berichte im CSV-Format zu exportieren. Darüber hinaus können Sie mit der Option **OData kopieren** die zugehörige OData-Abfrage kopieren und teilen und mit **Bearbeiten** die Abfrage bearbeiten.
Sie können eine neue Abfrage für benutzerdefinierte Berichte basierend auf Maschinen, Verbindungen, Sitzungen oder Anwendungsinstanzen erstellen. Filterbedingungen können Sie auf der Basis von Feldern (z. B. Maschine, Bereitstellungsgruppe oder Zeitraum) festlegen. Falls erforderlich, geben Sie zusätzliche Spalten für den benutzerdefinierten Bericht an. In der Vorschau können Sie ein Beispiel für die Berichtsdaten anzeigen. Wenn Sie die benutzerdefinierte Berichtsabfrage speichern, wird sie der Liste der gespeicherten Abfragen hinzugefügt.

Sie können eine neue benutzerdefinierte Berichtsabfrage basierend auf einer kopierten OData-Abfrage erstellen. Wählen Sie hierfür die OData-Abfrageoption und fügen Sie die kopierte OData-Abfrage ein. Sie können die resultierende Abfrage für das Ausführen zu einem späteren Zeitpunkt speichern.

Die Flag-Symbole auf dem Diagramm weisen auf wichtige Ereignisse oder Aktionen für diesen Zeitraum hin. Bewegen Sie den Mauszeiger über das Flag und klicken Sie, um Ereignisse und Aktionen aufzulisten.

Hinweise:

- Anmeldedaten für HDX-Verbindungen werden für VDAs vor Version 7 nicht gesammelt. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.
- Bereitstellungsgruppen, die in Citrix Studio gelöscht wurden, stehen in den Trendfiltern von Director zur Auswahl bis die zugehörigen Daten bereinigt werden. Wenn Sie eine gelöschte Bereitstellungsgruppe wählen, werden Diagramme für verfügbare Daten angezeigt. Die Tabellen zeigen jedoch keine Daten an.
- Wenn eine Maschine mit aktiven Sitzungen von einer Bereitstellungsgruppe in eine andere verschoben wird, werden in den Tabellen **Ressourcenauslastung und Lastauswertungspro-**

grammindex der neuen Bereitstellungsgruppe Metriken angezeigt, die aus den alten und neuen Bereitstellungsgruppen konsolidiert wurden.

Exportieren von Berichten

Sie können Trenddaten zum Generieren normaler Auslastungs- und Kapazitätsverwaltungsberichte exportieren. Der Export kann als PDF-, Excel- und CSV-Datei erfolgen. Berichte in PDF- und Excel-Format enthalten Trenddaten in Diagramm- und Tabellenform. CSV-Berichte enthalten Tabellendaten, die zum Generieren von Ansichten verarbeitet oder archiviert werden können.

Exportieren eines Berichts

1. Rufen Sie die Registerkarte **Trends** auf.
2. Legen Sie Filterkriterien und Zeitraum fest und klicken Sie auf **Anwenden**. Das Trenddiagramm und die Tabelle werden mit Daten aufgefüllt.
3. Klicken Sie auf **Exportieren**, geben Sie einen Namen für den Bericht ein und wählen Sie das Format.

Director generiert den Bericht basierend auf den von Ihnen gewählten Filterkriterien. Wenn Sie die Filterkriterien ändern, und klicken Sie auf **Anwenden** und erst dann auf **Exportieren**.

Hinweis: Das Exportieren einer großen Datenmenge führt zu einer stark erhöhten CPU- und Speicherauslastung auf dem Director-Server, dem Delivery Controller und den SQL Server-Computern. Die unterstützte Anzahl gleichzeitiger Exportvorgänge und die Menge der exportierbaren Daten sind auf Standardlimits festgelegt, um die optimale Leistung beim Exportieren zu erreichen.

Unterstützte Limits beim Exportieren

Exportierte PDF- und Excel-Berichte enthalten vollständige Diagramme gemäß den ausgewählten Filterkriterien. Die Tabellendaten sind jedoch in allen Berichtsformaten auf das Standardtabellenzeilenlimit bzw. das Standarddatensatzlimit beschränkt. Die Standardlimits für die Zahl der Datensätze hängen jeweils vom Berichtformat ab.

Sie können die Standardlimits in den Director-Anwendungseinstellungen in Internetinformationsdienste (IIS) ändern.

Berichtformat	Standardlimit für Datensätze	Felder in Director-Anwendungseinstellungen	Maximal unterstützte Zahl von Datensätzen
PDF	500	UI.ExportPdfDrilldownLimit	5000
[Excel]	100.000	UI.ExportExcelDrilldownLimit	1.000.000

Berichtformat	Standardlimit für Datensätze	Felder in Director-Anwendungseinstellungen	Maximal unterstützte Zahl von Datensätzen
CSV	100.000 (10.000.000 auf Registerkarte “Sitzungen”)	UI.ExportCsvDrilldownLimit	100.000

Ändern des Limits exportierbarer Datensätze

1. Öffnen Sie die IIS-Verwaltungskonsole.
2. Wechseln Sie zur Director-Website unter der Standardwebsite.
3. Doppelklicken Sie auf **Anwendungseinstellungen**.
4. Bearbeiten Sie das Feld oder fügen Sie ein neues Feld hinzu.

Die in den Anwendungseinstellungen hinzugefügten Werte setzen die Standardwerte außer Kraft.

Warnung: Das Festlegen eines Werts, der die maximal unterstützte Anzahl von Datensätzen übersteigt, kann die Exportleistung senken und wird nicht unterstützt.

Fehlerbehandlung

Dieser Abschnitt enthält Informationen zur Behandlung von Fehlern, die beim Export auftreten können.

- **Timeout in Director**

Dieser Fehler kann aufgrund von Netzwerkproblemen oder einer hohen Ressourcenauslastung auf dem Director-Server oder beim Überwachungsdienst auftreten.

Das Standardtimeout ist 100 Sekunden. Erhöhen Sie in IIS die Timeoutdauer für den Director-Dienst im Feld **Connector.DataServiceContext.Timeout** der Director-Anwendungseinstellungen:

1. Öffnen Sie die IIS-Verwaltungskonsole.
2. Wechseln Sie zur Director-Website unter der Standardwebsite.
3. Doppelklicken Sie auf **Anwendungseinstellungen**.
4. Bearbeiten Sie den Wert **Connector.DataServiceContext.Timeout**.

- **Timeout in Überwachungsdienst**

Dieser Fehler kann aufgrund von Netzwerkproblemen oder einer hohen Ressourcenauslastung bei Überwachungsdienst oder auf dem SQL Server-Computer auftreten.

Zur Erhöhung der Timeoutdauer für den Überwachungsdienst führen Sie die folgenden PowerShell-Befehle auf dem Delivery Controller aus:


```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Maximum gleichzeitiger Export- oder Vorschauvorgänge in Verarbeitung**

Director unterstützt nur eine Export- oder Vorschauinstanz. Wenn gemeldet wird, dass das **Maximum gleichzeitiger Export- oder Vorschauvorgänge** überschritten wird, versuchen Sie den nächsten Export später erneut.

Das Maximum gleichzeitiger Export-/Vorschauvorgänge kann erhöht werden, doch dies kann Auswirkungen auf die Leistung von Director haben und wird nicht unterstützt:

1. Öffnen Sie die IIS-Verwaltungskonsole.
2. Wechseln Sie zur Director-Website unter der Standardwebsite.
3. Doppelklicken Sie auf **Anwendungseinstellungen**.
4. Bearbeiten Sie den **Wert UI.ConcurrentExportLimit**.

- **Nicht genügend Speicherplatz in Director**

Jeder Exportvorgang erfordert bis zu 2 GB Speicherplatz im Temp-Ordner von Windows. Führen Sie den Exportvorgang erneut durch, nachdem Sie auf dem Director-Server Speicherplatz freigegeben oder hinzugefügt haben.

Überwachen von Hotfixes

Zum Anzeigen der auf einem bestimmten Maschinen-VDA (physisch oder VM) installierten Hotfixes wählen Sie die Ansicht Maschinendetails.

Steuern der Energiezustände von Benutzermaschinen

Steuern Sie den Zustand der in Director ausgewählten Maschinen mit den Optionen für die Energieverwaltung. Diese Optionen stehen für Desktopbetriebssystemmaschinen, aber möglicherweise nicht für Serverbetriebssystemmaschinen zur Verfügung.

Hinweis: Diese Funktionen stehen nicht für physische Maschinen und Maschinen, die Remote-PC-Zugriff verwenden, zur Verfügung.

Befehl	Funktion
Restart	Die VM wird ordnungsgemäß heruntergefahren und alle ausgeführten Prozesse werden einzeln angehalten, bevor die VM neu gestartet wird. Wählen Sie diese Option beispielsweise für den Neustart von Maschinen, die in Director mit "Konnten nicht gestartet werden"ausgewiesen werden.
Neustart erzwingen	Die VM wird neu gestartet, ohne dass sie heruntergefahren wird. Dieser Befehl funktioniert genauso wie das Trennen des Netzsteckers eines physischen Servers und Neuanschließen und Einschalten des Servers.
Herunterfahren	Die VM wird ordnungsgemäß heruntergefahren und alle ausgeführten Prozesse werden einzeln angehalten.
Herunterfahren erzwingen	Die VM wird zwingend heruntergefahren, ohne dass das Verfahren zum Herunterfahren durchgeführt wird. Dieser Befehl funktioniert genauso wie das Trennen des Netzsteckers eines physischen Servers. Es werden möglicherweise nicht immer alle ausgeführten Prozesse heruntergefahren, sodass bei diesem Verfahren die Gefahr von Datenverlust besteht.
Suspend	Die laufende VM wird im aktuellen Zustand angehalten und dieser Zustand wird in einer Datei im Standardspeicherrepository gespeichert. Diese Option ermöglicht das Herunterfahren der VM auf dem Hostserver und später, nach einem Neustart, die Wiederaufnahme der VM mit dem ursprünglichen Ausführungsstatus.
Fortfahren	Nimmt eine angehaltene VM wieder auf und stellt den ursprünglichen Ausführungsstatus wieder her.
Starten	Startet eine ausgeschaltete VM.

Sollten die Energieverwaltungsaktionen fehlschlagen, zeigen Sie mit der Maus auf die Warnung und

es wird eine Meldung mit Details zum Fehler angezeigt.

Verhindern von Verbindungen mit Maschinen

Verwenden Sie den Wartungsmodus, um vorübergehend neue Verbindungen zu verhindern, während der entsprechende Administrator Wartungsaufgaben am Image durchführt.

Wenn Sie den Wartungsmodus auf Maschinen aktivieren, werden keine neuen Verbindungen zugelassen, bis Sie ihn wieder deaktivieren. Wenn Benutzer momentan angemeldet sind, wird der Wartungsmodus erst wirksam, sobald alle Benutzer abgemeldet sind. Benutzern, die sich nicht abmelden, müssen Sie eine Nachricht senden, die sie darüber informiert, dass die Maschine zu einem bestimmten Zeitpunkt heruntergefahren wird. Verwenden Sie die Energieverwaltung, um die Maschinen zwingend herunterzufahren.

1. Wählen Sie die Maschine aus, z. B. auf der Ansicht Benutzerdetails, oder eine Gruppe von Maschinen in der Ansicht Filter.
2. Klicken Sie auf Wartungsmodus und aktivieren Sie die Option.

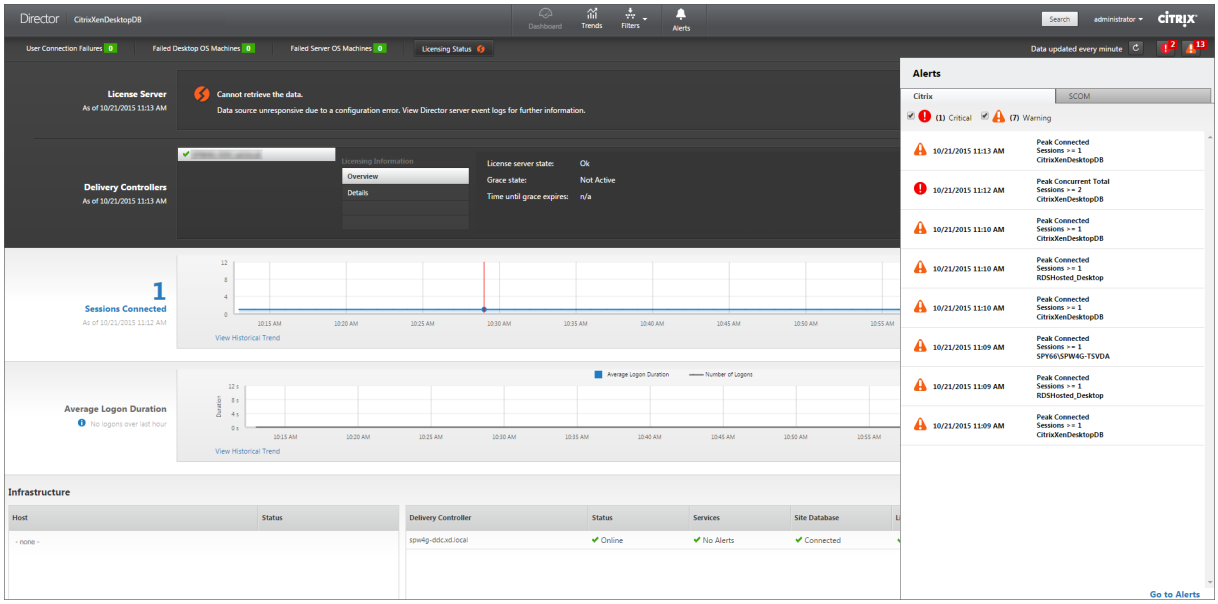
Wenn ein Benutzer versucht, eine Verbindung zu einem zugewiesenen Desktop herzustellen, während er im Wartungsmodus ist, wird eine Meldung angezeigt, dass der Desktop zurzeit nicht verfügbar ist. Es können keine neuen Verbindungen hergestellt werden, bis der Wartungsmodus deaktiviert wird.

Warnungen und Benachrichtigungen

August 15, 2023

Anzeigen von Warnungen

In Director werden im Dashboard und in anderen Ansichten der oberen Ebene Warnungen und kritische Warnungen mit entsprechenden Symbolen angezeigt. Warnungen stehen für Sites mit **Platinum**-Lizenz zur Verfügung. Die Anzeige von Warnungen wird jede Minute automatisch aktualisiert und kann bei Bedarf auch manuell aktualisiert werden.

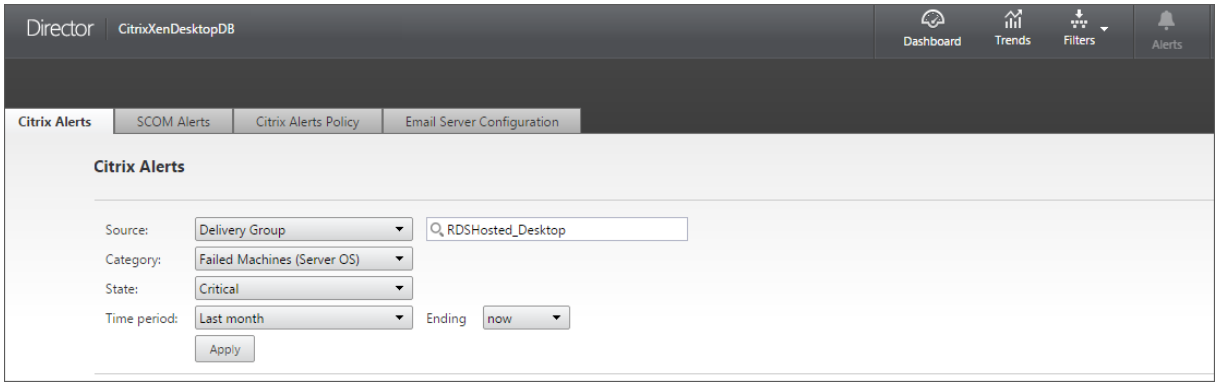


Eine Warnung (gelbes Dreieck) zeigt an, dass der Schwellenwert einer Bedingung erreicht oder überschritten wurde.

Eine kritische Warnung (roter Kreis) zeigt an, dass der kritische Schwellenwert einer Bedingung erreicht oder überschritten wurde.

Sie können detaillierte Informationen zu Warnungen anzeigen, indem Sie eine Warnung in der Seitenleiste auswählen und unten in der Seitenleiste auf **Warnmeldungen** oder oben auf der Director-Seite **Warnungen** klicken.

In der Ansicht “Warnungen”können Sie Warnungen filtern und exportieren. Beispielsweise können Sie fehlerhafte Serverbetriebssystemmaschinen für eine bestimmte Bereitstellungsgruppe im vergangenen Monat oder alle Warnungen für einen bestimmten Benutzer anzeigen. Weitere Informationen finden Sie unter Exportieren von Berichten.



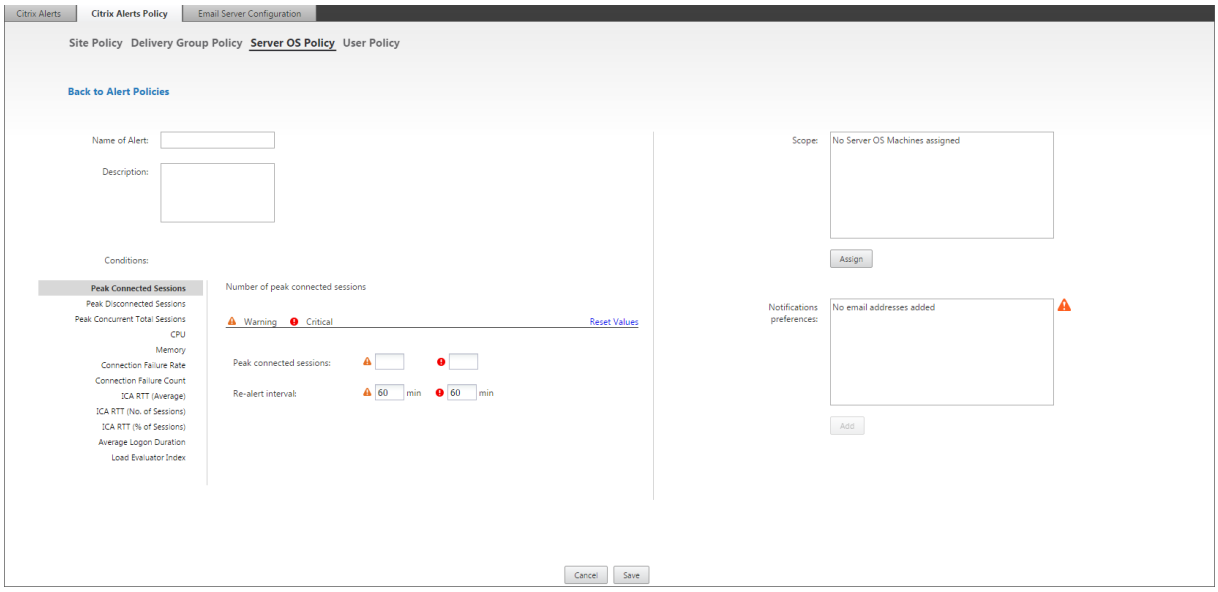
Citrix Warnmeldungen. Citrix Warnungen in Director stammen von Citrix Komponenten. Sie können Citrix Warnungen in Director über **Warnungen** > **Citrix Benachrichtigungsrichtlinie** konfigurieren. Im Rahmen der Konfiguration können Sie den Versand von Benachrichtigungen per E-Mail an Personen und Gruppen festlegen, wenn die Schwellenwerte überschritten werden. Sie können die

Benachrichtigungen als Octoblu-Webhooks oder SNMP-Traps konfigurieren. Weitere Informationen zum Einrichten von Citrix Warnungen finden Sie unter Erstellen von Benachrichtigungsrichtlinien.

SCOM-Warnungen: Warnungen von Microsoft System Center 2012 Operations Manager (SCOM) enthalten detaillierte Angaben zu Datencenterintegrität und Leistung in Director. Weitere Informationen finden Sie unter SCOM-Warnungen.

Die neben den Warnsymbolen vor dem Erweitern der Randleiste angezeigte Zahl entspricht der Summe der Citrix und SCOM-Warnungen.

Erstellen von Benachrichtigungsrichtlinien



Gehen Sie zum Erstellen einer Benachrichtigungsrichtlinie, z. B. zum Generieren einer Warnung bei Eintreten bestimmter Sitzungszahlbedingungen, folgendermaßen vor:

1. Gehen Sie zu **Warnungen**> **Citrix Benachrichtigungsrichtlinie** und wählen Sie beispielsweise “Server OS-Richtlinie”aus.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein und legen Sie die Bedingungen zum Auslösen der Warnung fest. Geben Sie beispielsweise für die Kategorie “Warnung” und “Kritisch”Werte für “Max. verbundener Sitzungen”, “Max. getrennter Sitzungen”und “Max. gleichzeitiger Sitzungen insgesamt”ein. Die Werte der Kategorie “Warnung”dürfen nicht größer sein als die der Kategorie “Kritisch”. Weitere Informationen finden Sie unter Bedingungen für Benachrichtigungsrichtlinien.
4. Legen Sie das Wiederholungsintervall fest. Wenn die Bedingungen für die Warnung weiterhin erfüllt sind, wird die Warnung nach diesem Zeitintervall neu ausgelöst und es wird, sofern dies in der Benachrichtigungsrichtlinie so festgelegt ist, eine E-Mail-Benachrichtigung

generiert. Wird eine Warnung geschlossen, wird nach dem Warnmeldungsintervall keine E-Mail-Benachrichtigung generiert.

5. Legen Sie den Bereich fest. Wählen Sie beispielsweise eine Bereitstellungsgruppe.
6. Geben Sie in den Benachrichtigungseinstellungen an, wer per E-Mail benachrichtigt werden soll, wenn die Warnung ausgelöst wird. Zum Festlegen von E-Mail-Einstellungen für Benachrichtigungsrichtlinien müssen Sie auf der Registerkarte **E-Mail-Serverkonfiguration** einen E-Mail-Server angeben.
7. Klicken Sie auf **Speichern**.

Informationen zur Konfiguration von Octoblu-Webhooks finden Sie unter Konfigurieren von Benachrichtigungsrichtlinien mit Octoblu-WebHooks.

Informationen zur Konfiguration von SNMP-Traps finden Sie unter Konfigurieren von Benachrichtigungsrichtlinien mit SNMP-Traps.

Wird eine Richtlinie mit einem Bereich von 20 oder mehr Bereitstellungsgruppen erstellt, kann es ca. 30 Sekunden dauern, bis die Konfiguration abgeschlossen ist. Während dieses Zeitraums wird ein Drehfeld angezeigt.

Wenn Sie mehr als 50 Richtlinien für bis zu 20 eindeutige Bereitstellungsgruppen (insgesamt 1000 Bereitstellungsgruppenziele) erstellen, nimmt die Reaktionszeit u. U. um mehr als 5 Sekunden zu.

Verschieben einer Maschine mit aktiven Sitzungen von einer Bereitstellungsgruppe in eine andere löst u. U. fälschlicherweise Bereitstellungsgruppenwarnungen aus, die mit Maschinenparametern definiert wurden.

Bedingungen für Benachrichtigungsrichtlinien

Bedingung der Benachrichtigungsrichtlinie	Beschreibung und empfohlene Aktionen
Max. verbundener Sitzungen	Maximalzahl verbundener Sitzungen Prüfen Sie die Maximalzahl verbundener Sitzungen in der Trendansicht von Director. Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist. Fügen Sie neue Maschinen hinzu, falls erforderlich.

Bedingung der Benachrichtigungsrichtlinie	Beschreibung und empfohlene Aktionen
Max. getrennter Sitzungen	Maximalzahl getrennter Sitzungen Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht von Director. Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist. Fügen Sie neue Maschinen hinzu, falls erforderlich. Melden Sie getrennte Sitzungen ab, falls erforderlich.
Max. gleichzeitiger Sitzungen insgesamt	Maximalzahl gleichzeitiger Sitzungen Prüfen Sie die Maximalzahl getrennter Sitzungen in der Trendansicht von Director. Vergewissern Sie sich, dass genügend Kapazität für die Sitzungslast verfügbar ist. Fügen Sie neue Maschinen hinzu, falls erforderlich. Melden Sie getrennte Sitzungen ab, falls erforderlich.
CPU	Prozentuale CPU-Auslastung Identifizieren Sie die Prozesse und Ressourcen, die CPU-Ressourcen verbrauchen. Beenden Sie, falls erforderlich, den Prozess. Bei Beenden des Prozesses gehen nicht gespeicherte Daten verloren. Funktioniert alles erwartungsgemäß, fügen Sie zusätzliche CPU-Ressourcen künftig hinzu. **Hinweis:** Die Richtlinieneinstellung “Ressourcenüberwachung aktivieren”ist auf Maschinen mit VDAs standardmäßig zur Überwachung von CPU- und Arbeitsspeicherleistungsindikatoren zugelassen. Wenn diese Richtlinie deaktiviert wird, werden keine Warnungen über CPU- und Arbeitsspeicherbedingungen ausgelöst. Weitere Informationen finden Sie unter Überwachungsrichtlinie.

Bedingung der Benachrichtigungsrichtlinie	Beschreibung und empfohlene Aktionen
Speicher	Prozentuale Speicherauslastung Identifizieren Sie die Prozesse und Ressourcen, die Arbeitsspeicher verbrauchen. Beenden Sie, falls erforderlich, den Prozess. Bei Beenden des Prozesses gehen nicht gespeicherte Daten verloren. Funktioniert alles erwartungsgemäß, fügen Sie zusätzlichen Arbeitsspeicher künftig hinzu. **Hinweis:** Die Richtlinieneinstellung “Ressourcenüberwachung aktivieren”ist auf Maschinen mit VDAs standardmäßig zur Überwachung von CPU- und Arbeitsspeicherleistungsindikatoren zugelassen. Wenn diese Richtlinie deaktiviert wird, werden keine Warnungen über CPU- und Arbeitsspeicherbedingungen ausgelöst. Weitere Informationen finden Sie unter Einstellungen der Überwachungsrichtlinie.
Verbindungsfehlerrate	Verbindungsfehler während der letzten Stunde in Prozent. Verhältnis der Summe aller Fehler zur Summe aller Verbindungsversuche. Überprüfen Sie in Director die Trendansicht zu Verbindungsfehlern auf Ereignisse aus dem Konfigurationsprotokoll. Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind.
Anzahl Verbindungsfehler	Zahl der Verbindungsfehler während der letzten Stunde. Überprüfen Sie in Director die Trendansicht zu Verbindungsfehlern auf Ereignisse aus dem Konfigurationsprotokoll. Prüfen Sie, ob Anwendungen bzw. Desktops erreichbar sind.

Bedingung der Benachrichtigungsrichtlinie	Beschreibung und empfohlene Aktionen
ICA RTT (Durchschnitt)	Durchschnittliche ICA-Roundtripzeit. Überprüfen Sie die Aufschlüsselung der ICA-Roundtripzeit über NetScaler HDX Insight, um die Ursache zu finden. Wenn NetScaler nicht verfügbar ist, überprüfen Sie die ICA-Roundtripzeit und die Latenz in der Ansicht “Benutzerdetails”in Director, um festzustellen, ob es sich um ein Netzwerkproblem oder ein Problem mit XenDesktop/XenApp handelt. Weitere Informationen finden Sie in der Dokumentation zu NetScaler Insight Center unter Use Cases: HDX Insight.
ICA RTT (Anzahl an Sitzungen)	Anzahl der Sitzungen, die den Schwellenwert für die ICA-Roundtripzeit überschreiten. Überprüfen Sie in NetScaler HDX Insight, wie viele Sitzungen eine hohe ICA-Roundtripzeit haben. Weitere Informationen finden Sie in der Dokumentation zu NetScaler Insight Center unter HDX Insight Reports. Wenn NetScaler nicht verfügbar ist, suchen Sie die Ursache zusammen mit dem Netzwerkteam.
ICA RTT (% der Sitzungen)	Prozentsatz der Sitzungen, die die durchschnittliche ICA-Roundtripzeit überschreiten. Überprüfen Sie in NetScaler HDX Insight, wie viele Sitzungen eine hohe ICA-Roundtripzeit haben. Weitere Informationen finden Sie in der Dokumentation zu NetScaler Insight Center unter HDX Insight Reports. Wenn NetScaler nicht verfügbar ist, suchen Sie die Ursache zusammen mit dem Netzwerkteam.
ICA RTT (Benutzer)	ICA-Roundtripzeit für Sitzungen, die von dem angegebenen Benutzer gestartet werden. Die Warnung wird ausgelöst, wenn die ICA-Roundtripzeit den Schwellenwert bei mindestens einer Sitzung überschreitet.

Bedingung der Benachrichtigungsrichtlinie	Beschreibung und empfohlene Aktionen
Fehlerhafte Maschinen (Desktop-OS)	Zahl fehlerhafter Desktopbetriebssystemmaschinen. Fehler können aus verschiedenen Gründen auftreten und werden entsprechend im Dashboard von Director oder in gefilterten Ansichten angezeigt. Führen Sie eine Ursachendiagnose mit Citrix Scout durch. Weitere Informationen finden Sie unter Behandeln von Benutzerproblemen.
Fehlerhafte Maschinen (Server-OS)	Zahl fehlerhafter Serverbetriebssystemmaschinen. Fehler können aus verschiedenen Gründen auftreten und werden entsprechend im Dashboard von Director oder in gefilterten Ansichten angezeigt. Führen Sie eine Ursachendiagnose mit Citrix Scout durch.
Durchschnittliche Anmeldedauer	Durchschnittliche Dauer der Anmeldungen in der letzten Stunde. Überprüfen Sie die aktuellen Daten zur Anmeldedauer im Dashboard von Director. Melden sich viele Benutzer innerhalb kurzer Zeit an, kann die Anmeldung länger dauern. Überprüfen Sie Baseline und Aufschlüsselung der Anmeldungen zur Ursachenfindung. Weitere Informationen finden Sie unter Diagnose von Benutzeranmeldeproblemen.
Anmeldedauer (Benutzer)	Dauer der Anmeldungen des angegebenen Benutzers in der letzten Stunde.
Lastauswertungsprogrammindex	Wert des Lastauswertungsprogrammindex der letzten 5 Minuten. Überprüfen Sie Director auf Serverbetriebssystemmaschinen, die unter Spitzenlast (Maximallast) laufen. Zeigen Sie den Dashboard- (Fehler) und den Trend-Lastauswertungsindexbericht an.

Konfigurieren von Benachrichtigungsrichtlinien mit Octoblu-WebHooks

Neben E-Mail-Benachrichtigungen können Sie auch Benachrichtigungsrichtlinien mit Octoblu-WebHooks zum Initiieren von IoT-Services konfigurieren.

Hinweis: Für dieses Feature sind Director und Delivery Controller ab Version 7.11 erforderlich.

Beispiele für IoT-Services, die Warnungen verwenden können, wären der Versand von SMS-Benachrichtigungen an Support-Mitarbeiter oder die Integration in spezielle Incident-Auflösungsplattformen zur Unterstützung der Benachrichtigungsnachverfolgung.

Sie können eine Benachrichtigungsrichtlinie mit HTTP-Rückruf oder HTTP POST mit PowerShell-Cmdlets konfigurieren. Die wurden auf die Unterstützung von Webhooks erweitert.

Informationen zum Erstellen eines Octoblu-Workflows und zum Erhalt der entsprechenden WebHook-URL finden Sie im Octoblu Developer Hub.

Zum Konfigurieren einer Octoblu-WebHook-URL für eine neue oder vorhandene Benachrichtigungsrichtlinie verwenden Sie die nachfolgend aufgeführten PowerShell-Cmdlets.

Erstellen einer neuen Benachrichtigungsrichtlinie mit einer Webhook-URL:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    Description <Policy description> -Enabled $true -Webhook <Webhook
    URL>
```

Hinzufügen einer Webhook-URL zu einer vorhandenen Benachrichtigungsrichtlinie:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

Aufrufen der Hilfe zu PowerShell-Befehlen (Beispiel):

```
Get-Help  <Set-MonitorNotificationPolicy>
```

Über die Benachrichtigungsrichtlinie generierte Benachrichtigungen lösen den WebHook mit einem POST-Aufruf an die WebHook-URL aus. Die POST-Meldung enthält die Benachrichtigungsinformationen im JSON-Format:

```
{
 "NotificationId" : \<Notification Id\>,

"Target" : <Notification Target Id>,

"Condition" : <Condition that was violated>,

"Value" : <Threshold value for the Condition>,

"Timestamp": <Time in UTC when notification was generated>,

"PolicyName": <Name of the Alert policy>,

```



```
"Description": <Description of the Alert policy>,

"Scope" : <Scope of the Alert policy>,

"NotificationState": <Notification state critical, warning, healthy or
   dismissed>,

"Site" : \<Site name\> }

<!--NeedCopy-->
```

Konfigurieren von Benachrichtigungsrichtlinien mit SNMP-Traps

Wenn eine mit einem SNMP-Trap konfigurierte Warnung ausgelöst wird, wird das SNMP-Trap an den konfigurierten Netzwerk-Listener zur weiteren Verarbeitung gesendet. Citrix Warnungen unterstützen Traps mit SNMP ab Version 2. Derzeit kann das Trap an einen Listener weitergeleitet werden.

Hinweis: Für dieses Feature sind Director und Delivery Controller ab Version 7.12 erforderlich.

Zum Konfigurieren von SNMP-Traps verwenden Sie die folgenden PowerShell-Cmdlets:

- Aufrufen der aktuellen SNMP-Serverkonfiguration:

```
Get-MonitorNotificationSnmpServerConfiguration
```

- Festlegen der Serverkonfiguration (SNMP-Version 2):

```
Set-MonitorNotificationSnmpServerConfiguration -ServerName <
   Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
   CommunityString public -Protocol V2
```

- Festlegen der Serverkonfiguration (SNMP-Version 3):

```
$authpass = "<authentication password>" | ConvertTo-SecureString
   -AsPlainText -Force
$privpass = "<Privacy password>" | ConvertTo-SecureString -
   AsPlainText -Force
Set-MonitorNotificationSnmpServerConfiguration -ServerName <
   Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
   EngineId <Engine Id> -AuthPassword $authpass -PrivPassword
   $privpass -PrivPasswordProtocol <Privacy password protocol> -
   AuthPasswordProtocol <Authentication password protocol> -
   Protocol V3
<!--NeedCopy-->
```

- Aktivieren von SNMP-Traps für eine vorhandene Benachrichtigungsrichtlinie:

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <Policy ID
   >
```

- Erstellen einer neuen Benachrichtigungsrichtlinie mit SNMP-Traps:


```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    IsSnmpEnabled $true -Description <Policy description> -Enabled
     $true
```

Das Format der OIDs in SNMP-Trapnachrichten von Director ist wie folgt:
1.3.6.1.4.1.3845.100.1.<UID>*
Die ***<UID>*** wird seriell für jede in Director definierte Benachrichtigungsrichtlinie generiert. Die OIDs sind daher für jede Benutzerumgebung eindeutig.

- Verwenden Sie **1.3.6.1.4.1.3845.100.1** zum Filtern aller Trap-Nachrichten von Director.
- Verwenden Sie **1.3.6.1.4.1.3845.100.1.*<UID>*** zum Filtern und Behandeln von Trapnachrichten über spezifische Warnungen.

Mit dem folgenden Cmdlet können Sie die für die Benachrichtigungsrichtlinien in Ihrer Umgebung definierten UIDs abrufen:

```
Get-MonitorNotificationPolicy
```

Sie können SNMP-Traps an SCOM weiterleiten. Konfigurieren Sie hierfür SCOM so, dass der Delivery Controller auf Trap-Nachrichten lauscht.

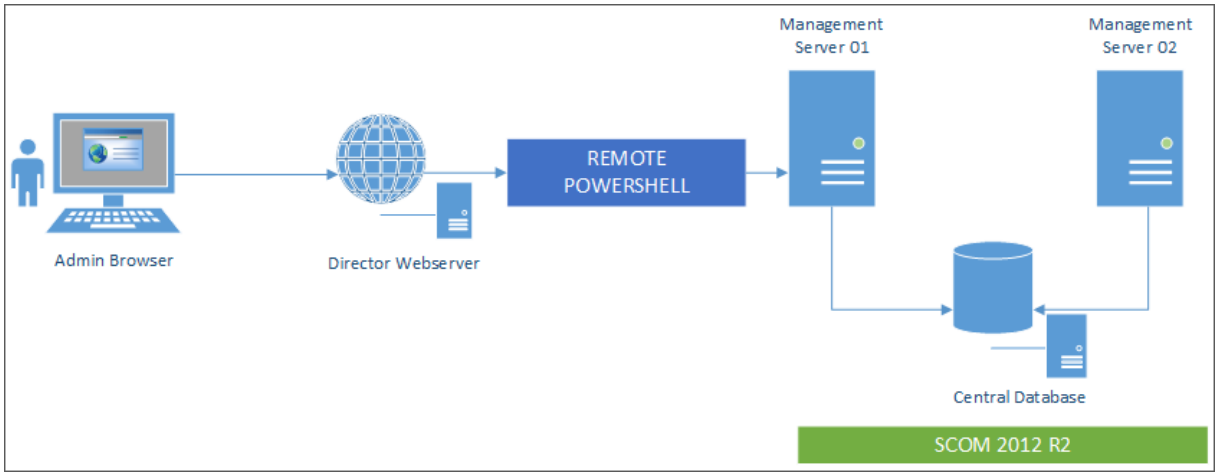
Konfigurieren der Integration von SCOM-Warnungen

Wird SCOM integriert, können Warnungen von SCOM im Dashboard und in anderen Ansichten der obersten Ebene in Director angezeigt werden.

SCOM-Warnungen werden parallel mit Citrix Warnungen angezeigt. Sie können auf SCOM-Warnungen über die SCOM-Registerkarte auf der Randleiste zugreifen und Details anzeigen.

Sie können Warnungen eines Alters von bis zu einem Monat anzeigen, sortieren und filtern und die gefilterten Informationen in CSV-, Excel- und PDF-Berichte exportieren. Weitere Informationen finden Sie unter Exportieren von Berichten.

Bei einer SCOM-Integration werden Daten mit Remote-PowerShell 3.0 oder höher beim SCOM-Verwaltungsserver abgefragt und es besteht eine beständige Runspace-Verbindung in der Director-Sitzung des Benutzers. Director und der SCOM-Server müssen über dieselbe PowerShell-Version verfügen.



Anforderungen für die SCOM-Integration:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 oder höher (PowerShell-Versionen in Director und auf dem SCOM-Server müssen übereinstimmen)
- Quad-Core-CPU mit 16 GB RAM (empfohlen)
- Ein primärer Verwaltungsserver für SCOM muss in der web.config-Datei von Director konfiguriert werden. Dafür können Sie das Tool DirectorConfig verwenden.

Hinweis:

- Citrix empfiehlt die Konfiguration des Director-Administratorkontos mit der SCOM-Rolle "Operator", damit die vollständigen Warnungsinformationen in Director abgerufen werden können. Ist das nicht möglich, kann mit dem DirectorConfig-Tool ein SCOM-Administratorkonto in der Datei web.config konfiguriert werden.
- Citrix empfiehlt, nicht mehr als 10 Director-Administratoren pro SCOM-Verwaltungsserver zu konfigurieren, um eine optimale Leistung sicher zu stellen.

Auf dem Director-Server

1. Geben Sie **Enable-PSRemoting** ein, um PowerShell-Remoting zu aktivieren.
2. Fügen Sie den SCOM-Verwaltungsserver der Liste "TrustedHosts"hinzu. Öffnen Sie eine PowerShell-Eingabeaufforderung und führen Sie die folgenden Befehle aus:

    a) Abrufen der aktuellen TrustedHosts-Liste

```
        Get-Item WSMAN:\localhost\Client\TrustedHosts
<!--NeedCopy-->
```

```
1.  Add the FQDN of the SCOM Management Server to the list of
    TrustedHosts. \<Old Values\> represents the existing set of entries
    returned from Get-Item cmdlet
```



```
        Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM
            Management Server>,<Old Values>"
<!--NeedCopy-->
```

1. Konfigurieren Sie SCOM mit dem Tool DirectorConfig.

```
    C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
<!--NeedCopy-->
```

Auf dem SCOM-Verwaltungsserver

1. Weisen Sie einer SCOM-Administratorrolle Director-Administratoren zu.

   a) Öffnen Sie die SCOM-Verwaltungskonsole und navigieren Sie zu **Verwaltung** > **Sicherheit** > **Benutzerrollen**.

   b) Unter "Benutzerrollen"können Sie Benutzerrollen erstellen und bearbeiten. Es gibt vier Kategorien von SCOM-Operatorrollen, die die Art des Zugriffs auf SCOM-Daten definieren. Beispielsweise kann die Rolle "Schreibgeschützt"den Verwaltungsbereich nicht sehen und keine Regeln, Maschinen und Konten erkennen oder verwalten. Eine Operatorrolle entspricht einer vollständigen Administratorrolle.

   Hinweis: Die folgenden Operationen sind nicht verfügbar, wenn der Director-Administrator eine andere Rolle als "Operator"hat:

   - Sind mehrere Verwaltungsserver konfiguriert und fällt der primäre Server aus, kann der Director-Administrator keine Verbindung mit dem sekundären Verwaltungsserver herstellen. Der primäre Verwaltungsserver ist der in der Director-Datei web.config konfigurierte Server und identisch mit dem Server, der im DirectorConfig-Tool in Schritt 3 angegeben wurde. Die sekundären Verwaltungsserver stehen mit dem primären Verwaltungsserver in einer Peerbeziehung.
   - Beim Filtern von Warnungen kann der Director-Administrator die Warnungsquelle nicht suchen. Dies erfordert Operator-Berechtigungen.

   c) Zum Ändern einer Benutzerrolle klicken Sie mit der rechten Maustaste auf die Rolle und dann auf **Eigenschaften**.

   d) In dem Dialogfeld mit den Benutzerrolleneigenschaften können Sie Director-Administratoren zu der angegebenen Benutzerrolle hinzufügen oder aus dieser entfernen.

2. Fügen Sie der Benutzergruppe "Remoteverwaltung"auf dem SCOM-Verwaltungsserver Director-Administratoren hinzu. Dadurch können Director-Administratoren eine Remote-PowerShell-Verbindung herstellen.

3. Geben Sie **Enable-PSRemoting** ein, um PowerShell-Remoting zu aktivieren.

4. Legen Sie die Limits für die Eigenschaften der WS-Verwaltung fest:

   a) Ändern von MaxConcurrentUsers:

   Befehlszeilenschnittstelle (CLI):

   ```
   winrm set winrm/config/winrs @{
    MaxConcurrentUsers = "20" }
   ```

   PS:

   ```
   Set -Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
   ```

   b) Ändern von MaxShellsPerUser:

   Befehlszeilenschnittstelle (CLI):

   ```
   winrm set winrm/config/winrs @{
    MaxShellsPerUser="20" }
   ```

   PS:

   ```
   Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
   ```

   c) Ändern von MaxMemoryPerShellMB:

   Befehlszeilenschnittstelle (CLI):

   ```
   winrm set winrm/config/winrs @{
    MaxMemoryPerShellMB="1024" }
   ```

   PS:

   ```
   Set -Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
   ```

5. Um sicherzustellen, dass die SCOM-Integration in Umgebungen mit gemischten Domänen funktioniert, legen Sie folgenden Registrierungseintrag fest:

   Pfad: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

   Schlüssel: LocalAccountTokenFilterPolicy

Typ: DWord

Wert: 1

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Nach dem Einrichten der SCOM-Integration wird möglicherweise die Meldung "Die aktuellen SCOM-Warnmeldungen können nicht abgerufen werden"angezeigt. Suchen Sie in den Director-Serverereignisprotokollen weitere Informationen. Anhand der Informationen in den Serverereignisprotokollen können Sie das Problem identifizieren und beheben. Mögliche Ursachen:

- Unterbrechung der Netzwerkverbindung am Computer mit Director oder SCOM
- SCOM-Dienst nicht verfügbar oder überlastet
- Keine Autorisierung aufgrund einer Änderung an den Berechtigungen des Benutzers
- Fehler in Director beim Verarbeiten der SCOM-Daten
- Nicht übereinstimmende PowerShell-Version zwischen Director und SCOM-Server.

Delegierte Administration und Director

May 24, 2024

Bei der delegierten Administration werden drei Konzepte eingesetzt: Administratoren, Rollen und Geltungsbereiche. Berechtigungen richten sich nach der Administratorrolle und dem Geltungsbereich dieser Rolle. Beispiel: Einem Administrator wird die Helpdeskadministratorrolle zugewiesen, bei der der Geltungsbereich die Verantwortung für Endbenutzer in nur einer Site umfasst.

Weitere Informationen über das Erstellen von delegierten Administratoren finden Sie unter Delegierte Administration.

Durch die administrativen Berechtigungen wird festgelegt, wie die Director-Benutzeroberfläche für Administratoren dargestellt wird und welche Aufgaben sie ausführen können. Mit Berechtigungen wird Folgendes festgelegt:

- Die Seiten, auf die der Administrator zugreifen kann, kollektiv als "Ansicht"bezeichnet
- Die Desktops, Maschinen und Sitzungen, die der Administrator anzeigen und verwenden kann
- Die Befehle, die der Administrator ausführen kann, z. B. das Spiegeln einer Benutzersitzung oder das Aktivieren des Wartungsmodus

Über die integrierten Rollen und Berechtigungen wird außerdem gesteuert, wie Administratoren Director verwenden:

Administratorrolle	Berechtigungen in Director
Volladministrator	Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten.
Bereitstellungsgruppenadministrator	Hat vollständigen Zugriff auf alle Ansichten und kann alle Befehle ausführen, einschließlich Spiegeln einer Benutzersitzung, Energieverwaltung und Sitzungverwaltung, Aktivieren des Wartungsmodus und Exportieren von Trenddaten.
Lesezugriffadministrator	Kann auf alle Ansichten zugreifen und alle Objekte in angegebenen Geltungsbereichen sowie globale Informationen anzeigen. Kann Berichte aus HDX-Kanälen herunterladen und Trenddaten mit der Exportoption in der Ansicht “Trends”exportieren. Kann keine anderen Befehle ausführen oder Daten in den Ansichten ändern.
Helpdeskadministrator	Kann nur auf die Ansichten “Helpdesk”und “Benutzerdetails”zugreifen und nur Objekte anzeigen, die dem Administrator zur Verwaltung übertragen wurden. Kann eine Benutzersitzung spiegeln und Befehle für diesen Benutzer ausführen. Kann Vorgänge im Wartungsmodus ausführen. Kann Energieoptionen auf Desktopbetriebssystemmaschinen verwenden. Kann nicht auf das Dashboard, Trends, Warnungen oder Filteransichten zugreifen. Kann keine Energieoptionen auf Serverbetriebssystemmaschinen verwenden.
Maschinenkatalogadministrator	Kein Zugriff. Dieser Administrator wird für Director nicht unterstützt und er kann keine Daten anzeigen. Dieser Benutzer kann auf die Seite “Maschinendetails”zugreifen (maschinenbasierte Suche).

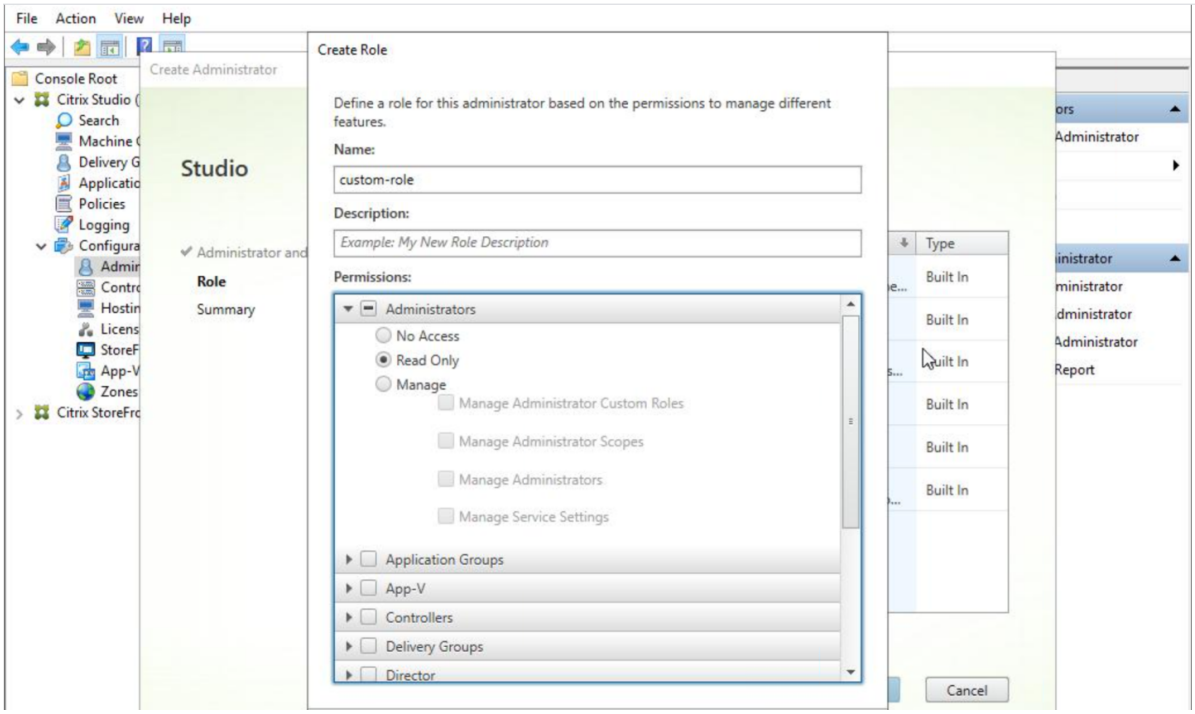
Administratorrolle	Berechtigungen in Director
Hostadministrator	Kein Zugriff. Dieser Administrator wird für Director nicht unterstützt und er kann keine Daten anzeigen.

Konfigurieren von benutzerdefinierten Rollen für Director-Administratoren

In Studio können Sie auch Director-spezifische benutzerdefinierte Rollen konfigurieren, die den Anforderungen Ihrer Organisation besser gerecht werden und eine flexiblere Delegierung von Berechtigungen ermöglichen. Sie können beispielsweise die integrierte Helpdeskadministratorrolle einschränken, sodass dieser Administrator keine Sitzungen abmelden kann.

Wenn Sie eine benutzerdefinierte Rolle mit Director-Berechtigungen erstellen, müssen Sie dieser auch andere allgemeine Berechtigungen erteilen:

- Delivery Controller-Berechtigung zur Anmeldung bei Director –mindestens Lesezugriff im Administratormodus
- Berechtigungen für Bereitstellungsgruppen zum Anzeigen der zu diesen gehörigen Daten in Director –mindestens Lesezugriff



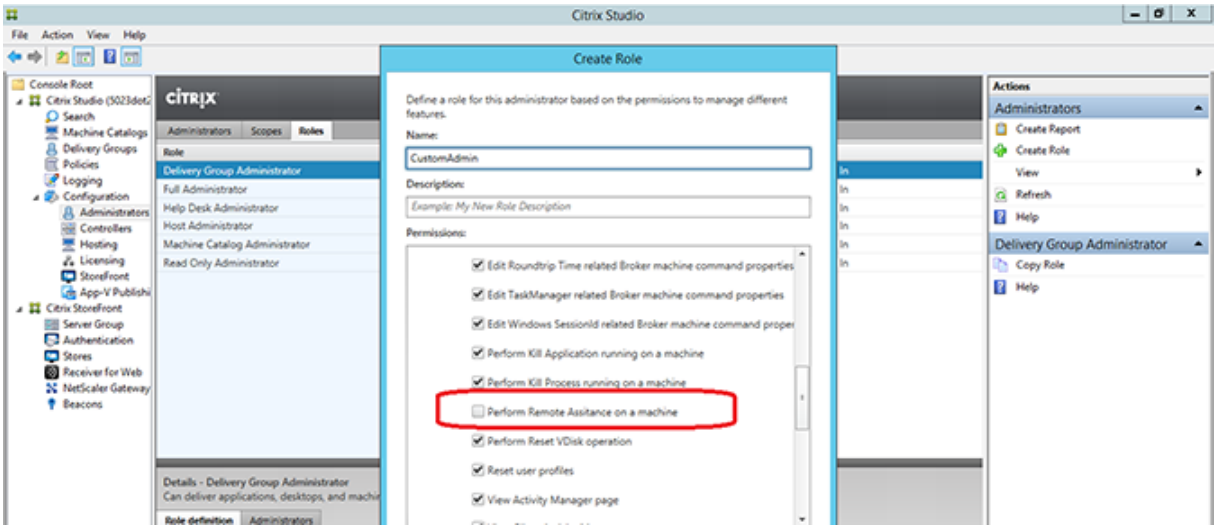
Alternativ können Sie eine benutzerdefinierte Rolle erstellen, indem Sie eine vorhandene Rolle kopieren und dieser zusätzliche Berechtigungen für die verschiedenen Ansichten erteilen. Sie kön-

nen beispielsweise die Rolle “Helpdesk”kopieren und Berechtigungen zum Anzeigen des Dashboards oder der Seiten “Filter”hinzufügen.

Wählen Sie die Director-Berechtigungen für die benutzerdefinierte Rolle, die Folgendes enthält:

- Abbrechen von auf Maschine ausgeführter Anwendung erzwingen
- Abbrechen von auf Maschine ausgeführtem Prozess erzwingen
- Remoteunterstützung für Maschine ausführen
- Vorgang zum Zurücksetzen von vDisk ausführen
- Benutzerprofile zurücksetzen
- Clientdetailseite anzeigen
- Dashboardseite anzeigen
- Filterseite anzeigen
- Maschinendetailseite anzeigen
- Trendseite anzeigen
- Benutzerdetailseite anzeigen

In diesem Beispiel ist das Spiegeln (Remoteunterstützung für Maschine ausführen) deaktiviert.



Es können Abhängigkeiten zwischen einer Berechtigung und weiteren Berechtigungen bestehen, die auf der Benutzeroberfläche in Kraft treten. Durch Auswahl der Berechtigung **Abbrechen von auf Maschine ausgeführter Anwendung erzwingen** wird die Funktion **Anwendung beenden** nur in den Bereichen aktiviert, für die die Rolle die Berechtigung hat. Sie können die folgenden Bereichsberechtigungen auswählen:

- Filterseite anzeigen
- Benutzerdetailseite anzeigen
- Maschinendetailseite anzeigen
- Clientdetailseite anzeigen

Aus der Liste der Berechtigungen für andere Komponenten sollten Sie zusätzlich folgende Berechtigungen von Bereitstellungsgruppen berücksichtigen:

- Aktivieren/Deaktivieren des Wartungsmodus einer Maschine mit der Bereitstellungsgruppenmitgliedschaft
- Ausführen von Energievorgängen auf Windows-Desktopmaschinen mit der Bereitstellungsgruppenmitgliedschaft
- Ausführen der Sitzungsverwaltung auf Maschinen unter mit der Bereitstellungsgruppenmitgliedschaft

Sichere Bereitstellung von Director

July 10, 2020

In diesem Artikel werden Bereiche behandelt, die sich bei der Bereitstellung und Konfiguration von Director auf die Systemsicherheit auswirken können.

Konfigurieren von Microsoft Internetinformationsdienste (IIS)

Sie können Director mit einer eingeschränkten IIS-Konfiguration konfigurieren. Dies ist jedoch nicht die IIS-Standardkonfiguration.

Dateinamenerweiterungen

Sie können nicht aufgeführte Dateinamenerweiterungen ausschließen.

Director benötigt die Dateinamenerweiterungen bei der Anforderungsfilterung:

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .woff
- .woff2
- .png
- .eot
- .svg

- .ttf
- .json
- . (für Umleitungen)

Director benötigt die folgenden HTTP-Verben bei der Anforderungsfilterung. Sie können nicht aufgeführte Verben ausschließen.

- GET
- POST
- HEAD

Director erfordert Folgendes nicht:

- ISAPI-Filter
- ISAPI-Erweiterungen
- CGI-Programme
- FastCGI-Programme

Wichtig:

- Director erfordert volles Vertrauen. Legen Sie jedoch nicht die globale .NET-Vertrauensebene auf "Hoch"oder niedriger fest.
- Director hat einen separaten Anwendungspool. Zum Ändern der Director-Einstellungen wählen Sie die Director-Site und führen Sie die Änderungen durch.

Konfigurieren von Benutzerrechten

Wenn Director installiert wird, werden den Anwendungspools die Anmeldeberechtigung "Anmelden als Dienst"und die Privilegien "Anpassen von Speicherkontingenten für einen Prozess", "Generieren von Sicherheitsüberwachungen"und "Ersetzen eines Tokens auf Prozessebene"zugewiesen. Dies ist normales Installationsverhalten beim Erstellen von Anwendungspools.

Sie brauchen die Benutzerrechte nicht zu ändern. Diese Privilegien werden von Director nicht verwendet und werden automatisch deaktiviert.

Kommunikation mit Director

Citrix empfiehlt für Produktionsumgebungen die Verwendung von IPsec (Internet Protocol Security) oder von HTTPS-Protokollen zum Schutz der Datenübertragung zwischen Director und Ihren Servern. IPsec bietet eine Reihe von Standarderweiterungen des Internetprotokolls, die authentifizierte und verschlüsselte Kommunikation mit Datenintegrität und Schutz vor Wiedergabeangriffen bieten. Da IPsec ein Protokollsatz der Vermittlungsschicht ist, können Protokolle höherer Stufen es unverändert

verwenden. HTTPS verwendet die Transport Layer Security (TLS), um eine sichere Datenverschlüsselung zu erzielen.

Hinweis:

- Citrix empfiehlt dringend, keine ungeschützten Verbindungen mit Director in einer Produktionsumgebung zu aktivieren.
- Die von Director ausgehende sichere Kommunikation erfordert die separate Konfiguration für jede Verbindung.
- SSL wird nicht empfohlen. Verwenden Sie stattdessen das sicherere TLS-Protokoll.
- Sie müssen die Kommunikation mit NetScaler mit TLS und nicht IPsec schützen.

Informationen zum Schützen der Kommunikation zwischen Director und XenApp und XenDesktop-Servern (für die Überwachung und Berichte) finden Sie unter Data Access Security.

Informationen zum Schützen der Kommunikation zwischen Director und NetScaler (für NetScaler Insight) finden Sie unter Konfigurieren der Netzwerkanalyse.

Informationen zum Schützen der Kommunikation zwischen Director und Lizenzserver finden Sie unter Schützen der License Administration Console.

Isolierung der Director-Sicherheit

Falls Sie Webanwendungen in derselben Webdomäne (Domänenname und Port) wie Director bereitstellen, können die mit diesen Webanwendungen verbundenen Sicherheitsrisiken eventuell auch die Sicherheit der Director-Bereitstellung negativ beeinflussen. Ist höhere Sicherheit erforderlich, empfiehlt Citrix die Bereitstellung von Director in einer getrennten Webdomäne.

Konfigurieren von Berechtigungen für VDAs vor XenDesktop 7

July 1, 2019

Wenn Benutzer VDAs einer Version vor XenDesktop 7 haben, ergänzt Director Informationen aus der Bereitstellung durch Echtzeitstatus und -metrik über Windows-Remoteverwaltung (WinRM).

Darüber hinaus können Sie mit dem hier beschriebenen Verfahren WinRM für die Verwendung mit Remote PC in XenDesktop 5.6 Feature Pack1 konfigurieren.

Standardmäßig verfügen nur lokale Administratoren des Desktopcomputers (in der Regel Domänenadministratoren und andere privilegierte Benutzer) über die Berechtigungen, die zum Anzeigen der Echtzeitdaten erforderlich sind.

Informationen zum Installieren und Konfigurieren von WinRM finden Sie unter CTX125243.

Um anderen Benutzern das Anzeigen von Echtzeitdaten zu ermöglichen, müssen Sie diesen Berechtigungen erteilen. Beispiel: Angenommen, es gibt mehrere Director-Benutzer (HelpDeskUserA, HelpDeskUserB usw.), die zu einer Active Directory-Sicherheitsgruppe namens "HelpDeskUsers" gehören. Der Gruppe wurde in Studio die Helpdeskadministratorrolle mit den erforderlichen Delivery Controller-Berechtigungen zugewiesen. Die Gruppe benötigt jedoch auch Zugriff auf Informationen vom Desktopcomputer.

Sie haben zwei Möglichkeiten, die Berechtigungen für den erforderlichen Zugriff zu konfigurieren:

- Erteilen von Berechtigungen für die Director-Benutzer (Identitätswechselmodell)
- Erteilen von Berechtigungen für den Director-Dienst (Modell mit vertrauenswürdigem Subsystem)

Erteilen von Berechtigungen für die Director-Benutzer (Identitätswechselmodell)

Director verwendet standardmäßig ein Identitätswechselmodell: Die WinRM-Verbindung mit der Desktopmaschine wird mit der Identität des Director-Benutzers hergestellt. Aus diesem Grund muss der Benutzer über die erforderlichen Berechtigungen auf dem Desktop verfügen.

Sie können diese Berechtigungen mit einer der folgenden beiden Methoden konfigurieren (nachfolgend beschrieben):

1. Hinzufügen von Benutzern zur lokalen Administratorgruppe auf der Desktopmaschine.
2. Erteilen der von Director benötigten spezifischen Berechtigungen für Benutzer. Bei dieser Option wird vermieden, dass Director-Benutzer (beispielsweise die HelpDeskUsers-Gruppe) Volladministratorrechte auf der Maschine erhalten.

Erteilen von Berechtigungen für den Director-Dienst (Modell mit vertrauenswürdigem Subsystem)

Anstatt den Director-Benutzern Berechtigungen für die Desktopmaschinen zu erteilen, können Sie Director so konfigurieren, dass WinRM-Verbindungen mit einer Dienstidentität hergestellt werden, und ausschließlich dieser Dienstidentität die entsprechenden Berechtigungen erteilen.

Bei diesem Modell sind die Benutzer von Director nicht berechtigt, selbst WinRM-Aufrufe zu tätigen. Sie können nur mit Director auf die Daten zugreifen.

Der Director-Anwendungspool in IIS ist für die Ausführung als Dienstidentität konfiguriert. Dies ist standardmäßig das virtuelle Konto "APPPOOL\Director". Beim Herstellen von Remoteverbindungen wird dieses Konto als das Active Directory-Computerkonto des Servers angezeigt, z. B. MyDomain\DirectorServer$. Sie müssen dieses Konto mit den entsprechenden Berechtigungen konfigurieren.

Wenn mehrere Director-Websites bereitgestellt werden, müssen Sie das Computerkonto jedes Webservers in eine Active Directory-Sicherheitsgruppe setzen, die entsprechende Berechtigungen hat.

Um Director so einzustellen, dass anstelle der Benutzeridentität die Dienstidentität für WinRM verwendet wird, konfigurieren Sie die folgende Einstellung, wie unter Erweiterte Konfiguration beschrieben:

```
Service.Connector.WinRM.Identity = Service
<!--NeedCopy-->
```

Sie haben zwei Möglichkeiten, diese Berechtigungen zu konfigurieren:

1. Hinzufügen des Dienstkontos zur lokalen Administratorgruppe auf der Desktopmaschine.
2. Erteilen Sie dem Dienstkonto die für Director erforderlichen Berechtigungen (siehe weiter unten). So kann eine Erteilung von Volladministratorrechten für das Dienstkonto auf der Maschine vermieden werden.

Zuweisen Sie von Berechtigungen zu einem Benutzer oder einer Gruppe

Die folgenden Berechtigungen sind erforderlich, damit Director auf die von der Desktopmaschine benötigten Informationen über WinRM zugreifen kann:

- Lese- und Ausführberechtigungen in WinRM RootSDDL
- WMI-Namespace-Berechtigungen:
  - root/cimv2 –Remotezugriff
  - root/citrix –Remotezugriff
  - root/RSOP –Remotezugriff und Ausführen
- Zugehörigkeit zu diesen lokalen Gruppen:
  - Systemmonitorbenutzer
  - Ereignisprotokollleser

Das ConfigRemoteMgmt.exe-Tool, das zum automatischen Erteilen dieser Berechtigungen verwendet wird, befindet sich auf dem Installationsmedium in den Ordnern x86\Virtual Desktop Agent und x64\Virtual Desktop Agent und auf dem Installationsmedium im Ordner C:\inetpub\wwwroot\Director\tools. Sie müssen allen Director-Benutzern Berechtigungen erteilen.

Um einer Active Directory-Sicherheitsgruppe, einem Benutzer oder einem Computerkonto Berechtigungen zu erteilen, oder um Aktionen auszuführen wie “Anwendung beenden”und “Prozess beenden”, führen Sie das Tool mit Administratorrechten an einer Eingabeaufforderung mit den folgenden Argumenten aus:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name
<!--NeedCopy-->
```


Wobei “Name”eine Sicherheitsgruppe, ein Benutzer oder ein Computerkonto ist.

Erteilen der erforderlichen Berechtigungen für eine Benutzersicherheitsgruppe:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
<!--NeedCopy-->
```

Erteilen von Berechtigungen für ein bestimmtes Computerkonto:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
<!--NeedCopy-->
```

Für die Aktionen “Prozess beenden”, “Anwendung beenden”und “Spiegeln”:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
<!--NeedCopy-->
```

Erteilen von Berechtigungen für eine Benutzergruppe:

```
ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
<!--NeedCopy-->
```

Anzeigen der Hilfe für das Tool:

```
ConfigRemoteMgmt.exe
<!--NeedCopy-->
```

Konfigurieren der Netzwerkanalyse

August 15, 2023

Hinweis: Die Verfügbarkeit dieser Funktion richtet sich nach der Lizenzierung und den Administratorberechtigungen.

Director ermöglicht in Kombination mit NetScaler Insight Center bzw. NetScaler MAS die Netzwerkanalyse und Leistungsverwaltung:

- Die Netzwerkanalyse nutzt HDX Insight-Berichte aus NetScaler Insight Center oder NetScaler MAS und liefert eine kontextbezogene Ansicht der Anwendungen und Desktops im Netzwerk. Director bietet mit diesem Feature eine erweiterte Analyse des ICA-Datenverkehrs in der Bereitstellung.
- Die Leistungsverwaltung bietet eine Verlaufsspeicherung und Trendberichte. Anhand der Beibehaltung historischer Daten können Sie im Gegensatz zur Echtzeitbewertung Trendberichte über Kapazität und Integrität usw. erstellen.

Nachdem Sie dieses Feature in Director aktivieren, liefern HDX Insight-Berichte zusätzliche Informationen an Director:

- Auf der Registerkarte "Netzwerk"der Seite "Trends"werden bereitstellungsübergreifend Auswirkungen auf Latenz und Bandbreite für Anwendungen, Desktops und Benutzer angezeigt.
- Auf der Seite Benutzerdetails werden Latenz- und Bandbreiteninformationen zu spezifischen Benutzersitzungen angezeigt.

Einschränkungen:

- Die Roundtripzeitdaten für die ICA-Sitzung werden in Receiver für Windows 3.4 oder höher und Receiver für Mac 11.8 oder höher richtig angezeigt. Bei früheren Versionen von Receiver werden die Daten nicht richtig angezeigt.
- In der Trendansicht werden Anmeldedaten für HDX-Verbindungen für VDAs vor Version 7 nicht gesammelt. Für frühere VDAs werden die Diagrammdaten als 0 angezeigt.

Zur Aktivierung der Netzwerkanalyse müssen Sie NetScaler Insight Center oder NetScaler MAS in Director installieren und konfigurieren. Director erfordert NetScaler MAS Version 11.1 Build 49.16 oder höher. Insight Center und MAS sind virtuelle Geräte, die unter Citrix XenServer ausgeführt werden. Mit der Netzwerkanalyse sammelt Director Daten zur Bereitstellung.

Weitere Informationen finden Sie in der Dokumentation zu NetScaler MAS.

1. Suchen Sie auf dem Server, auf dem Director installiert ist, das Befehlszeilentool DirectorConfig in C:\inetpub\wwwroot\Director\tools und führen Sie es mit dem Parameter "/configNetScaler" an der Eingabeaufforderung aus.
2. Wenn Sie dazu aufgefordert werden, geben Sie den Namen (FQDN oder IP-Adresse) der Maschine mit NetScaler Insight Center bzw. NetScaler MAS, den Benutzernamen, das Kennwort und den HTTP- oder HTTPS-Verbindungstyp ein und wählen Sie die NetScaler Insight Center- bzw. NetScaler MAS-Integration.
3. Melden Sie sich zum Prüfen der Änderungen ab und wieder an.

Behandeln von Benutzerproblemen

August 18, 2021

In der Ansicht **Helpdesk** (Seite **Aktivitätsmanager**) in Director zeigen Sie Informationen über den Benutzer an:

- Überprüfen Sie die Details zur Anmeldung des Benutzers, zur Verbindung und zu den Anwendungen.
- Spiegeln Sie die Maschine des Benutzers.
- Zeichnen Sie die ICA-Sitzung auf.
- Behandeln Sie das Problem mit den in der folgenden Tabelle empfohlenen Aktionen und eskalieren Sie das Problem ggf. an den entsprechenden Administrator.

Tipps zur Problembehandlung

Benutzerproblem	Vorschläge
Anmeldung dauert lange oder schlägt periodisch oder wiederholt fehl	Diagnose von Benutzeranmeldeproblemen
Anwendung ist langsam oder reagiert nicht mehr	Beheben von Anwendungsstörungen
Verbindung ist fehlgeschlagen	Wiederherstellen von Desktopverbindungen
Sitzung ist langsam oder reagiert nicht	Wiederherstellen von Sitzungen
Aufzeichnen von Sitzungen	Aufzeichnen von Sitzungen
Video ist langsam oder von schlechter Qualität	Ausführen von HDX-Kanalsystemberichten

Hinweis: Um sicherzustellen, dass die Maschine nicht im Wartungsmodus ist, überprüfen Sie in der Ansicht "Benutzerdetails"den Bereich "Maschinendetails".

Tipps zur Suche

Wenn Sie den Namen des Benutzers im Suchfeld eingeben, sucht Director in Active Directory nach Benutzern in allen Sites, die für Director konfiguriert wurden.

Wenn Sie den Namen einer Maschine, die von mehreren Benutzern verwendet wird, in ein Suchfeld eingeben, zeigt Director die Maschinendetails für die angegebene Maschine an.

Wenn Sie einen Endpunktnamen in ein Suchfeld eingeben, verwendet Director die nicht authentifizierten (anonymen) und die authentifizierten Sitzungen, die mit einem bestimmten Endpunkt verbunden sind, sodass Probleme in nicht authentifizierten Sitzungen behandelt werden können. Stellen Sie sicher, dass Endpunktnamen eindeutig sind, damit die Problembehandlung von nicht authentifizierten Sitzungen durchgeführt werden kann.

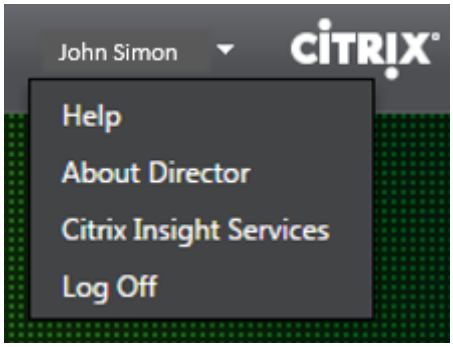
Die Suchergebnisse schließen auch Benutzer ein, die derzeit keine Maschine verwenden bzw. keiner Maschine zugewiesen sind.

- Bei der Suche wird die Groß- und Kleinschreibung nicht beachtet.
- Teileinträge ergeben eine Liste möglicher Übereinstimmungen.
- Nachdem Sie einige Buchstaben eines zweiteiligen Namens (Benutzername, Nachname und Vorname oder Anzeigename) durch Leerzeichen getrennt eingegeben haben, enthalten die Ergebnisse Übereinstimmungen für beide Zeichenfolgen. Wenn Sie zum Beispiel jo rob eingeben, werden Zeichenfolgen wie "John Robertson"oder "Robert, Jones"als Ergebnisse angezeigt.

Klicken Sie auf das Director-Logo, um zur Startseite zurückzukehren.

Zugreifen auf Citrix Insight Services

Für zusätzliche Diagnoseinformationen können Sie über die Dropdownliste "Benutzer"in Director auf Citrix Insight Services (CIS) zugreifen. Die Informationen in CIS stammen aus mehreren Quellen einschließlich Call Home und Citrix Scout.



Hochladen von Informationen zur Problembehandlung an den technischen Support von Citrix

Führen Sie Citrix Scout auf einem Delivery Controller oder VDA aus, um wichtige Datenpunkte und CDF-Traces (Citrix Diagnostics Facility) für die Fehlerbehebung auf ausgewählten Computern zu erfassen. Mit Scout können Sie Daten sicher an CIS hochladen, um den technischen Support von Citrix bei der Problembehandlung zu unterstützen. Der technische Support von Citrix nutzt die CIS-Plattform, um von Kunden gemeldete Probleme schneller zu lösen.

Scout wird mit XenApp- bzw. XenDesktop-Komponenten installiert. Je nach Windows-Version erscheint Scout im Startmenü bzw. Startbildschirm nach der Installation von (bzw. einem Upgrade auf) XenDesktop 7.1, XenDesktop 7.5, XenApp 7.5, XenDesktop 7.6, XenApp 7.6, XenDesktop 7.7 oder XenApp 7.7.

Zum Starten von Scout über das Startmenü oder den Startbildschirm wählen Sie "Citrix > Citrix Scout"
.

Informationen zum Verwenden und Konfigurieren von Scout und FAQ finden Sie unter CTX130147.

Senden von Nachrichten an Benutzer

July 1, 2019

Sie können über Director eine Nachricht an einen Benutzer senden, der mit einer oder mehreren Maschinen verbunden ist. Sie können beispielsweise mit dieser Funktion sofortige Benachrichtigun-

gen über administrative Aktionen senden, wie bevorstehende Desktopwartung, Abmeldungen bzw. Neustarts von Maschinen und das Zurücksetzen von Profilen.

1. Wählen Sie in der Ansicht Aktivitäts-Manager den Benutzer aus und klicken Sie auf Details.
2. Klicken in der Ansicht Benutzerdetails im Bereich Sitzungsdetails auf Nachricht senden.
3. Füllen Sie die Felder Betreff und Nachricht aus und klicken Sie auf Senden.

Wenn die Nachricht gesendet wird, wird in Director eine Bestätigungsmeldung angezeigt. Wenn die Maschine des Benutzers verbunden ist, wird dort eine entsprechende Nachricht angezeigt.

Wenn die Nachricht nicht gesendet wird, wird in Director eine Fehlermeldung angezeigt. Gehen Sie bei der Problembehandlung gemäß der Anweisungen in der Fehlermeldung vor. Geben Sie abschließend den Betreff und Text der Nachricht neu ein und klicken Sie auf Noch einmal versuchen.

Wiederherstellen von Sitzungen

August 18, 2021

Wenn eine Sitzung getrennt wird, bleibt sie aktiv und die Anwendungen werden weiter ausgeführt, das Benutzergerät kommuniziert jedoch nicht mehr mit dem Server.

Die Problembehandlung von Sitzungsfehlern erfolgt in der Ansicht “Benutzerdetails”im Bereich Sitzungsdetails. Sie können die Details der aktuellen Sitzung (durch die Sitzungs-ID gekennzeichnet) anzeigen.

Aktion	Beschreibung
Beenden von Anwendungen und Prozessen, die nicht reagieren	Klicken Sie auf die Registerkarte Anwendungen. Wählen Sie eine nicht reagierende Anwendung aus und klicken Sie auf Anwendung beenden. Sie können auch einen Prozess auswählen, der nicht reagiert, und auf Prozess beenden klicken. Beenden Sie auch Prozesse, die ungewöhnlich viel Speicher oder CPU-Ressourcen verbrauchen, da sie die CPU unbrauchbar machen können.
Trennen der Windows-Sitzung	Klicken Sie auf Sitzungssteuerung und wählen Sie dann Trennen. Diese Option steht nur für vermittelte Serverbetriebssystemmaschinen zur Verfügung. Für nicht vermittelte Sitzungen ist die Option deaktiviert.

Aktion	Beschreibung
Abmelden des Benutzers von der Sitzung	Klicken Sie auf Sitzungssteuerung und wählen Sie dann Abmelden.

Zum Testen der Sitzung kann der Benutzer versuchen, sich neu anzumelden. Sie können den Benutzer auch spiegeln, um diese Sitzung genauer zu beobachten.

Hinweis: Wenn VDAs vor XenDesktop 7 auf Benutzergeräten ausgeführt werden, kann Director keine vollständigen Informationen über die Sitzung anzeigen. Stattdessen wird in einer Meldung angezeigt, dass die Informationen nicht verfügbar sind. Diese Meldungen werden möglicherweise auf der Seite "Benutzerdetails"und im
Aktivitäts-Manager angezeigt.

Zurücksetzen von Personal vDisk

February 22, 2019

Achtung: Beim Zurücksetzen der Disk werden die Einstellungen auf die werksseitigen Standardwerte zurückgesetzt und alle Daten, einschließlich der Anwendungen, werden gelöscht. Die Profildaten bleiben gespeichert, es sei denn, Sie haben den Personal vDisk-Standard geändert (d. h. das Umleiten der Profile vom Laufwerk C:) oder Sie verwenden keine Profillösung eines Drittanbieters.

Zum Zurücksetzen muss die Maschine mit Personal vDisk ausgeführt werden, der Benutzer muss aber nicht angemeldet sein.

Diese Option steht nur für Desktopbetriebssystemmaschinen zur Verfügung, sie ist für Serverbetriebssystemmaschinen deaktiviert.

1. Wählen Sie in der Ansicht Helpdesk die gewünschte Desktopbetriebssystemmaschine aus.
2. Klicken Sie in dieser Ansicht oder im Bereich Personalisierung der Ansicht Benutzerdetails auf Personal vDisk zurücksetzen.
3. Klicken Sie auf Zurücksetzen. Eine Warnmeldung gibt an, dass der Benutzer abgemeldet wird. Wenn der Benutzer abgemeldet ist (falls er angemeldet war), wird die Maschine neu gestartet.

Wenn das Zurücksetzen erfolgreich ist, wird im Feld Status im Bereich Personalisierung der Ansicht Benutzerdetails der Wert Wird ausgeführt angezeigt. Wenn das Zurücksetzen fehlgeschlagen ist, wird rechts neben"Wird ausgeführt"ein rotes X angezeigt. Wenn Sie auf dieses X zeigen, werden Informationen zu dem Fehler angezeigt.

Ausführen von HDX-Kanalsystemberichten

February 22, 2019

Prüfen Sie in der Ansicht "Benutzerdetails"im Bereich "HDX"den Status der HDX-Kanäle auf der Maschine des Benutzers. Dieser Bereich ist nur verfügbar, wenn die Maschine des Benutzers mit HDX verbunden ist.

Wenn eine Meldung angibt, dass die Informationen zurzeit nicht verfügbar sind, warten Sie eine Minute, bis die Seite aktualisiert ist, oder klicken Sie auf die Schaltfläche Aktualisieren. Die Aktualisierung von HDX-Daten kann etwas länger dauern als bei anderen Daten.

Klicken Sie zur Anzeige weiterer Informationen auf das Fehler- oder Warnsymbol.

Tipp: Sie können Informationen über andere Kanäle in demselben Dialogfeld einblenden, indem Sie in der linken Ecke der Titelleiste auf den Pfeil nach links oder rechts klicken.

Systemberichte über die HDX-Kanäle werden hauptsächlich vom Citrix Support für die weitere Problembehandlung verwendet.

1. Klicken Sie im Bereich HDX auf Systembericht herunterladen.
2. Sie können die XML-Berichtdatei anzeigen oder speichern.
    - Klicken Sie zur Ansicht der XML-Datei auf Öffnen. Die XML-Datei wird in demselben Fenster wie die Anwendung Director angezeigt.
    - Klicken Sie zum Speichern der XML-Datei auf Speichern. Das Dialogfeld Speichern unter wird angezeigt, in dem Sie angeben, an welchem Speicherort auf der Director-Maschine die Datei heruntergeladen wird.

Spiegeln von Benutzern

August 18, 2021

Mit dem Feature Benutzer spiegeln in Director können Sie die virtuelle Maschine oder Sitzung eines Benutzers direkt anzeigen und damit arbeiten. Der Benutzer muss mit der zu spiegelnden Maschine verbunden sein. Wenn der Benutzer verbunden ist, wird der Name der verbundenen Maschine in der Titelleiste des Benutzers angezeigt.

1. Wählen Sie in der Ansicht Details die Benutzersitzung aus.
2. Aktivieren Sie die Spiegelung für die ausgewählte Benutzersitzung:
    - Klicken Sie zur Maschinenüberwachung in der Ansicht Aktivitäts-Manager auf Spiegeln.

- Klicken Sie zur Sitzungsüberwachung in der Ansicht Benutzerdetails im Bereich Sitzungsdetails auf Spiegeln.

3. Nach Initialisierung der Verbindung werden Sie in einem Dialogfeld aufgefordert, die MSRCINCIDENT-Datei zu öffnen oder zu speichern.
4. Öffnen Sie die Vorfalldatei mit dem Remoteunterstützung-Viewer, wenn er nicht standardmäßig ausgewählt ist. Auf dem Benutzergerät wird eine Bestätigungsaufforderung angezeigt.
5. Weisen Sie die Benutzer an, auf Ja zu klicken, um die Maschinen- oder die Sitzungsfreigabe zu starten.

Fordern Sie den Benutzer auf, die Tastatur- und Maussteuerung freizugeben, damit Sie die Steuerung übernehmen können.

Anpassen des Microsoft Internet Explorer-Browsers für das Spiegeln

Richten Sie den Microsoft Internet Explorer-Browser so ein, dass die heruntergeladene Datei zur Microsoft-Remoteunterstützung (.msra) automatisch mit dem Remoteunterstützungsclient geöffnet wird.

Hierzu müssen Sie die Einstellung Automatische Eingabeaufforderung für Dateidownloads im Gruppenrichtlinien-Editor aktivieren:

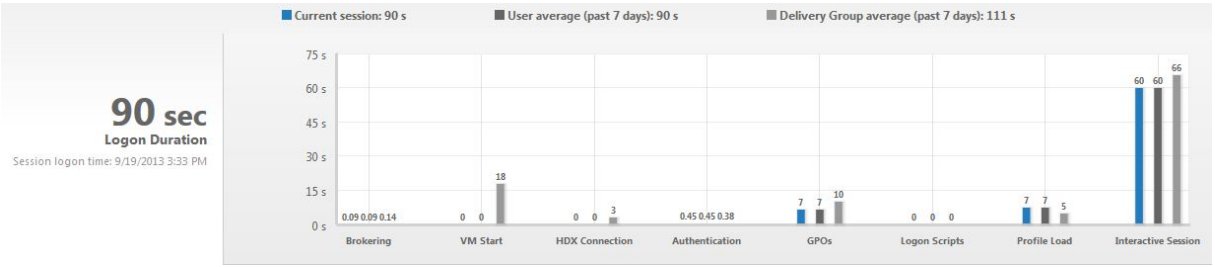
Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer > Internetsystemsteuerung > Sicherheitsseite > Internetzone > Automatische Eingabeaufforderung für Dateidownloads.

Diese Option ist standardmäßig für Sites in der lokalen Intranetzone aktiviert. Wenn die Director-Site nicht zur lokalen Intranetzone gehört, sollten Sie die Site manuell dieser Zone hinzufügen.

Diagnose von Benutzeranmeldeproblemen

November 29, 2018

Mit den Anmeldedauerdaten können Sie Benutzeranmeldeprobleme beheben. In der Ansicht “Benutzerdetails”wird die Dauer als ein Zahlenwert angezeigt, darunter die Anmeldezeit und ein Diagramm der Phasen des Anmeldeprozesses.



Wenn Benutzer sich bei XenApp und XenDesktop anmelden, verfolgt der Überwachungsdienst die Phasen des Anmeldeprozesses ab Herstellung der Verbindung über Citrix Receiver bis zu dem Moment, in dem der Desktop einsatzbereit ist. Die hohe Zahl auf der linken Seite repräsentiert die Gesamtdauer der Anmeldung. Sie errechnet sich aus der auf das Herstellen der Verbindung und das Abrufen eines Desktops vom Delivery Controller aufgewendeten Zeit plus der für Authentifizierung und Anmeldung bei einem virtuellen Desktop aufgewendeten Zeit. Die Dauer wird in Sekunden (oder Sekundenbruchteilen) in der lokalen Zeit im Webbrowser des Administrators angezeigt.

Mit den folgenden allgemeinen Schritten beheben Sie Benutzeranmeldeprobleme:

1. Überprüfen Sie in der Ansicht **Benutzerdetails** im Bereich "Anmeldedauer", welcher Anmeldezustand vorliegt.
    - Wenn Benutzer sich anmelden, wird der Anmeldeprozess in der Ansicht widergespiegelt.
    - Wenn der Benutzer bereits angemeldet ist, wird im Bereich "Anmeldedauer"angezeigt, wie viel Zeit für die Anmeldung an der aktuellen Sitzung benötigt wurde.
2. Überprüfen Sie die Phasen des Anmeldeprozesses.

Phase des Anmeldeprozesses	Beschreibung
Vermittlung	Zur Zuweisung des Desktops zum Benutzer benötigte Zeit.
VM-Start	Zum Starten einer virtuellen Maschine benötigte Zeit, wenn eine Sitzung den Start einer Maschine erforderte.
HDX-Verbindung	Zum Einrichten der HDX-Verbindung vom Client zur virtuellen Maschine benötigte Zeit.
Authentifizierung	Zum Abschließen der Authentifizierung bei der Remotesitzung benötigte Zeit.
Gruppenrichtlinienobjekte	Zum Anwenden von Gruppenrichtlinienobjekten benötigte Zeit, wenn Gruppenrichtlinieneinstellungen auf den virtuellen Maschinen aktiviert sind.

Phase des Anmeldeprozesses	Beschreibung
Anmeldeskripts	Zum Ausführen von Anmeldeskripts benötigte Zeit, wenn Anmeldeskripts für die Sitzung konfiguriert sind.
Profilladezeit	Zum Laden des Profils benötigte Zeit, wenn für den Benutzer Profileinstellungen auf der virtuellen Maschine konfiguriert sind.
Interaktive Sitzung	Zum Übergeben von Tastatur- und Maussteuerung an den Benutzer benötigte Zeit, nachdem das Profil geladen wurde. Dies dauert normalerweise am längsten von allen Phasen des Anmeldeprozesses und wird wie folgt berechnet: **Dauer der interaktiven Sitzung = Zeitstempel des Ereignisses "Desktop bereit" (Ereignis-ID 1000 auf VDA) - Zeitstempel des Ereignisses "Profilladezeit"(Ereignis-ID 2 auf VDA)**.

Die Gesamtanmeldedauer ist keine genaue Summe der einzelnen Phasen. Beispiel: Einige Phasen treten parallel auf und in anderen Phasen wird eine zusätzliche Verarbeitung durchgeführt, die zu einer längeren Anmeldedauer als die Summe der einzelnen Phasen führen kann.

Hinweis: Im Anmeldedauerdiagramm werden die Anmeldephasen in Sekunden angezeigt. Zeitwerte unter einer Sekunde werden als Sekundenbruchteile angezeigt. Werte, die größer sind als eine Sekunde, werden auf die nächste halbe Sekunde aufgerundet. Aufgrund des Diagrammdesigns kann ein Höchstwert von 200 Sekunden auf der Y-Achse angezeigt werden. Bei Werten über 200 Sekunden wird der tatsächliche Wert über dem Balken angezeigt.

Tipps zur Problembehandlung

Um ungewöhnliche oder unerwartete Werte im Diagramm zu finden, vergleichen Sie die in jeder Phase der aktuellen Sitzung benötigte Zeit mit der durchschnittlichen Dauer für diesen Benutzer in den letzten sieben Tagen sowie mit der durchschnittlichen Dauer in den letzten sieben Tagen für alle Benutzer diese Bereitstellungsgruppe.

Eskalieren Sie wie erforderlich. Beispiel: Wenn der VM-Start langsam ist, liegt das Problem möglicherweise am Hypervisor, Sie können das Problem also an den Hypervisoradministrator eskalieren. Wenn die Vermittlungsdauer zu lang ist, können Sie das Problem dem Siteadministrator melden, damit der Lastausgleich auf dem Delivery Controller überprüft wird.

Überprüfen Sie ungewöhnliche Unterschiede, u. a.:

- Fehlende (aktuelle) Anmeldeleisten
- Große Abweichung zwischen der aktuellen und der durchschnittlichen Dauer für diesen Benutzer. Mögliche Ursachen:
  - Es wurde eine neue Anwendung installiert.
  - Das Betriebssystem wurde aktualisiert.
  - Es wurden Konfigurationsänderungen vorgenommen.
  - Das Profil des Benutzers ist sehr groß. In diesem Fall ist auch die Profilladezeit hoch.
- Große Abweichung zwischen den Anmeldewerten des Benutzers (aktuelle und durchschnittliche Dauer) und der durchschnittlichen Dauer der Bereitstellungsgruppe.

Klicken Sie ggf. auf **Neu starten**, um den Anmeldeprozess des Benutzers zu beobachten und Probleme zu beheben, z. B. VM-Start oder Brokering.

Aufzeichnen von Sitzungen

August 18, 2021

Sie können mit den Steuerelementen der Sitzungsaufzeichnung der Seiten **Benutzerdetails** und **Maschinendetails** in Director ICA-Sitzungen aufzeichnen. Dieses Feature steht bei Sites mit **Platinum**-Lizenz zur Verfügung.

Informationen zum Konfigurieren der Sitzungsaufzeichnung unter Director mit dem DirectorConfig-Tool finden Sie unter **Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers** im Abschnitt Installieren, Aktualisieren und Deinstallieren der Sitzungsaufzeichnung.
Die Steuerelemente der Sitzungsaufzeichnung sind in Director nur dann verfügbar, wenn der angemeldete Benutzer die Berechtigung zum Ändern der Richtlinien für die Sitzungsaufzeichnung hat. Diese Berechtigung kann in der Autorisierungskonsole für die Citrix Sitzungsaufzeichnung eingestellt werden (siehe Erstellen und Aktivieren von Aufzeichnungsrichtlinien).
Hinweis: Über Director oder die Richtlinienkonsole für die Sitzungsaufzeichnung gemachte Änderungen an den Einstellungen für die Sitzungsaufzeichnung werden in den nachfolgenden ICA-Sitzungen wirksam.

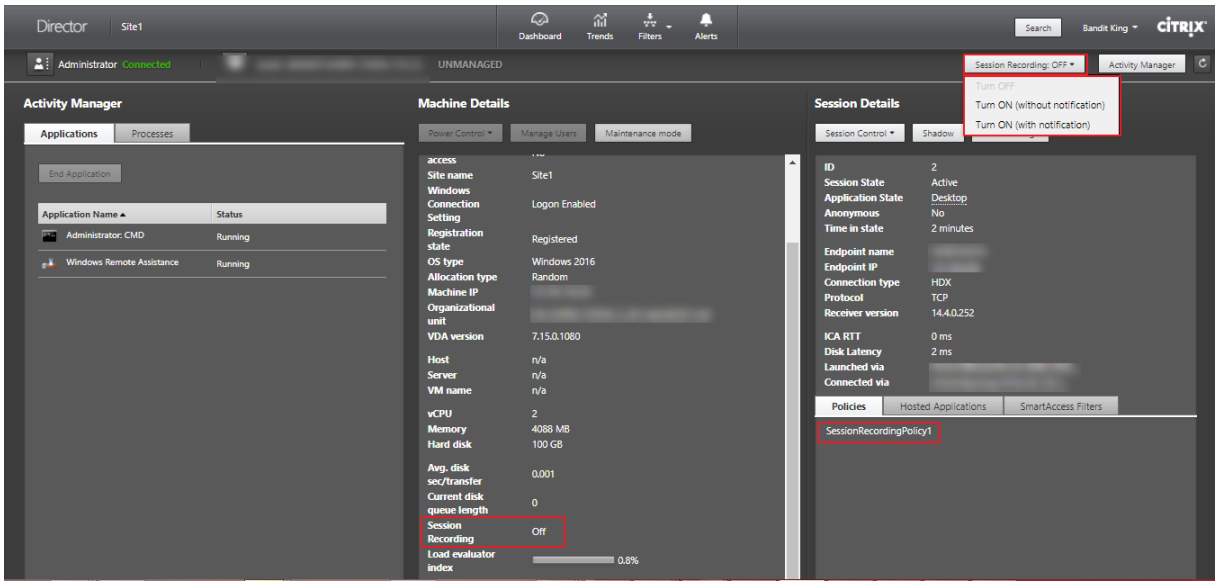
Steuerelemente der Sitzungsaufzeichnung in Director

Sie können die Sitzungsaufzeichnung für einzelne Benutzer auf der Seite **Aktivitätsmanager** oder **Benutzerdetails** aktivieren. Anschließende Sitzungen werden für den Benutzer dann auf allen unterstützten Servern aufgezeichnet.

Sie haben folgende Möglichkeiten:

- Einschalten (mit Benachrichtigung): Der Benutzer wird über die Aufzeichnung der Sitzung beim Anmelden bei der ICA-Sitzung benachrichtigt.
- Einschalten (ohne Benachrichtigung): Die Sitzung wird ohne Benachrichtigung des Benutzers aufgezeichnet.
- Ausschalten: Die Aufzeichnung von Sitzungen wird für den Benutzer deaktiviert.

Im Bereich Richtlinie wird der Name der aktiven Sitzungsaufzeichnungsrichtlinie angezeigt.



Sie können die Sitzungsaufzeichnung für einzelne Maschinen über die Seite "Maschinendetails"aktivieren. Auf der Maschine werden dann nachfolgende Sitzungen aufgezeichnet. Im Bereich Maschinendetails wird der Status der Sitzungsaufzeichnungsrichtlinie für die Maschine angezeigt.

Wiederherstellen von Desktopverbindungen

November 29, 2018

Überprüfen Sie von Director den Verbindungsstatus des Benutzers für die aktuelle Maschine in der Titelleiste des Benutzers.

Wenn die Desktopverbindung fehlgeschlagen ist, wird die Fehlerursache angezeigt, um Sie bei der Problembehandlung zu unterstützen.

Aktion	Beschreibung
Stellen Sie sicher, dass die Maschine nicht im Wartungsmodus ist.	Achten Sie auf der Seite Benutzerdetails darauf, dass der Wartungsmodus deaktiviert ist.
Neustarten der Maschine des Benutzers	Wählen Sie die Maschine aus und klicken Sie auf Neu starten. Verwenden Sie diese Option, wenn die Maschine des Benutzers nicht mehr reagiert oder keine Verbindung herstellen kann, z. B. wenn die Maschine sehr viele CPU-Ressourcen verbraucht und dies die CPU unbrauchbar macht.

Beheben von Anwendungsstörungen

August 18, 2021

Klicken Sie in der Ansicht **Aktivitätsmanager** auf die Registerkarte **Anwendungen**. Sie können alle Anwendungen auf allen Maschinen anzeigen, auf die dieser Benutzer zugreifen kann, einschließlich der lokalen und der gehosteten Anwendungen für die derzeit verbundene Maschine und den aktuellen Status der einzelnen Maschine.

Hinweis: Wenn die Registerkarte “Anwendungen”abgeblendet ist, wenden Sie sich an einen Administrator, der die Berechtigung hat, die Registerkarte zu aktivieren.

Die Liste enthält nur die Anwendungen, die in der Sitzung gestartet wurden.

Für Serverbetriebssystemmaschinen und Desktopbetriebssystemmaschinen werden Anwendungen für jede getrennte Sitzung angezeigt. Wenn der Benutzer nicht verbunden ist, werden keine Anwendungen angezeigt.

Aktion	Beschreibung
Beenden der Anwendung, die nicht reagiert	Wählen Sie die Anwendung aus, die nicht reagiert, und klicken Sie auf Anwendung beenden. Wenn die Anwendung beendet ist, fordern Sie den Benutzer auf, sie neu zu starten.
Beenden von Prozessen, die nicht reagieren	Wenn Sie die erforderlichen Berechtigungen haben, klicken Sie auf die Registerkarte Prozesse. Wählen Sie einen Prozess aus, der mit dieser Anwendung zusammenhängt oder der viele CPU-Ressourcen oder viel Speicher verbraucht, und klicken Sie auf Prozess beenden. Wenn Sie nicht die erforderlichen Berechtigungen zum Beenden des Prozesses haben, schlägt das Beenden fehl.
Neustarten der Maschine des Benutzers	Nur Desktopbetriebssystemmaschinen: Klicken Sie für die ausgewählte Sitzung auf “Neu starten”. Sie können auch in der Ansicht “Maschinendetails”die Maschine mit den Energiesteuerelementen neu starten oder herunterfahren. Fordern Sie den Benutzer auf, sich neu anzumelden, sodass Sie die Anwendung überprüfen können. Für Serverbetriebssystemmaschinen steht die Option “Neu starten”nicht zur Verfügung. Melden Sie stattdessen den Benutzer ab und fordern Sie ihn auf, sich neu anzumelden.
Versetzen der Maschine in den Wartungsmodus	Wenn das Image einer Maschine gewartet werden muss, z. B. mit Patches oder anderen Updates, versetzen Sie die Maschine in den Wartungsmodus. Klicken Sie in der Ansicht “Maschinendetails”auf Details und aktivieren Sie die Option “Wartungsmodus”. Eskalieren Sie an den entsprechenden Administrator.

Zurücksetzen eines Benutzerprofils

August 18, 2021

Achtung: Wenn ein Profil zurückgesetzt wird, werden die Ordner und Dateien des Benutzers zwar gespeichert und in das neue Profil kopiert, aber die meisten Benutzerdaten werden gelöscht (z. B. wird die Registrierung zurückgesetzt und die Anwendungseinstellungen werden möglicherweise gelöscht).

1. Suchen Sie in Director den Benutzer, dessen Profil Sie zurücksetzen möchten, und wählen Sie seine Benutzersitzung aus.
2. Klicken Sie auf **Profil zurücksetzen**.
3. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
4. Fordern Sie den Benutzer auf, sich neu anzumelden. Der Ordner und Dateien, die aus dem Profil des Benutzers gespeichert wurden, werden in das neue Profil kopiert.
   Wichtig: Wenn der Benutzer Profile auf mehreren Plattformen (z. B. Windows 8 und Windows 7) hat, fordern Sie ihn auf, sich zuerst bei dem gleichen Desktop oder bei der gleichen App anzumelden, bei dem bzw. der er Probleme hatte. Dies stellt sicher, dass das richtige Profil zurückgesetzt wird.
   Wenn das Profil ein Citrix Benutzerprofil ist, ist es zum Zeitpunkt der Benutzerdesktopanzeige bereits zurückgesetzt. Bei Microsoft-Roamingprofilen dauert die Ordnerwiederherstellung möglicherweise noch kurze Zeit an. Der Benutzer muss angemeldet bleiben, bis die Wiederherstellung abgeschlossen ist.

Hinweis: Bei den zuvor erläuterten Schritten wird davon ausgegangen, dass Sie XenDesktop (Desktop-VDA) verwenden. Wenn Sie XenApp (Server-VDA) verwenden, müssen Sie angemeldet sein, um das Profil zurückzusetzen. Der Benutzer muss sich dann abmelden und neu anmelden, um das Zurücksetzen des Profils abzuschließen.

Wenn das Profil nicht erfolgreich zurückgesetzt wird (z. B. der Benutzer kann sich nicht wieder anmelden oder einige der Dateien fehlen), müssen Sie das ursprüngliche Profil manuell wiederherstellen.

Die Ordner (und die Dateien) des Benutzerprofils werden gespeichert und in das neue Profil kopiert. Dabei gilt folgende Kopierreihenfolge:

- Desktop
- Cookies
- Favoriten
- Documente
- Bilder
- Musik

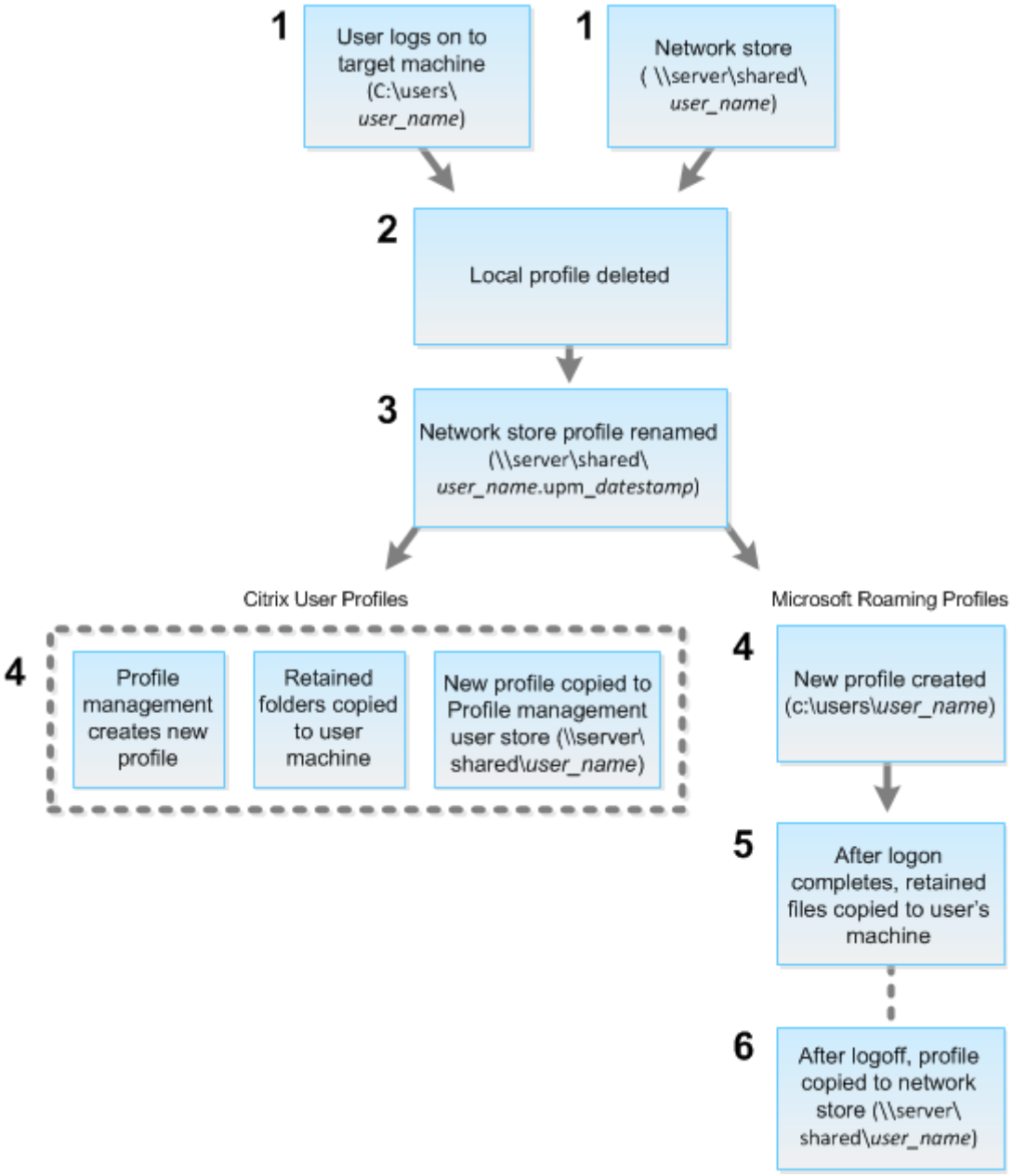
- Videos

Hinweis: In Windows 8 und höheren Versionen werden Cookies beim Zurücksetzen des Profils nicht kopiert.

Verarbeiten von zurückgesetzten Profilen

Alle Citrix Benutzerprofile oder Microsoft Roamingprofile können zurückgesetzt werden. Wenn der Benutzer sich abmeldet und Sie den Befehl zum Zurücksetzen wählen (entweder in Director oder mit dem PowerShell SDK), identifiziert Director zunächst das verwendete Benutzerprofil und gibt dann den entsprechenden Befehl zum Zurücksetzen. Director erhält die Informationen über die Profilverwaltung, einschließlich Informationen zur Profilgröße, zum Typ und den Anmeldezeiten.

Dieses Diagramm zeigt den Prozess, der auf die Benutzeranmeldung folgt.



1. Der Befehl zum Zurücksetzen von Director gibt den Profiltyp an. Der Profilverwaltungsdienst versucht dann, ein Profil dieses Typs zurückzusetzen und sucht die entsprechende Netzwerkfreigabe (Benutzerspeicher). Wenn der Benutzer von der Profilverwaltung verarbeitet wird, aber einen Roamingprofilbefehl erhält, wird er abgelehnt (oder umgekehrt).
2. Wenn ein lokales Profil vorhanden ist, wird es gelöscht.
3. Das Netzwerkprofil wird umbenannt.
4. Die nächste Aktion hängt davon ab, ob es sich bei dem Profil, das zurückgesetzt wird, um ein Citrix Benutzerprofil oder ein Microsoft Roamingprofil handelt.

    - Für Citrix Benutzerprofile wird das neue Profil mit den Importregeln der Profilverwaltung

erstellt, die Ordner werden in das Netzwerkprofil zurückkopiert und der Benutzer kann sich wie gewohnt anmelden. Wenn ein Roamingprofil für das Zurücksetzen verwendet wird, bleiben alle Registrierungseinstellungen im Roamingprofil im zurückgesetzten Profil gespeichert.
Hinweis: Sie können in der Profilverwaltung konfigurieren, dass das Roamingprofil ggf. von einem Vorlagenprofil überschrieben wird.

- Für Microsoft Roamingprofile wird ein neues Profil von Windows erstellt, und die Ordner werden bei Anmeldung des Benutzers auf das Benutzergerät zurückkopiert. Bei der nächsten Benutzerabmeldung wird das neue Profil in den Netzwerkspeicher kopiert.

Manuelles Wiederherstellen eines Profils nach einer fehlgeschlagenen Zurücksetzung

1. Fordern Sie den Benutzer auf, sich von allen Sitzungen abzumelden.
2. Löschen Sie das lokale Profil, sofern vorhanden.
3. Suchen Sie den archivierten Ordner auf der Netzwerkfreigabe, bei dem das Datum und die Uhrzeit dem Ordnernamen angehängt wurden, also den Ordner mit der Erweiterung .upm_datumsstempel.
4. Löschen Sie den aktuellen Profilnamen, d. h. die Datei ohne die Erweiterung upm_datumsstempel.
5. Benennen Sie den archivierten Ordner unter Verwendung des ursprünglichen Profilnamens (d. h. ohne Datums- und Uhrzeitangabe) um. Sie haben das Profil auf den ursprünglichen Zustand zurückgesetzt.

Problembehandlung bei Anwendungen

August 18, 2021

Überwachen von Anwendungen in Echtzeit

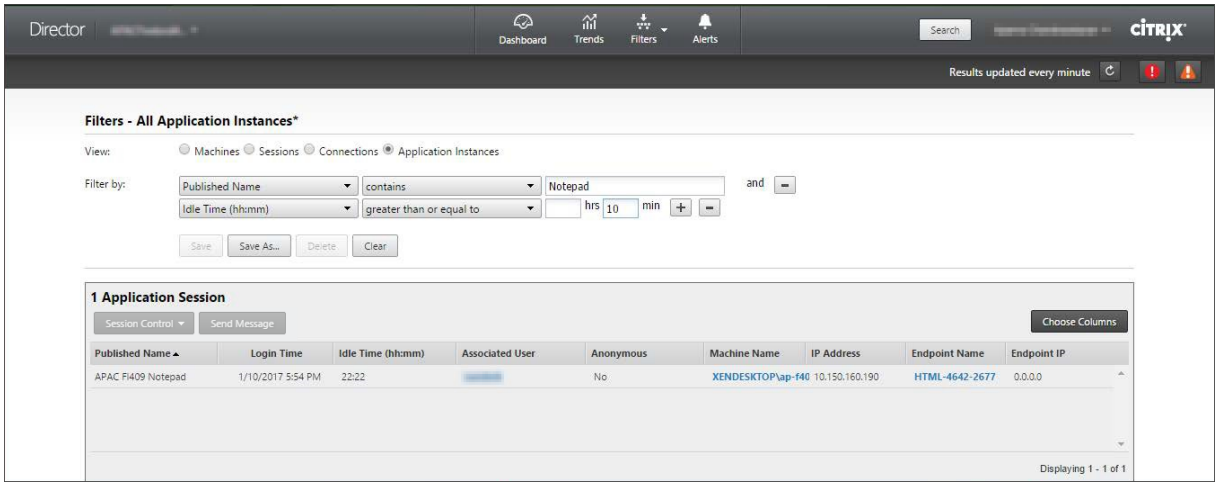
Zur Problembehandlung bei Anwendungen und Sitzungen können Sie anhand von Leerlaufkennzahlen feststellen, welche Instanzen über ein bestimmtes Zeitlimit hinaus inaktiv bleiben.

Typische Einsatzbereiche für die Problembehandlung bei Anwendungen ist der Gesundheitssektor, wo Mitarbeiter Anwendungslizenzen gemeinsam verwenden. Sie müssen dort Sitzungen und Anwendungsinstanzen im Leerlauf beenden, um die XenApp- und XenDesktop-Umgebung zu bereinigen, Server mit schlechter Leistung neu zu konfigurieren oder Anwendungen zu warten oder zu aktualisieren.

Die Filterseite **Anwendungsinstanzen** enthält alle Instanzen von Anwendungen auf VDAs für Server- und Desktopbetriebssysteme. Die Leerlaufzeit wird für Anwendungsinstanzen auf Serverbetriebssystem-VDAs angezeigt, die mindestens 10 Minuten im Leerlauf sind.

Hinweis: Die Kennzahlen für Anwendungsinstanzen stehen in Sites mit allen Lizenztypen zur Verfügung.

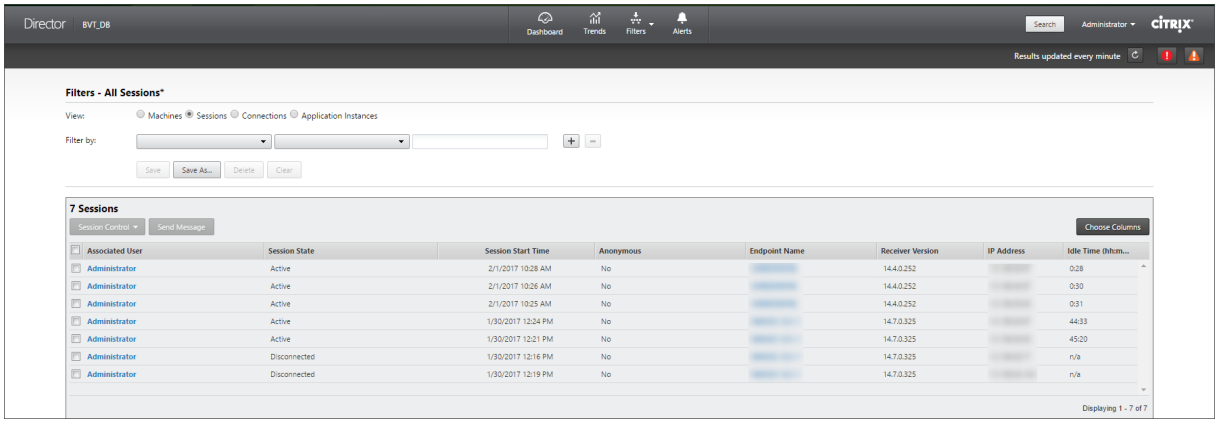
Anhand dieser Informationen können Sie Instanzen suchen, die länger als vorgegeben im Leerlauf sind und diese abmelden oder trennen. Wählen Sie hierfür **Filter > Anwendungsinstanzen** und wählen Sie einen vorhandenen Filter oder **Alle Anwendungsinstanzen** und erstellen Sie Ihren eigenen Filter.



Beispiel für einen Filter: Wählen Sie für **Filtern nach** die Kriterien **Veröffentlichter Name** (der Anwendung) und **Leerlaufzeit**. Legen Sie für **Leerlaufzeit** unter **größer als oder gleich** ein Zeitlimit fest und speichern Sie den Filter. Wählen Sie aus der gefilterten Liste die Anwendungsinstanzen aus. Wählen Sie die Option zum Senden von Nachrichten oder wählen Sie im Dropdownmenü **Sitzungssteuerung** den Befehl **Abmelden** oder **Trennen**, um die Instanzen zu beenden.

Hinweis: Diese Aktion trennt die aktuelle Sitzung bzw. meldet sie ab und damit auch alle zu der Sitzung gehörenden Anwendungsinstanzen.

Sie können Sitzungen im Leerlauf auf der Filterseite **Sitzungen** über den Sitzungszustand und die Leerlaufkennzahl suchen. Sortieren Sie die Anzeige nach der Spalte **Leerlaufzeit** oder definieren Sie einen Filter, um Sitzungen zu identifizieren, die über eine bestimmte Zeitspanne hinaus inaktiv sind. Die Leerlaufzeit wird für Sitzungen auf Serverbetriebssystem-VDAs aufgelistet, die mindestens 10 Minuten im Leerlauf sind.



Für **Leerlaufzeit** wird **Nicht zutreffend** angezeigt, wenn die Sitzungs- oder Anwendungsinstanz

- erst bis zu 10 Minuten im Leerlauf ist
- auf einem Desktopbetriebssystem-VDA gestartet wurde
- oder auf einem VDA einer Version bis 7.12 ausgeführt wird

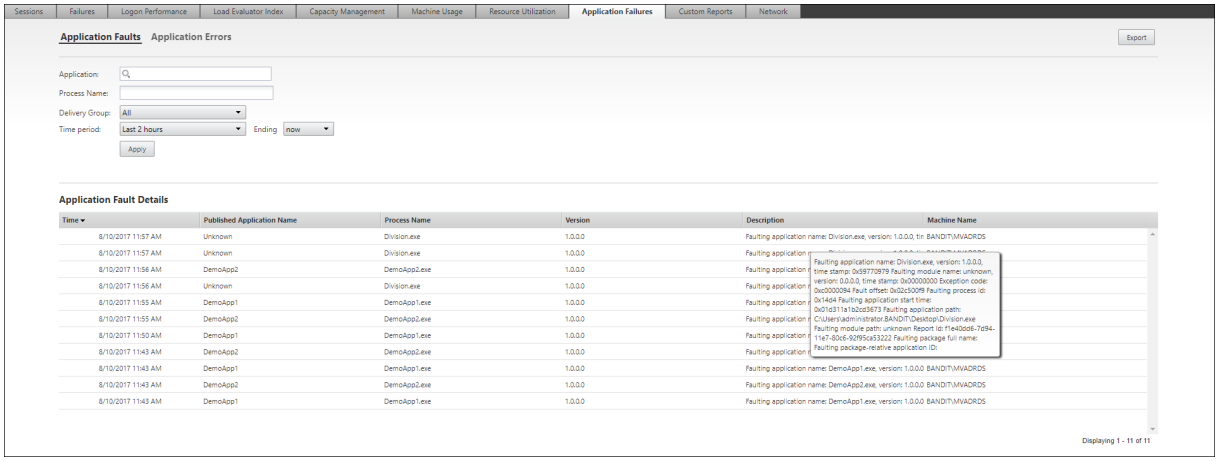
Überwachen historischer Anwendungsstörungen

Auf der Registerkarte **Trends** > **Anwendungsstörungen** werden Fehler bei den veröffentlichten Anwendungen auf den VDAs angezeigt.

Anwendungsstörungstrends für Sites mit Platinum- oder Enterprise-Lizenz für die letzten 2 oder 24 Stunden, die letzten 7 Tage und den letzten Monat zur Verfügung. Für Sites mit anderen Lizenzen stehen sie für die letzten 2 oder 24 Stunden und die letzten 7 Tage zur Verfügung. Es werden Anwendungstörungen überwacht, die in der Ereignisanzeige mit der Quelle “Anwendungsfehler”protokolliert werden. Klicken Sie auf **Exportieren** zum Generieren von Berichten im CSV-, Excel- oder PDF-Format.

Die Einstellungen zur Datenaufbewahrung für die Überwachung von Anwendungsstörungen, “GroomApplicationErrorsRetentionDays”und “GroomApplicationFaultsRetentionDays”, sind in der Standardeinstellung für Sites mit Platinum und anderen Lizenzen auf einen Tag festgelegt. Sie können diese Einstellung mit folgendem PowerShell-Befehl ändern:

```
*Set-MonitorConfiguration -\<setting name\> \<value\>*
```

Anwendungsstörungen werden basierend auf dem Schweregrad als **Anwendungsausfall** oder als **Anwendungsfehler** klassifiziert. Auf der Registerkarte "Anwendungsausfälle"werden Fehler angezeigt, die zum Verlust von Funktionalität oder Daten führen. Anwendungsfehler sind Probleme ohne direkte Relevanz, die ggf. zukünftige Probleme verursachen können.

Zum Filtern der Störungen stehen folgende Optionen zur Verfügung: **Name der veröffentlichten Anwendung**, **Prozessname**, **Bereitstellungsgruppe** und **Zeitraum**. Die Tabelle enthält den Fehler bzw. Fehlercode und eine kurze Problembeschreibung. Detaillierte Fehlerbeschreibungen werden als QuickInfo angezeigt.

Hinweis: Der Name der veröffentlichten Anwendung wird als "Unbekannt"angezeigt, wenn der Name der entsprechenden Anwendung nicht ermittelt werden kann. Das ist normalerweise der Fall, wenn bei einer gestarteten Anwendung in einer Desktopsitzung ein Fehler auftritt oder wenn ein Fehler die Folge einer unbehandelten, durch eine abhängige ausführbare Datei verursachten Ausnahme ist.

Standardmäßig werden nur Störungen von Anwendungen überwacht, die auf Serverbetriebssystem-VDAs gehostet werden. Sie können die Überwachungseinstellungen über die Überwachungsgruppenrichtlinien ändern: "Überwachung von Anwendungsausfällen aktivieren", "Überwachung von Ausfällen auf Desktop-OS-VDAs"und "Von der Fehlerüberwachung ausgeschlossene Anwendungen" . Weitere Informationen finden Sie unter Richtlinien für die Überwachung auf Anwendungsfehler im Artikel "Einstellungen der Überwachungsrichtlinie".

Problembehandlung bei Maschinen

August 18, 2021

Wählen Sie in der Ansicht **Filter** > **Maschinen** die Option **Desktopbetriebssystemmaschinen** oder **Serverbetriebssystemmaschinen**, um die in der Site konfigurierten Maschinen anzuzeigen. Die Registerkarte "Server-OS-Maschinen"enthält den Lastauswertungsindex, der die Verteilung der

Leistungsindikatoren und Quickinfo der Sitzungsanzahl angibt, wenn Sie mit dem Mauszeiger auf den Link zeigen.

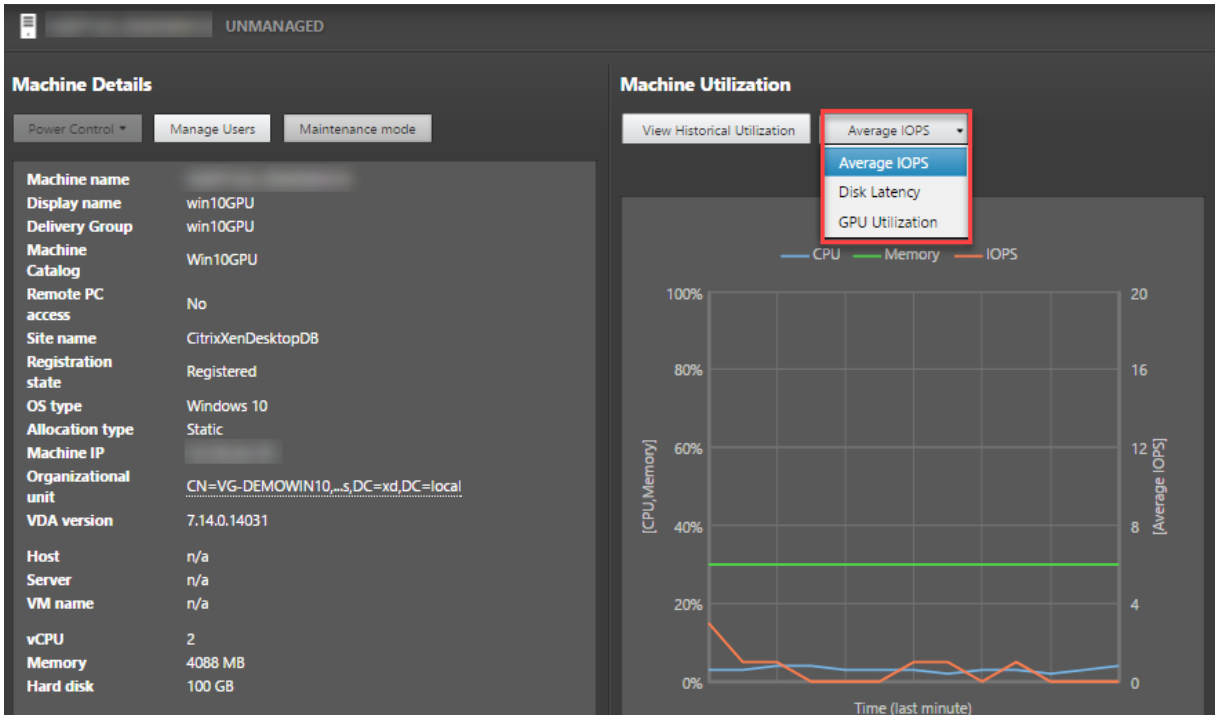
Klicken Sie für fehlerhafte Maschinen auf **Fehlerursache**, um eine detaillierte Beschreibung des Fehlers und Empfehlungen zur Behebung aufzurufen. Informationen zu Ursachen von Maschinen- und Verbindungsfehler sowie empfohlene Korrekturmaßnahmen finden Sie in dem Handbuch Citrix Director 7.12 Failure Reasons Troubleshooting Guide.

Klicken Sie auf Link mit dem Maschinennamen, um die Seite **Maschinendetails** aufzurufen. Die Seite "Maschinendetails"enthält die Einzelheiten zu der Maschine, der Infrastruktur und den auf die Maschine angewandten Hotfixes. Der Bereich **Maschinenauslastung** enthält die Maschinenauslastung in Diagrammform.

Echtzeit-Ressourcennutzung auf Maschinen

Im Bereich **Maschinenauslastung** wird die Echtzeit-Auslastung von CPU und Speicher angezeigt. Darüber hinaus stehen für Sites mit Delivery Controller(n) und VDAs ab Version **7.14** Diagramme zur Datenträger- und GPU-Überwachung zur Verfügung.

Datenträgerüberwachung, durchschnittliche IOPS und Datenträgerlatenz sind wichtige Kennzahlen für die Leistungsmessung, mit deren Hilfe Sie VDAs überwachen und Probleme bei VDA-Datenträgern beheben können. Das Diagramm der durchschnittlichen IOPS repräsentiert die durchschnittliche Zahl der Lese-/Schreibvorgänge auf einem Datenträger. Wählen Sie **Datenträgerlatenz**, um ein Diagramm der Verzögerung zwischen Datenanforderungen und Datenrückgabe vom Datenträger in Millisekunden anzuzeigen.



Über **GPU-Auslastung** können Sie die prozentuale Auslastung von GPU, GPU-Speicher und Encoder sowie Decoder aufrufen und anhand dieser Informationen GPU-Probleme auf Serverbetriebssystem- oder Desktopbetriebssystem-VDAs behandeln. Die GPU-Auslastungsdiagramme stehen nur bei VDAs mit 64-Bit-Versionen von Windows, NVIDIA Tesla M60-GPUs und Grafiktreibern ab Version 369.17 zur Verfügung.

Auf den VDAs muss HDX 3D Pro für die GPU-Beschleunigung aktiviert sein. Weitere Informationen finden Sie unter "GPU-Beschleunigung für Windows-Desktopbetriebssysteme"sowie "GPU-Beschleunigung für Windows-Serverbetriebssysteme".

Wenn ein VDA auf mehrere GPUs greift, zeigt das Auslastungsdiagramm den Durchschnitt der bei den einzelnen GPUs gesammelten Kennzahlen. GPU-Kennzahlen werden für den gesamten VDA und nicht für einzelne Prozesse gesammelt.

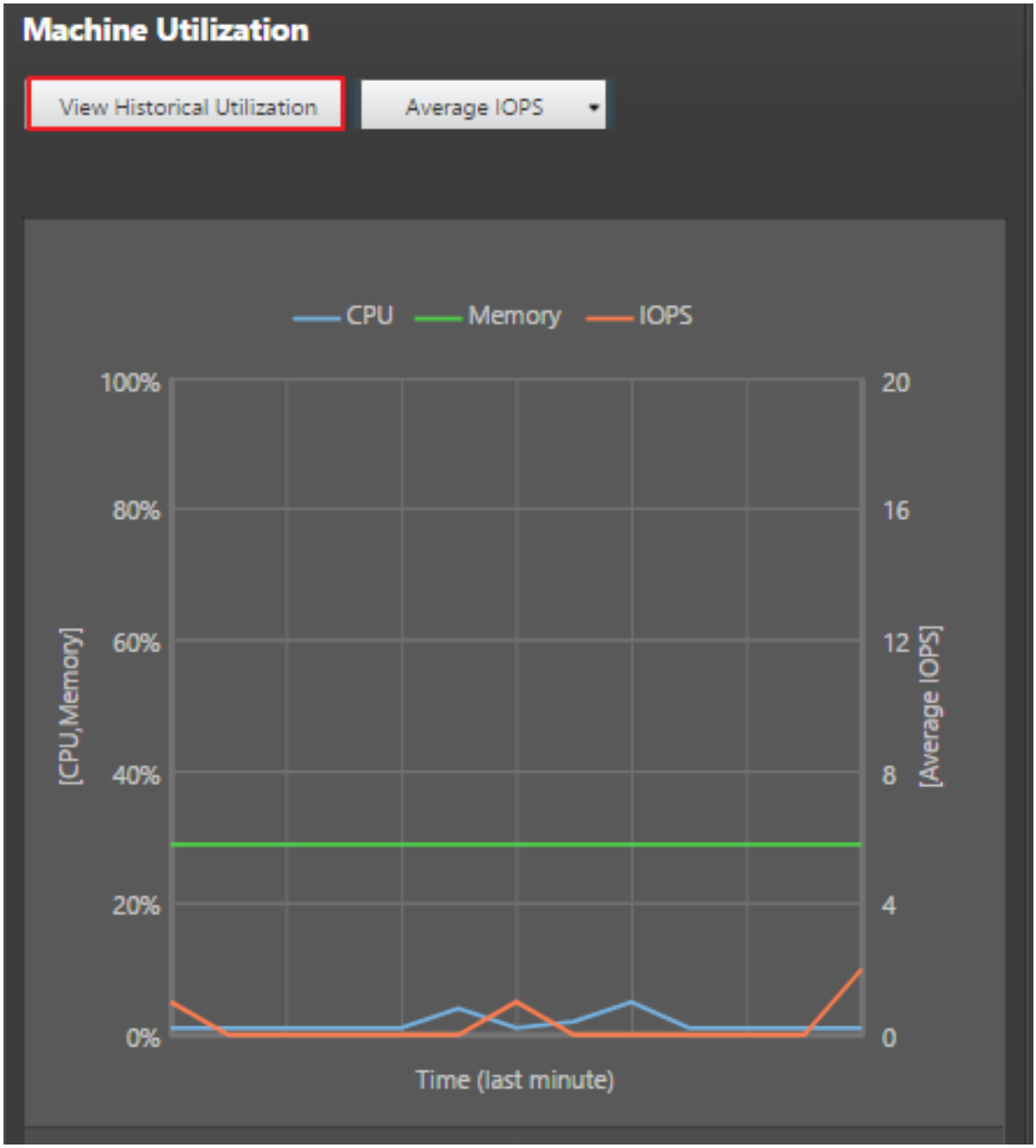
Historische Ressourcennutzung auf Maschinen

Klicken Sie im Bereich **Maschinenauslastung** auf **Historische Auslastung anzeigen**, um die historische Auslastung der Ressourcen auf der ausgewählten Maschine anzuzeigen.

Die Auslastungsdiagramme enthalten wichtige Leistungsindikatoren für CPU, Speicher, maximale gleichzeitige Sitzungen, durchschnittliche IOPS und Datenträgerlatenz.

Hinweis: Die Überwachungsrichtlinieneinstellung **Prozessüberwachung aktivieren** muss auf "Zugelassen"festgelegt sein, damit Daten für die Tabelle "Top-10-Prozesse"auf der Seite "Historische Maschinenauslastung"gesammelt und angezeigt werden können. Die Sammlung ist standardmäßig auf "Nicht zugelassen"festgelegt.

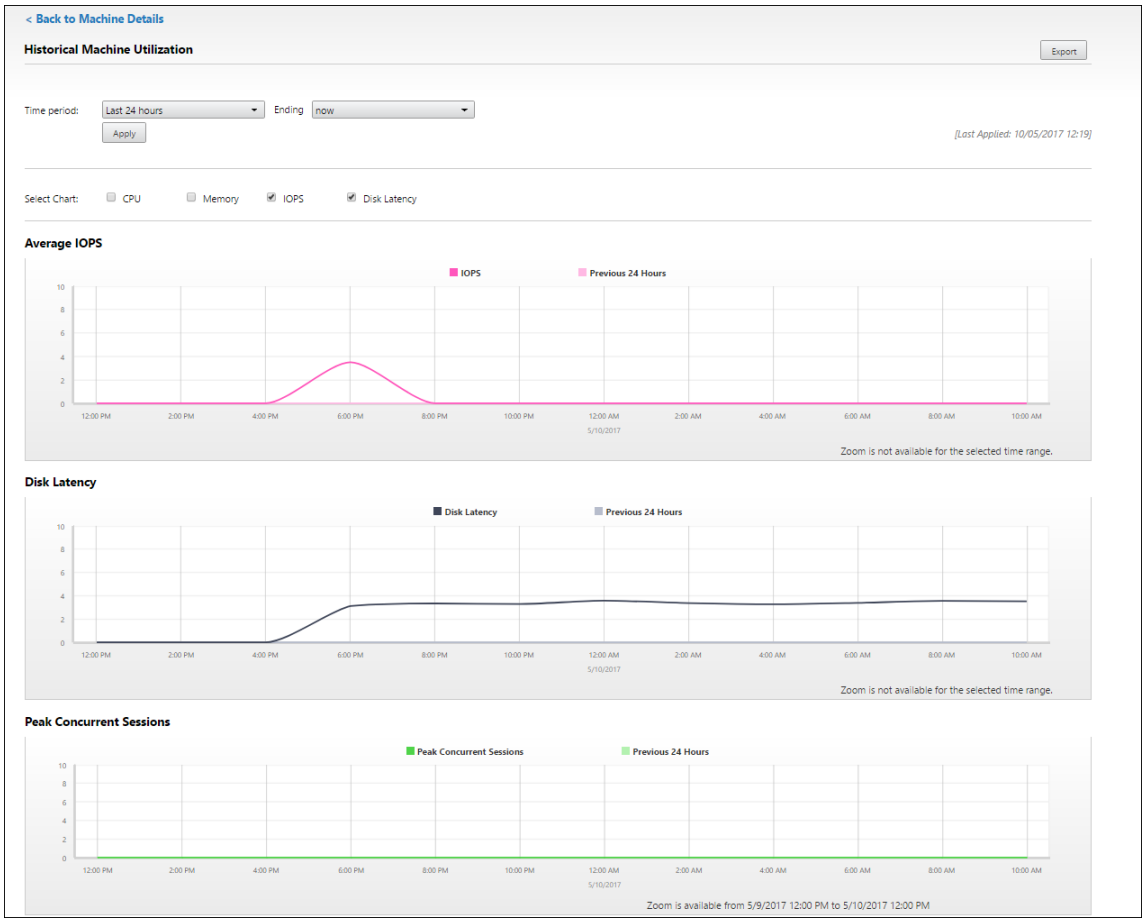
Daten zur CPU- und Arbeitsspeicherauslastung sowie IOPS und Datenträgerlatenz werden standardmäßig gesammelt. Die Datensammlung kann über die Richtlinieneinstellung **Ressourcenüberwachung aktivieren** deaktiviert werden.



1. Wählen Sie im Bereich **Maschinenauslastung** der Ansicht **Maschinendetails** die Option **Historische Auslastung anzeigen**. Damit wird die Seite **Historische Maschinenauslastung** geöffnet.
2. Legen Sie den **Zeitraum** für die Anzeige auf die letzten 2 oder 24 Stunden, auf die letzten 7 Tage, den letzten Monat oder das letzte Jahr fest.

Hinweis: IOPS-Durchschnitt und Datenträgerlatenz sind nur für die letzten 24 Stunden, den letzten Monat und das letzte Jahr verfügbar. Eine benutzerdefinierte Einstellung der Endzeit wird nicht unterstützt.

3. Klicken Sie auf **Anwenden** und wählen Sie die erforderlichen Diagramme aus.
4. Zeigen Sie auf die einzelnen Abschnitte des Diagramms, um weitere Informationen zu dem ausgewählten Zeitabschnitt einzublenden.



Wenn Sie beispielsweise **Letzte 2 Stunden** auswählen, gelten als Basiszeitraum die 2 Stunden vor dem ausgewählten Zeitraum. Angezeigt werden die Trends für CPU, Arbeitsspeicher und Sitzungen über die letzten 2 Stunden und die Grundlinienzeit.

Wenn Sie **Letzten Monat** auswählen, gilt der Vormonat als Basiszeitraum. Wählen Sie die Anzeige der durchschnittlichen IOPS und Datenträgerlatenz im letzten Monat und den Basiszeitraum.

5. Klicken Sie auf **Exportieren**, um die Ressourcenauslastungsdaten für den gewählten Zeitraum zu exportieren. Weitere Informationen finden Sie unter "Überwachen von Bereitstellungen"im Abschnitt Exportieren von Berichten.
6. Unterhalb der Diagramme wird eine Tabelle mit den 10 Prozessen mit der höchsten CPU-

bzw. Speicherauslastung angezeigt. Sie können diese nach einer beliebigen Spalte (Anwendungsname, Benutzername, Sitzungs-ID, CPU-Durchschnitt, CPU-Maximum, Speicherdurchschnitt und Speichermaximum) sortieren. Die Spalten für IOPS und Datenträgerlatenz können nicht sortiert werden.

Hinweis: Die Sitzungs-ID für Systemprozesse wird mit "0000"angegeben.

7. Zum Anzeigen des historischen Trends für den Ressourcenverbrauch einzelner Prozesse können Sie einen Drilldown für jeden der aufgelisteten Top-10-Prozesse durchführen.

Featurekompatibilitätsmatrix

August 18, 2021

Sie können zwar innerhalb jeder Site ältere VDA- oder Delivery Controller-Versionen verwenden, jedoch sind dann u. U. nicht alle Features der aktuellen Director-Version verfügbar. Darüber hinaus hängt die Verfügbarkeit von Features von der Lizenz der Site ab. Citrix empfiehlt die Ausführung von Director, Delivery Controllern und VDAs in der gleichen Version.

Hinweis: Nach dem Upgrade eines Delivery Controllers werden Sie beim Öffnen von Studio aufgefordert, die Site zu aktualisieren. Weitere Informationen finden Sie unter **Upgrade einer Bereitstellung** im Abschnitt Aktualisierungsreihenfolge.

In der folgenden Tabelle sind Director-Features und die erforderliche Mindestversion von Delivery Controller (DC), VDA und anderer abhängiger Komponenten sowie die Lizenz-Edition aufgeführt.

Director-Version	Feature	Abhängigkeiten - erforderliche Mindestversion	Edition
7.15	Überwachen von Anwendungsstörungen	DC 7.15 und VDA 7.15	Alle
7.14	Anwendungszentrierte Problembehandlung	DC 7.13 und VDA 7.13	Alle
7.14	Datenträgerüberwachung	DC 7.14 und VDA 7.14	Alle
7.14	GPU-Überwachung	DC 7.14 und VDA 7.14	Alle
7.13	Transportprotokoll in den Sitzungsdetails	DC 7.x und VDA 7.13	Alle

Director-Version	Feature	Abhängigkeiten - erforderliche Mindestversion	Edition
7.12	Benutzerfreundliche Beschreibung von Verbindungs- und Maschinenfehlern	DC 7.12 und VDA 7.x	Alle
7.12	Historische Daten in Enterprise Edition länger verfügbar	DC 7.12 und VDA 7.x	Enterprise
7.12	Benutzerdefinierte Berichte	DC 7.12 und VDA 7.x	Platinum
7.12	Automatisierte Director-Benachrichtigungen mit SNMP-Traps	DC 7.12 und VDA 7.x	Platinum
7.11	Ressourcenauslastungsbericht	DC 7.11 und VDA 7.11	Alle
7.11	Warnungen erweitert auf CPU-, Speicher- und ICA-RTT-Bedingungen	DC 7.11 und VDA 7.11	Platinum
7.11	Verbesserungen am Berichtexport	DC 7.11 und VDA 7.x	Alle
7.11	Automatisierte Director-Benachrichtigungen mit Citrix Octoblu	DC 7.11 und VDA 7.x	Platinum
7.11	Kombination mit NetScaler MAS	DC 7.11, VDA 7.x und MAS-Version 11.1 Build 49.16	Platinum
7.9	Anmeldedauer	DC 7.9 und VDA 7.x	Alle
7.7	Proaktive Überwachung und Warnungen	DC 7.7 und VDA 7.x	Platinum

Director-Version	Feature	Abhängigkeiten - erforderliche Mindestversion	Edition
7.7	SCOM-Integration	DC 7.7, VDA 7.x, SCOM 2012 R2 und PowerShell 3.0	Platinum
7.7	Integration der Windows-Authentifizierung	DC 7.x und VDA 7.x	Alle
7.7	Nutzung von Desktop- und Serverbetriebssystem	DC 7.7 und VDA 7.x	Platinum
7.6.300	Unterstützung für Framehawk Virtual Channel	DC 7.6 und VDA 7.6	Alle
7.6.200	Integration der Sitzungsaufzeichnung	DC 7.6 und VDA 7.x	Platinum
7	Integration von HDX Insight	DC 7.6, VDA 7.x und NetScaler Insight Center	Platinum

Datengranularität und -beibehaltung

March 19, 2020

Aggregation von Datenwerten

Der Überwachungsdienst erfasst diverse Daten über Benutzersitzungsnutzung, Benutzeranmeldeleistung, Sitzungslastausgleich und zu Fehlern bei Verbindungen und Maschinen. Die Daten werden je nach Kategorie unterschiedlich aggregiert. Zum Interpretieren der Daten sind Kenntnisse über die Aggregation der mit den OData-Methoden-APIs abgerufenen Datenwerte unverzichtbar. Beispiel:

- Fehler bei verbundenen Sitzungen und Maschinen treten über einen Zeitraum verteilt auf. Daher werden sie per Zeitraum als Höchstwerte angegeben.

- Die Anmeldedauer ist ein Zeitlängenwert und wird daher als Durchschnitt per Zeitraum angegeben.
- Die Anzahl der Anmeldungen und Verbindungsfehler repräsentieren eine Anzahl von Vorkommen in einem bestimmten Zeitraum und werden als Summen in einem Zeitraum gemacht.

Gleichzeitigkeit von Daten

Sitzungen müssen sich überschneiden, um als gleichzeitig angesehen zu werden. Bei einem Zeitintervall von 1 Minute werden jedoch alle Sitzungen in dieser Minute (mit oder ohne Überschneidung) als gleichzeitig angesehen, d. h. das Intervall ist so klein, dass sich der Mehraufwand für die Berechnung der Genauigkeit nicht lohnt. Finden die Sitzungen in der gleichen Stunde, aber nicht in der gleichen Minute statt, werden sie als einander nicht überschneidend angesehen.

Korrelation zwischen Zusammenfassungstabellen und Rohdaten

Das Datenmodell stellt Metriken auf zwei verschiedene Arten dar:

- Die Zusammenfassungstabellen zeigen aggregierte Ansichten der Metriken in Granularitäten pro Minute, Stunde und Tag an.
- Die Rohdaten stehen für einzelne Ereignisse oder den aktuellen Zustand, der bzw. die für eine Sitzung, Verbindung, Anwendung und andere Objekte protokolliert werden.

Wenn Sie versuchen, Daten über API-Aufrufe hinweg oder innerhalb des Datenmodells selbst zu korrelieren, sollten Sie die folgenden Konzepte und Einschränkungen kennen:

- **Keine Zusammenfassungsdaten für Teilintervalle:** Die Zusammenfassungen von Metriken erfüllen die Anforderungen von historischen Trends über lange Zeiträume hinweg. Diese Metriken werden für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Für Teilintervalle am Anfang (die ältesten verfügbaren Daten) und am Ende der Datensammlung gibt es keine Zusammenfassungsdaten. Beim Anzeigen der Aggregation eines Tages (Intervall=1440) bedeutet dies, dass der erste Tag und der aktuelle unvollständige Tag keine Daten aufweisen. Obwohl für diese Teilintervalle u. U. Rohdaten vorhanden sind, werden sie nie zusammengefasst. Sie können das früheste und letzte Aggregationsintervall für eine bestimmte Datengranularität festlegen, indem Sie die Mindest- und Höchstwerte für "SummaryDate"aus einer bestimmten Zusammenfassungstabelle nehmen. Die Spalte "SummaryDate"stellt den Start des Intervalls dar. Die Spalte "Granularity"steht für die Länge des Intervalls der aggregierten Daten.
- **Korrelation nach Zeit:** Metriken werden, wie oben beschrieben, für vollständige Intervalle in der Zusammenfassungstabelle aggregiert. Sie können für historische Trends verwendet werden, aber rohe Ereignisdaten stellen möglicherweise einen aktuelleren Zustand dar als die

Zusammenfassung für die Trendanalyse. Bei zeitbasierten Vergleichen zwischen der Zusammenfassung und den Rohdaten muss beachtet werden, dass es keine Zusammenfassungsdaten für Teilintervalle gibt, die am Anfang und Ende des Zeitraums auftreten.

- **Verpasste und latente Ereignisse:** Wenn Ereignisse verpasst werden oder während des Aggregationszeitraums latent sind, sind die für die Zusammenfassungstabelle aggregierten Metriken möglicherweise ungenau. Obwohl der Überwachungsdienst versucht, einen genauen aktuellen Zustand zu erhalten, wird die Aggregation für verpasste oder latente Ereignisse nicht im Nachhinein neu für die Zusammenfassungstabellen berechnet.
- **Hochverfügbare Verbindungen:** Bei hoher Verfügbarkeit von Verbindungen entstehen in den Zusammenfassungsdaten für aktuelle Verbindungen Lücken, aber die Sitzungsinstanzen werden dennoch in den Rohdaten ausgeführt.
- **Beibehaltungszeitraum für Daten:** Daten werden in den Zusammenfassungstabellen basierend auf einem anderen Bereinigungszeitplan beibehalten als Rohdaten von Ereignissen. Daten fehlen möglicherweise, weil die Zusammenfassungstabellen oder die unformatierten Tabellen bereinigt wurde. Beibehaltungszeiträume können unterschiedliche Granularitäten für Zusammenfassungsdaten aufweisen. Daten basierend auf niedrigerer Granularität (Minuten) werden schneller bereinigt als Daten, die auf höherer Granularität (Tage) basieren. Wenn Daten bereinigt wurden und in einer Granularitätskategorie fehlen, sind sie möglicherweise in einer höheren Granularitätskategorie. API-Aufrufe geben nur Daten für die angeforderte Granularität zurück. Wenn für eine Granularität keine Daten zurückgegeben werden, sind möglicherweise für den gleichen Zeitraum Daten für eine höhere Granularität vorhanden.
- **Zeitzonen:** Metriken werden mit UTC-Zeitstempeln gespeichert. Zusammenfassungstabellen werden basierend auf stündlichen Zeitzonengrenzen aggregiert. Bei Zeitzonen, die nicht in diese stündlichen Grenzen fallen, gibt es möglicherweise Unstimmigkeiten beim Ort der Datenaggregation.

Datengranularität und -beibehaltung

Die Granularität der aggregierten Daten, die von Director abgerufen werden, ist eine Funktion des angeforderten Zeitraums (T). Folgende Regeln gelten:

- 0 < T <= 1 Stunde: minutengenaue Granularität wird verwendet
- 0 <T <=30 Tage: stundengenaue Granularität wird verwendet
- T > 31 Tage: tagesgenaue Granularität wird verwendet

Angeforderte Daten, die nicht von aggregierten Daten stammen, stammen von den rohen Sitzungs- und Verbindungsinformationen. Diese Menge dieser Daten nimmt schnell zu, daher haben sie eine eigene Bereinigungseinstellung. Bereinigung gewährleistet, dass nur relevante Daten langfristig gespeichert werden. Damit wird eine bessere Leistung sichergestellt, während die für die Berichterstellung erforderliche Granularität beibehalten werden kann. Bei einer Site mit Platinum-Lizenz kann

der Aufbewahrungszeitraum auf die gewünschte Anzahl an Tagen eingestellt werden, ansonsten wird der Standardwert verwendet.

Um auf die Einstellungen zuzugreifen, führen Sie die folgenden PowerShell-Befehle auf dem Delivery Controller aus:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>

<!--NeedCopy-->
```

Mit den folgenden Einstellungen wird die Bereinigung gesteuert:

	Einstellungsname	Betroffene Bereinigung	Standardwert für Platinum (Tage)	Standardwert für andere Lizenzen (Tage)
1	GroomSessionsRetentionDays	Beibehaltungszeitraum für Sitzungs- und Verbindungsinformationen nach Beenden der Sitzung	90	7
2	GroomFailuresRetentionDays	Einträge für MachineFailureLog und ConnectionFailureLog	90	7
3	GroomLoadIndexesRetentionDays	Einträge für LoadIndex	90	7

	Einstellungsname	Betroffene Bereinigung	Standardwert für Platinum (Tage)	Standardwert für andere Lizenzen (Tage)
4	GroomDeletedRetentionDays	MaintainDays, Katalog-, Desktopgruppen- und Hypervisoren-titäten, die einen LifecycleState von “Deleted” haben. Dadurch werden auch zugehörige Einträge für Sitzung, Sitzungsde-tail, Zusammen-fassung, Fehler oder LoadIndex gelöscht.	90	7
5	GroomSummariesRetentionDays	Einträge für Desktop-GroupSum-mary, FailureLog-Summary und LoadIndex-Summary. Aggregierte Daten, tägliche Granularität	90	7

	Einstellungsname	Betroffene Bereinigung	Standardwert für Platinum (Tage)	Standardwert für andere Lizenzen (Tage)
6	GroomMachineHotfixLogRetentionDays	Auf VDA- und Controller-maschinen angewendete Hotfixes	90	90
7	GroomMinuteRetentionDays	Aggregierte Daten - minutengenaue Granularität	3	3
8	GroomHourlyRetentionDays	Aggregierte Daten - stundengenaue Granularität	32	7
9	GroomApplicationUsageRetentionDays	Anwendungsverlauf	90	0
10	GroomNotificationLogRetentionDays	Benachrichtigungsprotokolldaten	90	
11	GroomResourceUsageRawDataRetentionDays	Rohdaten zur Ressource-nauslastung	1	1
12	GroomResourceUsageMinuteDataRetentionDays	Zusammengefasste Daten zur Ressource-nauslastung mit minuten-genauer Granularität	7	7
13	GroomResourceUsageHourDataRetentionDays	Zusammengefasste Daten zur Ressource-nauslastung mit stunden-genauer Granularität	30	7

	Einstellungsname	Betroffene Bereinigung	Standardwert für Platinum (Tage)	Standardwert für andere Lizenzen (Tage)
14	GroomResourceUsageDayDataRetentionDays	Zugeordnete Daten zur Ressourcennauslastung mit tagesgenauer Granularität	90	7
15	GroomProcessUsageRawDataRetentionDays	Rohdaten zur Prozessauslastung	1	1
16	GroomProcessUsageMinuteDataRetentionDays	Zugeordnete Daten zur Auslastung mit minutengenauer Granularität	3	3
17	GroomProcessUsageHourDataRetentionDays	Zugeordnete Daten zur Auslastung mit stundengenauer Granularität	7	7
18	GroomProcessUsageDayDataRetentionDays	Zugeordnete Daten zur Auslastung mit tagesgenauer Granularität	30	7
19	GroomSessionMetricsDataRetentionDays	Daten zu Sitzungskennzahlen	1	1
20	GroomMachineMetricsDataRetentionDays	Daten zu Maschinenkennzahlen	3	3

	Einstellungsname	Betroffene Bereinigung	Standardwert für Platinum (Tage)	Standardwert für andere Lizenzen (Tage)
21	GroomMachineMatchingDataRetentionDays	Zuordnung gespeicherter Daten zu Maschinenkennzahlen	90	7
22	GroomApplicationErrorsRetentionDays	Anwendungsfehlerdaten	1	1
23	GroomApplicationFaultsRetentionDays	Anwendungsabsturzdaten	1	1

Achtung: Nach dem Ändern von Werten in der Überwachungsdienstdatenbank ist ein Neustart des Diensts erforderlich, damit die neuen Werte wirksam werden. Führen Sie Änderungen an der Überwachungsdienstdatenbank nur mit Anleitung vom Citrix Support durch.

Hinweise zum Bereinigen der Aufbewahrung:
Die Einstellungen GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays und GroomSessionMetricsDataRetentionDays sind auf den Standardwert 1 beschränkt. GroomProcessUsageMinuteDataRetentionDays ist auf den Standardwert 3 beschränkt. Die PowerShell- Befehle zum Festlegen dieser Werte wurden deaktiviert, da die Menge der Prozessdaten schnell anwächst. Außerdem gelten folgende lizenzbasierte Aufbewahrungseinstellungen:

- **Sites mit Premium-Lizenz** - Sie können den Aufbewahrungszeitraum auf eine beliebige Anzahl an Tagen aktualisieren.
- **Sites mit Advanced-Lizenz** - Der Aufbewahrungszeitraum ist für alle Einstellungen auf 31 Tage beschränkt.
- **Alle anderen Sites** - Der Beibehaltungszeitraum ist für alle Einstellungen auf 7 Tage beschränkt.

Ausnahmen:

- GroomApplicationInstanceRetentionDays kann nur für Sites mit Premium-Lizenz festgelegt werden.
- GroomApplicationErrorsRetentionDays und GroomApplicationFaultsRetentionDays sind bei Sites mit Premium-Lizenz auf 31 Tage begrenzt.

Das Beibehalten von Daten über lange Zeiträume hinweg hat die folgenden Auswirkungen auf die Größe von Tabellen:

- **Stundengenaue Daten:** Wenn Sie stundengenaue Daten bis zu zwei Jahre lang in der Datenbank speichern, wächst die Datenbank einer Site mit 1000 Bereitstellungsgruppen ungefähr wie folgt an:

1000 Bereitstellungsgruppen x 24 Stunden/Tag x 365 Tage/Jahr x 2 Jahre = 17.520.000 Datenreihen. Diese große Datenmenge in den Aggregationstabellen hat beträchtliche Auswirkungen auf die Leistung. Wenn man bedenkt, dass die Dashboarddaten aus dieser Tabelle gezogen werden, sind die Anforderungen an den Datenbankserver möglicherweise riesig. Übermäßig viele Daten können dramatische Auswirkungen auf die Leistung haben.

- **Sitzungs- und Ereignisdaten:** Diese Daten werden jedes Mal gesammelt, wenn eine Sitzung gestartet und eine Verbindung/Wiederverbindung hergestellt wird. Bei einer großen Site (100.000 Benutzer) nimmt die Menge dieser Daten sehr schnell zu. Beispielsweise entsprechen die über zwei Jahre gespeicherten Tabellen mehr als ein TB Daten und erfordern eine High-End-Unternehmensdatenbank.

Ursachen und Behebung von Fehlern in Citrix Director

August 18, 2021

In den folgenden Tabellen werden Fehlerkategorien, Ursachen und Maßnahmen zur Lösung der Probleme beschrieben. Weitere Informationen finden Sie unter Aufzählungswerte, Fehlercodes und Beschreibungen.

Verbindungsfehler

Kategorie	Grund	Problem	Aktion
Nicht zutreffend	[0] Unbekannt. Fehlercode ist nicht zugewiesen.	Der Überwachungsdienst kann den Grund für den Start- oder Verbindungsfehler nicht anhand der vom Brokerdienst erhaltenen Informationen ermitteln.	Sammeln Sie CDF-Protokolle auf dem Controller und wenden Sie sich an den Citrix Support.
[0] -	[1] -	-	Nicht zutreffend

Kategorie	Grund	Problem	Aktion
[2] MachineFailure	[2] SessionPreparation	Vorbereitungsanforderung für Sitzung vom Delivery Controller an den VDA ist fehlgeschlagen. Mögliche Ursachen: Kommunikationsprobleme zwischen Controller und VDA, Probleme im Brokerdienst beim Erstellen einer Vorbereitungsanforderung oder Netzwerkprobleme, aufgrund derer der VDA die Anforderung nicht akzeptiert.	Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops enthalten Informationen zu häufigen Ursachen für Kommunikationsprobleme zwischen Controller und VDA.
[2] MachineFailure	[3] RegistrationTimeout	Der VDA war eingeschaltet, aber während des Registrierungsversuchs beim Delivery Controller ist ein Timeout aufgetreten.	Vergewissern Sie sich, dass der Citrix Brokerdienst auf dem Delivery Controller und der Desktopdienst auf dem VDA ausgeführt wird. Starten Sie die Dienste, wenn sie nicht ausgeführt werden.

Kategorie	Grund	Problem	Aktion
[1] ClientConnection-Failure	[4] ConnectionTimeout	Der Client hat keine Verbindung mit dem VDA hergestellt, nachdem der VDA für den Sitzungsstart vorbereitet worden war. Die Sitzung wurde erfolgreich gebrokert, beim Warten auf die Verbindung des Clients mit dem VDA ist jedoch ein Timeout aufgetreten. Mögliche Ursachen: Firewalleinstellungen, Netzwerkunterbrechungen oder Einstellungen, die Remoteverbindungen verhindern.	Überprüfen Sie in der Director-Konsole, ob der Client zurzeit eine aktive Verbindung hat, d. h. kein Benutzer ist beeinträchtigt. Wenn keine Sitzung vorhanden ist, überprüfen Sie die Ereignisprotokolle auf dem Client und auf dem VDA auf Fehler. Beheben Sie alle Probleme mit der Netzwerkverbindung zwischen dem Client und dem VDA.
[4] NoLicensesAvailable	[5] Licensing	Die Lizenzierungsanforderung ist fehlgeschlagen. Mögliche Ursachen: Unzureichende Anzahl von Lizenzen oder Lizenzserver seit mehr als 30 Tagen ausgefallen.	Stellen Sie sicher, dass der Lizenzserver online und erreichbar ist. Beheben Sie jegliche Fehler an der Netzwerkverbindung des Lizenzservers bzw. starten Sie den Lizenzserver neu, wenn er nicht einwandfrei läuft. Stellen Sie sicher, dass es in der Umgebung genug Lizenzen gibt und teilen Sie ggf. mehr zu.

Kategorie	Grund	Problem	Aktion
[1] ClientConnection-Failure	[6] Ticketing	Bei der Ticketausstellung ist ein Fehler aufgetreten, was darauf hinweist, dass die Clientverbindung zum VDA nicht mit der vermittelten Anforderung übereinstimmt. Ein Startanforderung-sticket wird vom Broker erstellt und in der ICA-Datei geliefert. Wenn der Benutzer versucht, eine Sitzung zu starten, validiert der VDA das Startan-forderungsticket in der ICA-Datei beim Broker. Mögliche Ursachen: ICA-Datei beschädigt oder der Benutzer versucht, eine nicht autorisierte Verbindung herzustellen.	Stellen Sie sicher, dass der Benutzer basierend auf in den Bereitstellungsgrup-pen definierten Benutzergruppen Zugriff auf die Anwendung oder den Desktop hat. Weisen Sie den Benutzer an, die Anwendung oder den Desktop neu zu starten, um festzustellen, ob es sich um ein einmaliges Problem handelt. Wenn das Problem erneut auftritt, überprüfen Sie die Ereignisprotokolle des Clientgeräts auf Fehlermeldungen. Stellen Sie sicher, dass der VDA, mit dem der Benutzer eine Verbindung herzustellen versucht, registriert ist. Ist er nicht registriert, überprüfen Sie die Ereignisprotokolle auf dem VDA und beheben Sie jegliche Reg-istrierungsprobleme.

Kategorie	Grund	Problem	Aktion
[1] ClientConnection-Failure	[7] Sonstiges	Nachdem der Client den VDA kontaktiert hatte, aber bevor die Verbindungssequenz abgeschlossen war, wurde eine Sitzung vom VDA als beendet gemeldet.	Stellen Sie sicher, dass die Sitzung nicht vor dem Start vom Benutzer beendet wurde. Starten Sie die Sitzung neu. Wenn das Problem weiter besteht, sammeln Sie die CDF-Protokolle und wenden Sie sich an den Support von Citrix.
[1] ClientConnection-Failure	[8] GeneralFail	Die Sitzung konnte nicht gestartet werden. Mögliche Ursachen: Der Start wurde angefordert, während der Broker noch im Start- bzw. der Initialisierung war, oder während des Brokerings ist ein interner Fehler aufgetreten.	Vergewissern Sie sich, dass der Citrix Brokerdienst ausgeführt wird, und starten Sie die Sitzung neu.
[5] Configuration	[9] MaintenanceMode	Der VDA oder die Bereitstellungsgruppe, zu der der VDA gehört, ist im Wartungsmodus.	Prüfen Sie, ob der Wartungsmodus erforderlich ist. Deaktivieren Sie den Wartungsmodus für die Bereitstellungsgruppe oder Maschine, wenn er nicht erforderlich ist, und weisen Sie den Benutzer an, weiterhin zu versuchen, die Verbindung wiederherzustellen.

Kategorie	Grund	Problem	Aktion
[5] Configuration	[10] ApplicationDisabled	Die Anwendung wurde vom Administrator deaktiviert und ist daher für Endbenutzer nicht zugänglich.	Wenn die Anwendung für Produktionsumgebungen vorgesehen ist, aktivieren Sie die Anwendung und weisen Sie den Benutzer an, die Verbindung wiederherzustellen.
[4] NoLicensesAvailable	[11] LicenseFeature Refused	Das verwendete Feature wird nicht von den vorhandenen Lizenzen abgedeckt.	Wenden Sie sich an einen Citrix Vertriebsmitarbeiter und lassen Sie sich bestätigen, welche Features von der Edition und dem Typ der vorhandenen Lizenz für Citrix Virtual Apps and Desktops abgedeckt werden.

Kategorie	Grund	Problem	Aktion
[3] NoCapacityAvailable	[13] SessionLimitReached	Alle VDAs werden verwendet und es gibt keine Kapazität zum Hosten zusätzlicher Sitzungen. Mögliche Ursachen: Alle VDAs werden verwendet (Einzelsitzungs-OS-VDAs) oder alle VDAs haben das konfigurierte Maximum für gleichzeitige Sitzungen erreicht (Multisitzungs-OS-VDAs).	Überprüfen Sie, ob VDAs im Wartungsmodus sind. Deaktivieren Sie den Wartungsmodus, wenn er nicht benötigt wird, um mehr Kapazität freizusetzen. Erhöhen Sie den Wert der Citrix Richtlinieneinstellung **Sitzungshöchstanzahl**, um mehr Sitzungen pro Server-VDA zuzulassen. Fügen Sie zusätzliche Multisitzungs-OS-VDAs hinzu. Fügen Sie zusätzliche Einzelsitzungs-OS-VDAs hinzu.
[5] Configuration	[14] DisallowedProtocol	Die Protokolle ICA und RDP sind nicht zulässig.	Führen Sie den PowerShell-Befehl **Get-BrokerAccessPolicyRule** auf dem Delivery Controller aus und überprüfen Sie, ob unter **AllowedProtocols** die gewünschten Protokolle aufgelistet werden. Dieses Problem tritt nur auf, wenn eine Fehlkonfiguration vorliegt.

Kategorie	Grund	Problem	Aktion
[5] Configuration	[15] ResourceUnavailable	Die Anwendung oder der Desktop, mit der bzw. dem der Benutzer eine Verbindung herstellen möchte, ist nicht verfügbar. Die Anwendung oder der Desktop ist möglicherweise nicht vorhanden oder es sind keine VDAs verfügbar, um sie/ihn auszuführen. Mögliche Ursachen: Die Veröffentlichung der Anwendung oder des Desktops wurde aufgehoben, die VDAs, die die Anwendung oder den Desktop hosten, haben die maximale Last erreicht oder die Anwendung oder der Desktop ist im Wartungsmodus.	Stellen Sie sicher, dass die Anwendung oder der Desktop immer noch veröffentlicht ist und die VDAs nicht im Wartungsmodus sind. Prüfen Sie, ob die Multisitzungs-OS-VDAs voll ausgelastet sind. Ist dies der Fall, stellen Sie weitere Multisitzungs-OS-VDAs bereit. Prüfen Sie, ob Einzelsitzungs-OS-VDAs für Verbindungen verfügbar sind. Stellen Sie bei Bedarf weitere Einzelsitzungs-OS-VDAs bereit.

Kategorie	Grund	Problem	Aktion
[5] Configuration	[16] ActiveSessionReconnectDisabled	Die ICA-Sitzung ist aktiv und mit einem anderen Endpunkt verbunden. Da **Wiederverbinden von aktiven Sitzungen** jedoch deaktiviert ist, kann der Client keine Verbindung mit der aktiven Sitzung herstellen.	Stellen Sie sicher, dass auf dem Delivery Controller **Wiederverbinden von aktiven Sitzungen** aktiviert ist. Stellen Sie sicher, dass der Wert von **DisableActiveSessionReconnect** in der Registrierung unter **HKEY_LOCAL_MACHINE\Software** auf 0 festgelegt ist.
[2] MachineFailure	[17] NoSessionToReconnect	Der Client hat versucht, die Verbindung mit einer bestimmten Sitzung wiederherzustellen, aber die Sitzung wurde beendet.	Versuchen Sie erneut, die Verbindung mit Workspace Control wiederherzustellen.

Kategorie	Grund	Problem	Aktion
[2] MachineFailure	[18] SpinUpFailed	Der VDA kann nicht für den Sitzungsstart eingeschaltet werden. Dies ist ein von Hypervisor gemeldetes Problem.	Wenn die Maschine weiterhin ausgeschaltet bleibt, versuchen Sie einen Start von Citrix Studio aus. Wenn dies fehlschlägt, überprüfen Sie die Verbindungen und Berechtigungen des Hypervisors. Wenn es sich bei dem VDA um eine über PVS bereitgestellte Maschine handelt, überprüfen Sie in der PVS-Konsole, ob die Maschine ausgeführt wird. Ist dies nicht der Fall, stellen Sie sicher, dass der Maschine eine persönliche vDisk zugewiesen ist, und melden Sie sich beim Hypervisor an, um die VM zurückzusetzen.
[2] MachineFailure	[19] Refused	Der Delivery Controller sendet eine Anforderung von einem Endbenutzer zum Vorbereiten einer Verbindung an den VDA, doch der VDA lehnt die Anforderung aktiv ab.	Prüfen Sie per Ping, ob Delivery Controller und VDA kommunizieren können. Ist dies nicht der Fall, lösen Sie jegliche Probleme mit der Firewall und dem Netzwerkrouting.

Kategorie	Grund	Problem	Aktion
[2] MachineFailure	[20] ConfigurationSet Failure	Der Delivery Controller hat die erforderlichen Konfigurationsdaten, wie Richtlinieneinstellungen und Sitzungsinformationen, während des Sitzungsstarts nicht an den VDA gesendet. Mögliche Ursachen: Kommunikationsprobleme zwischen Controller und VDA, Probleme im Brokerdienst beim Erstellen einer Konfigurationssatzanforderung oder Netzwerkprobleme, aufgrund derer der VDA die Anforderung nicht akzeptiert.	-
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	Die maximale Anzahl von Instanzen einer Anwendung wurde erreicht. Auf dem VDA können keine weiteren Instanzen der Anwendung geöffnet werden. Dieses Problem ist mit dem Feature für das Anwendungslimit verbunden.	Legen Sie die Anwendungseinstellung **Anzahl der gleichzeitig ausgeführten Instanzen beschränken auf** auf einen höheren Wert fest, wenn es die Lizenzierung erlaubt.

Kategorie	Grund	Problem	Aktion
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	Der Benutzer versucht, mehr als eine Instanz einer Anwendung zu öffnen, aber die Konfiguration der Anwendung lässt pro Benutzer nur eine Anwendungsinstanz zu. Dieses Problem ist mit dem Feature für das Anwendungslimit verbunden.	Standardmäßig ist nur eine Anwendungsinstanz pro Benutzer zulässig. Wenn mehrere Instanzen pro Benutzer erforderlich sind, deaktivieren Sie ggf. die Einstellung **Auf eine Instanz pro Benutzer beschränken** in der Anwendungseinstellung.
[1] ClientConnectionFailure	[23] Communication error	Der Delivery Controller hat versucht, Informationen an den VDA zu senden, z. B. eine Anforderung zum Vorbereiten einer Verbindung, aber während des Kommunikationsversuchs ist ein Fehler aufgetreten. Die Ursache sind u. U. Netzwerkstörungen.	Wird der Desktopdienst auf dem VDA bereits ausgeführt, starten Sie ihn neu, um den Registrierungsvorgang neu zu starten, und prüfen Sie, ob der VDA einwandfrei registriert wird. Prüfen Sie anhand des Anwendungsereignisprotokolls, ob die für den VDA konfigurierten Delivery Controller korrekt sind.

Kategorie	Grund	Problem	Aktion
[3] NoCapacityAvailable	[100] NoMachineAvailable Überwachungsdienst konvertiert [12] NoDesktopAvailable in diesen Fehlercode.	Der zugewiesene VDA, der die Sitzung starten soll, ist in einem ungültigen Zustand oder nicht verfügbar. Mögliche Ursachen: Der Energiezustand des VDAs ist unbekannt oder nicht verfügbar, der VDA wurde seit der letzten Benutzersitzung nicht neu gestartet, die Sitzung erfordert die aktivierte Sitzungsfreigabe doch diese ist deaktiviert oder der VDA wurde aus der Bereitstellungsgruppe oder der Site entfernt.	Prüfen Sie, ob der VDA in einer Bereitstellungsgruppe ist. Ist dies nicht der Fall, fügen Sie ihn der korrekten Bereitstellungsgruppe hinzu. Überprüfen Sie, ob ausreichend VDAs registriert und betriebsbereit sind, damit der vom Benutzer angeforderte veröffentlichte freigegebene Desktop oder die angeforderte Anwendung gestartet werden kann. Stellen Sie sicher, dass der Hypervisor, der die Verbindung hostet, nicht im Wartungsmodus ist.

Kategorie	Grund	Problem	Aktion
[2] MachineFailure	[101] MachineNotFunctional. Überwachungsdienst konvertiert [12] NoDesktopAvailable in diesen Fehlercode.	Der VDA ist nicht betriebsbereit. Mögliche Ursachen: Der VDA wurde aus der Bereitstellungsgruppe entfernt, der VDA ist nicht registriert, der Energiezustand des VDAs ist nicht verfügbar oder im VDA liegen Fehler vor.	Prüfen Sie, ob der VDA in einer Bereitstellungsgruppe ist. Ist dies nicht der Fall, fügen Sie ihn der korrekten Bereitstellungsgruppe hinzu. Prüfen Sie, ob der VDA in Citrix Studio als eingeschaltet angezeigt wird. Ist der Energiezustand mehrerer Maschinen unbekannt, beheben Sie Probleme bei der Hypervisor-Verbindung oder Hostingfehler. Stellen Sie sicher, dass der Hypervisor, der die Verbindung hostet, nicht im Wartungsmodus ist. Starten Sie den VDA neu, wenn die Probleme gelöst sind.

Maschinenfehlertyp

Fehlercode	Fehlercode-ID	Problem	Aktion
Unbekannt	-	-	-
Nicht registriert	3	-	-

Fehlercode	Fehlercode-ID	Problem	Aktion
MaxCapacity	4	Der Lastindex auf dem Hypervisor hat seine maximale Kapazität erreicht.	Stellen Sie sicher, dass alle Hypervisors eingeschaltet sind. Fügen Sie dem Hypervisor mehr Kapazität hinzu. Fügen Sie weitere Hypervisors hinzu.
StuckOnBoot	2	Die VM hat die Startsequenz nicht abgeschlossen und kommuniziert nicht mit dem Hypervisor.	Stellen Sie sicher, dass die VM auf dem Hypervisor erfolgreich gestartet wurde. Überprüfen Sie auch andere Meldungen auf der VM, z. B. zu Betriebssystemproblemen. Stellen Sie sicher, dass die Hypervisortools auf der VM installiert sind. Stellen Sie sicher, dass der VDA auf der VM installiert ist.
FailedToStart	1	Beim Starten der VM auf dem Hypervisor sind Probleme aufgetreten.	Überprüfen Sie die Hypervisorprotokolle.
-	0	-	-

Grund für die nicht vorhandene Registrierung von Maschinen (Fehlertyp “nicht registriert”oder “unbekannt”)

Fehlercode	Fehlercode-ID	Problem	Aktion
AgentShutdown	0	Der VDA wurde ordnungsgemäß heruntergefahren.	Schalten Sie den VDA ein, wenn er nicht aufgrund von Energieverwaltungsrichtlinien deaktiviert sein soll. Überprüfen die Ereignisprotokolle auf Fehler.
AgentSuspended	1	Der VDA ist im Ruhezustand oder Energiesparmodus.	Schalten Sie den VDA aus dem Ruhezustand um in den Betrieb. Deaktivieren Sie den Ruhezustand für Citrix Virtual Apps and Desktops-VDAs über die Energieeinstellungen.
IncompatibleVersion	100	Der VDA kann wegen einer Diskrepanz in den Citrix Protokollversionen nicht mit dem Delivery Controller kommunizieren.	Stellen Sie sicher, dass die Versionen von VDA und Delivery Controller dieselben sind.

Fehlercode	Fehlercode-ID	Problem	Aktion
AgentAddressResolutionFailed	101	Der Delivery Controller konnte die IP-Adresse des VDAs nicht auflösen.	Stellen Sie sicher, dass das VDA-Maschinenkonto in AD vorhanden ist. Ist dies nicht der Fall, erstellen Sie es. Überprüfen Sie den Namen und die IP-Adresse des VDAs in DNS. Sind sie nicht korrekt, korrigieren Sie sie. Ist das Problem verbreitet, prüfen Sie die DNS-Einstellungen auf den Delivery Controllern. Überprüfen Sie die DNS-Auflösung über den Controller mit dem Befehl `nslookup`.
	101	Der Delivery Controller konnte die IP-Adresse des VDAs nicht auflösen.	Stellen Sie sicher, dass das VDA-Maschinenkonto in AD vorhanden ist. Ist dies nicht der Fall, erstellen Sie es. Überprüfen Sie den Namen und die IP-Adresse des VDAs in DNS. Sind sie nicht korrekt, korrigieren Sie sie.

Fehlercode	Fehlercode-ID	Problem	Aktion
AgentNotContactable	102	Zwischen dem Delivery Controller und dem VDA ist ein Kommunikationsproblem aufgetreten.	Prüfen Sie per Ping, ob Delivery Controller und VDA kommunizieren können. Ist dies nicht der Fall, lösen Sie jegliche Probleme mit der Firewall und dem Netzwerk. Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) enthalten Informationen zu häufigen Ursachen für Kommunikationsprobleme zwischen Controller und VDA.

Fehlercode	Fehlercode-ID	Problem	Aktion
	102	Zwischen dem Delivery Controller und dem VDA ist ein Kommunikationsproblem aufgetreten.	Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) enthalten Informationen zu häufigen Ursachen für Kommunikationsprobleme zwischen Controller und VDA. Wenden Sie sich an den Citrix Support.
AgentWrongActiveDirectoryOU	103	Bei der Active Directory-Ermittlung ist ein Konfigurationsfehler aufgetreten. Die in der VDA-Registrierung konfigurierte sitespezifische Organisationseinheit, in der die Informationen zum Site-Controller in Active Directory gespeichert werden, ist für eine andere Site.	Stellen Sie sicher, dass die Active Directory-Konfiguration richtig ist, oder überprüfen Sie die Registrierungseinstellungen.

Fehlercode	Fehlercode-ID	Problem	Aktion
EmptyRegistrationRequest	104	Die vom VDA an den Delivery Controller gesendete Registrierungsanforderung war leer. Grund kann eine beschädigte VDA-Softwareinstallation sein.	Starten Sie den Desktopdienst auf dem VDA neu, um den Registrierungsvorgang neu zu starten, und validieren Sie die VDA-Registrierung mit dem Anwendungsereignisprotokoll.
MissingRegistrationCapabilities	105	Die VDA-Version ist nicht mit dem Delivery Controller kompatibel.	Aktualisieren Sie den VDA oder entfernen Sie den VDA und installieren Sie ihn neu.
MissingAgentVersion	106	Die VDA-Version ist nicht mit dem Delivery Controller kompatibel.	Installieren Sie die VDA-Software neu, wenn sich das Problem auf alle Maschinen auswirkt.

Fehlercode	Fehlercode-ID	Problem	Aktion
InconsistentRegistrationCapabilities	107	Der VDA kann seine Funktionen nicht an den Broker melden. Dies kann auf eine fehlende Kompatibilität zwischen VDA- und des Delivery Controller-Version zurückzuführen sein. Die Registrierungsfunktionen, die sich mit jeder Version ändern, werden in einer Form ausgedrückt, die nicht mit der Registrierungsanforderung übereinstimmt.	Stellen Sie sicher, dass die Versionen von VDA und Delivery Controller dieselben sind.
NotLicensedForFeature	108	Das Feature, das Sie verwenden möchten, ist nicht lizenziert.	Überprüfen Sie die Edition der Citrix Lizenzierung oder entfernen Sie den VDA und installieren Sie ihn neu.
	108	Das Feature, das Sie verwenden möchten, ist nicht lizenziert.	Wenden Sie sich an den Citrix Support.
UnsupportedCredentialSecurityversion	109	VDA und Delivery Controller verwenden nicht dieselben Verschlüsselungsmethoden.	Stellen Sie sicher, dass die Versionen von VDA und Delivery Controller dieselben sind.

Fehlercode	Fehlercode-ID	Problem	Aktion
InvalidRegistrationRequest	110	Der VDA hat eine Registrierungsanforderung an den Broker gesendet, aber der Inhalt der Anforderung ist beschädigt oder ungültig.	Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) enthalten Informationen zu häufigen Ursachen für Kommunikationsprobleme zwischen Controller und VDA.
SingleMultiSessionMismatch	111	Der Betriebssystemtyp des VDAs ist nicht mit dem Maschinenkatalog oder der Bereitstellungsgruppe kompatibel.	Fügen Sie den VDA dem richtigen Maschinenkatalogtyp oder der Bereitstellungsgruppe hinzu, die Maschinen mit dem gleichen Betriebssystem enthalten.
FunctionalLevelTooLowForCatalog	112	Der Maschinenkatalog hat eine höhere VDA-Funktionsebene als die installierte VDA-Version.	Stellen Sie sicher, dass die Funktionsebene des Maschinenkatalogs auf dem VDA mit der des VDAs übereinstimmt. Aktualisieren oder downgraden Sie den Maschinenkatalog so, dass er dem VDA entspricht.

Fehlercode	Fehlercode-ID	Problem	Aktion
FunctionalLevelTooLowForDesktopGroup	112	Die Bereitstellungsgruppe hat eine höhere VDA-Funktionsebene als die installierte VDA-Version.	Stellen Sie sicher, dass die Funktionsebene der VDA-Bereitstellungsgruppe mit der des VDAs übereinstimmt. Aktualisieren oder downgraden Sie den Maschinenkatalog so, dass er dem VDA entspricht.
PowerOff	200	Der VDA wurde nicht ordnungsgemäß heruntergefahren.	Wenn der VDA normalerweise eingeschaltet sein sollte, versuchen Sie, ihn über Citrix Studio zu starten und überprüfen Sie, ob er gestartet und richtig registriert wird. Beheben Sie jegliche Probleme beim Starten und bei der Registrierung. Überprüfen Sie die Ereignisprotokolle auf dem VDA, wenn er wieder ausgeführt wird, um die Ursache für das Herunterfahren zu bestimmen.

Fehlercode	Fehlercode-ID	Problem	Aktion
AgentRejectedSettingsUpdate	203	Einstellungen, z. B. Citrix Richtlinien, wurden geändert oder aktualisiert, doch beim Senden Änderungen an den VDA ist ein Fehler aufgetreten. Dies kann vorkommen, wenn die Änderungen nicht mit der VDA-Version kompatibel sind.	Aktualisieren Sie den VDA bei Bedarf. Überprüfen Sie, ob die angewendeten Aktualisierungen von der VDA-Version unterstützt werden.
SessionPrepareFailure	206	Der Broker hat keinen Audit der auf dem VDA ausgeführten Sitzungen durchgeführt.	Wenn es sich um ein verbreitetes Problem handelt, starten Sie ggf. den Citrix Brokerdienst auf dem Delivery Controller neu.
	206	Der Broker hat keinen Audit der auf dem VDA ausgeführten Sitzungen durchgeführt.	Wenden Sie sich an den Citrix Support.

Fehlercode	Fehlercode-ID	Problem	Aktion
ContactLost	207	Der Delivery Controller hat die Verbindung zum VDA verloren. Die Ursache sind u. U. Netzwerkstörungen.	Vergewissern Sie sich, dass der Citrix Brokerdienst auf dem Delivery Controller und der Desktopdienst auf dem VDA ausgeführt wird. Starten Sie die Dienste, wenn sie nicht ausgeführt werden. Wird der Desktopdienst auf dem VDA bereits ausgeführt, starten Sie ihn neu, um den Registrierungsvorgang neu zu starten, und prüfen Sie, ob der VDA einwandfrei registriert wird. Prüfen Sie anhand des Anwendungsereignis-protokolls, ob die für den VDA konfigurierten Delivery Controller korrekt sind. Prüfen Sie per Ping, ob Delivery Controller und VDA kommunizieren können. Ist dies nicht der Fall, lösen Sie jegliche Probleme mit der Firewall und dem Netzwerk.

Fehlercode	Fehlercode-ID	Problem	Aktion
	207	Der Delivery Controller hat die Verbindung zum VDA verloren. Die Ursache sind u. U. Netzwerkstörungen.	Stellen Sie sicher, dass der Desktopdienst auf dem VDA ausgeführt wird. Starten Sie ihn, wenn er nicht ausgeführt wird.
BrokerRegistrationLimitReached	301	Auf dem Delivery Controller wurde die konfigurierte maximale Anzahl von VDAs erreicht, die sich bei ihm registrieren dürfen. Standardmäßig sind auf einem Delivery Controller 10.000 VDA-Registrierungen zulässig.	Fügen Sie der Site Delivery Controller hinzu oder erstellen Sie eine Site. Mit dem Registrierungsschlüssel **HKEY_LOCAL_MACHINE\Software** können Sie auch die Anzahl der VDAs erhöhen, die gleichzeitig beim Delivery Controller registriert sein dürfen. Weitere Informationen finden Sie in dem Knowledge Center-Artikel Von Citrix Virtual Apps and Desktops verwendete Registrierungsschlüsseleinträge (CTX117446). Eine Erhöhung dieser Zahl erfordert möglicherweise mehr CPU- und Arbeitsspeicherressourcen für den Controller.

Fehlercode	Fehlercode-ID	Problem	Aktion
SettingsCreationFailure	208	Der Broker hat keinen Satz mit Einstellungen und Konfigurationen zum Senden an den VDA erstellt. Wenn der Broker die Daten nicht sammeln kann, schlägt die Registrierung fehl und der VDA ist nicht registriert.	Überprüfen Sie die Ereignisprotokolle auf dem Delivery Controller auf Fehler. Starten Sie den Brokerdienst neu, wenn kein spezifisches Problem in den Protokollen vermerkt ist. Wenn der Brokerdienst neu gestartet ist, starten Sie den Desktopdienst auf den betroffenen VDAs neu und prüfen Sie, ob die VDAs sich erfolgreich registrieren.
	208	Der Broker hat keinen Satz mit Einstellungen und Konfigurationen zum Senden an den VDA erstellt. Wenn der Broker die Daten nicht sammeln kann, schlägt die Registrierung fehl und der VDA ist nicht registriert.	Starten Sie den Desktopdienst auf den betroffenen VDAs neu und prüfen Sie, ob die VDAs sich erfolgreich registrieren. Wenden Sie sich an den Citrix Support.

Fehlercode	Fehlercode-ID	Problem	Aktion
SendSettingsFailure	204	Der Broker hat keine Einstellungen und Konfigurationsdaten an den VDA gesendet. Kann der Broker die Daten sammeln aber nicht senden, schlägt die Registrierung fehl.	Wenn nur ein VDA betroffen ist, starten Sie den Desktopdienst auf dem VDA neu, um die Neuregistrierung zu erzwingen und mit dem Anwendungsereignis-protokoll zu überprüfen, ob der VDA sich erfolgreich registriert. Beheben Sie jegliche aufgetretenen Fehler. Die Anweisungen zur Problembehandlung im Knowledge Center-Artikel Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668) enthalten Informationen zu häufigen Ursachen für Kommunikationsprob-leme zwischen Controller und VDA.
AgentRequested	2	Ein unbekannter Fehler ist aufgetreten.	Wenden Sie sich an den Citrix Support.
DesktopRestart	201	Ein unbekannter Fehler ist aufgetreten.	Wenden Sie sich an den Citrix Support.
DesktopRemoved	202	Ein unbekannter Fehler ist aufgetreten.	Wenden Sie sich an den Citrix Support.

Fehlercode	Fehlercode-ID	Problem	Aktion
SessionAuditFailure	205	Ein unbekannter Fehler ist aufgetreten.	Wenden Sie sich an den Citrix Support.
UnknownError	300	Ein unbekannter Fehler ist aufgetreten.	Wenden Sie sich an den Citrix Support.
RegistrationStateMismatch	302	Ein unbekannter Fehler ist aufgetreten.	Wenden Sie sich an den Citrix Support.
Unbekannt	-	Ein unbekannter Fehler ist aufgetreten.	Wenden Sie sich an den Citrix Support.

SDKs und APIs

August 18, 2021

Das aktuelle Release enthält mehrere SDKs und APIs. Weitere Informationen finden Sie unter Developer Documentation. Von dort aus können Sie auf Programmierinformationen für folgende Elemente zugreifen:

- Delivery Controller
- Überwachungsdienst-OData
- StoreFront

Mit dem Citrix Group Policy SDK können Sie Einstellungen und Filter für Gruppenrichtlinien anzeigen und konfigurieren. Es verwendet einen PowerShell-Anbieter, um einen virtuellen Datenträger zu erstellen, der mit den Maschinen- und Benutzereinstellungen und -filtern übereinstimmt. Der Anbieter wird als Erweiterung zu New-PSDrive angezeigt. Für die Verwendung des Group Policy SDKs muss Studio oder das XenApp- bzw. XenDesktop-SDK installiert sein. Weitere Informationen finden Sie unter Group Policy SDKs.

Delivery Controller SDK

Das SDK enthält mehrere PowerShell-Snap-Ins, die automatisch vom Installationsassistenten installiert werden, wenn Sie den Delivery Controller oder Studio installieren.

Berechtigungen: Sie müssen die Shell oder das Skript mit einer ID ausführen, die über Citrix Administratorrechte verfügt. Obwohl die Mitglieder der lokalen Administratorgruppe auf dem Controller automatisch über Volladministratorprivilegien verfügen, um XenApp bzw. XenDesktop zu installieren,

empfiehlt Citrix, dass Sie für den normalen Betrieb Citrix Administratoren mit den entsprechenden Rechten erstellen und nicht das lokale Administratorkonto verwenden. Wenn Sie Windows Server 2008 R2 ausführen, müssen Sie die Shell oder das Skript als Citrix Administrator und nicht als Mitglied der lokalen Administratorgruppe ausführen.

Zugreifen auf die Cmdlets:

1. Starten einer Shell in PowerShell: Öffnen Sie Studio, wählen Sie die Registerkarte **PowerShell** und klicken Sie auf **PowerShell starten**.
2. Legen Sie die Ausführungsrichtlinie in PowerShell fest, um SDK-Cmdlets in Skripts zu verwenden. Weitere Informationen zur PowerShell-Ausführungsrichtlinie finden Sie in der Dokumentation von Microsoft.
3. Fügen Sie mit dem Cmdlet **Add -PSSnapin** in der Windows PowerShell-Konsole die Snap-Ins hinzu, die Sie in der PowerShell-Umgebung benötigen.

V1 und V2 beziehen sich auf die Version des Snap-Ins. (XenDesktop 5-Snap-Ins sind Version 1; XenDesktop 7-Snap-Ins sind Version 2. Zum Installieren von XenDesktop 7-Snap-Ins geben Sie beispielsweise "Add-PSSnapin Citrix.ADIdentity.Admin.V2"ein.) Geben Sie zum Importieren aller Cmdlets "Add-PSSnapin Citrix"ein.⋆.Admin.V⋆

Nach dem Hinzufügen der Snap-Ins, können Sie auf die Cmdlets und die zugehörige Hilfe zugreifen.

Hinweis: Auf folgende Weise zeigen Sie die aktuelle XenApp- und XenDesktop-Hilfe zu PowerShell-Cmdlets an:

1. Fügen Sie mit der PowerShell-Konsole folgende Citrix Snap-Ins hinzu: Add –PSSnapin Citrix.⋆ .Admin.V⋆.
2. Folgen Sie den Anweisungen unter PowerShell Integrated Scripting Environment (ISE).

Group Policy SDKs

Für die Verwendung des Group Policy SDKs muss Studio oder das XenApp- bzw. XenDesktop-SDK installiert sein.

Zum Hinzufügen des Group Policy SDKs geben Sie **Add-PSSnapin citrix.common.grouppolicy** ein. (Zum Aufrufen der Hilfe geben Sie **help New-PSDrive -path localgpo:/** ein.)

Zum Erstellen einer virtuellen Festplatte und Laden dieser Festplatte mit Einstellungen geben Sie Folgendes ein: **New-PSDrive <*Standard Parameters*> [-PSProvider] CitrixGroupPolicy -Controller <*Zeichenfolge*>**, wobei die Controller-Zeichenfolge der vollqualifizierte Domänenname eines Controllers in der Site ist, aus der die Einstellungen geladen werden sollen.